nameshield
Online Assets Security

Comprendre les noms de domaine

Comment
optimiser sa visibilité
et défendre
sa marque
sur Internet.

Octobre 2016

Introduction

Depuis l'apparition du World Wide Web (WWW), littéralement la «toile (d'araignée) mondiale», communément appelé le Web, dans les années 1990 le nombre d'internautes n'a cessé d'augmenter, passant de 300 millions d'internautes en 2000 à 3,04 milliards en 2015 même si seule 42% de la population mondiale est connectée.

Face à l'incroyable développement d'Internet comme moyen privilégié de communication instantanée et globale, et alors que très peu de gens en dehors de la communauté technique savaient ce qu'était un nom de domaine, les utilisateurs réalisent aujourd'hui l'importance des noms de domaine dans l'acheminement du trafic de la messagerie électronique, la localisation de sites Web et surtout la construction d'une identité en ligne.
C'est grâce au nom de domaine que l'on vous repère sur internet, que vous êtes visible, que votre identité s'affiche et que vous développez votre business sur le net.

Les noms de domaine sont omniprésents dans le fonctionnement d'internet et il est impossible pour une entreprise voulant exister sur le net et développer son business, de ne pas déposer de noms de domaine

associés à son nom, sa marque, ses produits, ses services.

Enregistrer un nom de domaine n'est pas un acte anodin et nécessite de maîtriser de nombreux aspects marketing, juridiques, financiers, techniques, pour éviter des conséquences lourdes en termes de coûts et d'image.

Avec l'ouverture de plus de 1400 nouvelles extensions, le nom de domaine devient recherché et attaqué. Soyez donc conscient qu'un nom de domaine est porteur de l'image de l'entreprise au même titre que ses marques, qu'il fait partie de son capital immatériel, défendez-le !

Ce document a pour objectif de vous présenter de manière accessible l'évolution de la charte de nommage, les bonnes pratiques de gestion et d'optimisation de votre portefeuille de noms de domaine.

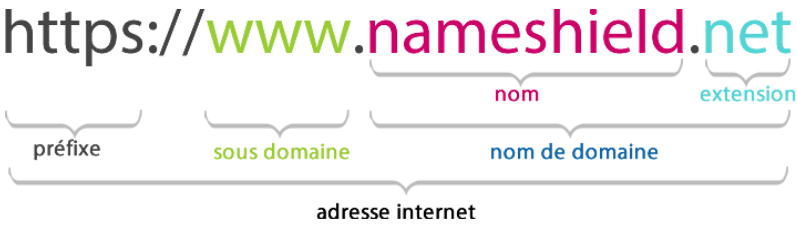
Bonne lecture.

Au sommaire

Les fondamentaux

C'est quoi un nom de domaine ?

Un nom de domaine est principalement utilisé pour identifier l'adresse d'un site internet et pour les courriers électroniques. Il est composé d'une série de caractères séparés par un point qui distingue l'extension (.com, .fr…).
Chaque ordinateur est relié à Internet via une adresse unique appelée "adresse IP" (adresse de protocole Internet). Le nom de domaine correspond donc à une adresse IP et permet d'identifier et de retenir plus facilement l'adresse d'un site Web.



Un nom de domaine est composé d'un nom (composé d'un ensemble de caractères alphanumériques), et d'un suffixe (.com, .fr, .eu, .org…). Cette suite constitue l'élément essentiel d'une adresse internet l'URL.

L'extension, que l'on appelle aussi suffixe du nom de domaine, correspond à la classification du domaine. On distingue ainsi plusieurs «catégories» de domaines, en fonction de leur origine géographique (.fr, .es, .it, .us…) ou de leur activité (.com pour commercial, .asso pour association, .org pour organisations à titre non lucratif…).

Le nom correspond le plus souvent au nom d'une marque, d'une société, d'une association, d'une personne. Il peut être constitué d'une suite de caractères (de A à Z et de 0 à 9) et d'un tiret. Le choix du nom du domaine est généralement libre… dans la mesure où celui-ci n'existe pas déjà ! C'est la fameuse règle du «premier arrivé, premier servi».

Le sous-domaine est la partie de l'adresse internet d'un site qui précède le nom de domaine. La syntaxe est «sousdomaine.votre-domaine.fr ». Le sous-domaine le plus connu et le plus utilisé est www (le web).

Vous pouvez créer simplement des sous-domaines qui permettront d'accéder rapidement à une partie de votre site comme par exemple : http://boutique.nameshield.net ou encore conseil.nameshield.net.

Les **sous-domaines** sont très pratiques pour scinder un site en plusieurs sections distinctes, avec chacune une adresse bien définie.

La lecture de décomposition d'un nom de domaine se fait de droite à gauche.

Le préfixe ou protocole de communication est une information technique terminée par «://». Le protocole le plus courant sur le Web est «http». Il est souvent absent dans ce qui est saisi par l'internaute car le navigateur le rajoute automatiquement lorsqu'il est absent. Les autres protocoles les plus connus sont : «https» (protocole sécurisé) et «ftp» (transfert de fichiers).

La lecture d'un nom de domaine

L'URL ou ADRESSE INTERNET

Pour l'internaute, la navigation sur Internet consiste, via son navigateur, à consulter des «pages Web» situées n'importe où dans le monde. Il faut donc pouvoir identifier chaque page de façon unique parmi les milliards de pages présentes sur le Net. Pour ce faire, chaque page Web est désignée par une URL (Uniform Resource Locator).

C'est à partir du nom de domaine complet que le serveur DNS « autorité » (et lui seul) peut donner l'adresse IP de la machine contenant la page Web recherchée.

Comme expliqué précédemment, la lecture d'un nom de domaine se fait de droite à gauche

Un «nom de domaine complet» est constitué d'une suite de «noms de domaines» organisés hiérarchiquement, le domaine de plus haut niveau étant situé à droite.

Le nom de domaine complet correspondant à l'ensemble des étiquettes des nœuds d'une arborescence, séparées par des points et terminé par un point final, est appelé adresse FQDN (Fully Qualified Domain Name, soit Nom de Domaine Totalement Qualifié)

Ainsi www.nameshield.net. représente une adresse FQDN.

Chaque nom de domaine est composé d'une chaîne de caractères. Les noms de domaine sont séparés par des «. points».

Considérant un domaine donné, le domaine de rang immédiatement inférieur (donc situé immédiatement à gauche) peut être considéré comme un «sous-domaine» du précédent (exemple : www. = sous domaine de Nameshield).

Le plus à droite : Le domaine de rang maximum est appelé la «**racine**» («root») de l'Internet. Par convention, ce domaine est représenté par un «.» sans rien à droite. En pratique, ce «.» n'est même jamais indiqué. Il est supposé exister par défaut (http://www.nameshield.net «.»)

A gauche du domaine racine : le domaine situé immédiatement à suivre est le «**Top Level Domain**», ou «**TLD**», ou «**extension**» (.net, .com, .fr, .biz, .paris).

A gauche du TLD : le nom de domaine situé immédiatement **à gauche du TLD** correspond à ce qu'on appelle habituellement le «**domaine**» d'une entreprise.

En continuant vers la gauche, les noms de domaine rencontrés sont dénommés «**noms de sous-domaine**» (de niveau 1, 2, … par rapport au «nom de domaine», le niveau hiérarchique changeant chaque fois qu'on rencontre un «.»).

L'adresse IP / Le système D.N.S.

L'ADRESSE IP (Internet Protocole)

Chaque ordinateur connecté à Internet dispose d'une adresse numérique unique (adresse IP) qui représente une chaîne de nombres difficile à mémoriser.

Une adresse IP est un numéro unique qui permet à un ordinateur connecté à un réseau utilisant le protocole TCP/IP (comme internet par exemple) de l'identifier. Une adresse IP est un nombre de 32 bits composé de 4 numéros allant de 0 à 255 séparés par des points, exemple: 192.68.122.28

Il existe deux types d'adresses IP «IPv4 et IPv6».

Le DNS est un protocole qui permet d'associer un nom de domaine (*plus facile à retenir) à* une adresse IP.
C'est la clé de voûte de l'internet !

IPv6 est l'aboutissement des travaux menés au cours des années 1990 pour succéder à IPv4. L'IPv6 dispose d'un espace d'adressage bien plus important qu'IPv4 et compte tenu du développement d'internet, cette quantité d'adresses considérable permettra une plus grande flexibilité dans l'attribution des adresses. Pour le moment, le déploiement d'IPv6 sur Internet est un peu compliqué en raison de l'incompatibilité des adresses IPv4 et IPv6. Pendant une phase de transition où coexistent IPv6 et IPv4, les hôtes disposent d'une *double pile*, c'est-à-dire qu'ils disposent à la fois d'adresses IPv6 et IPv4, et des tunnels permettant de traverser les groupes de routeurs qui ne prennent pas encore en charge IPv6.

La saturation progressive de la quantité d'adresses en IPV4 menace la croissance d'internet. D'ores et déjà l'Amérique du nord est officiellement à sec de nouvelles adresses IPV4…il est temps de déployer l'espace d'adressage l'IPV6.

LE DOMAIN NAME SYSTEM (D.N.S.)

Pour faciliter la recherche d'un site donné sur Internet, **le système de noms de domaine** (DNS) a été inventé. Le DNS permet d'associer un nom compréhensible (la redoute), à une adresse IP. On associe donc une adresse logique, le nom de domaine, à une adresse physique l'adresse IP.

Pour emprunter une analogie au système téléphonique, lorsque vous composez un numéro, le téléphone sonne à un endroit précis, car un plan de numérotation veille à ce que chaque numéro soit unique. C'est bien le numéro unique de votre contact.

Le DNS suit le même principe. Le nom de domaine et l'adresse IP qui le sous-tendent sont uniques. Le DNS permet à votre message d'atteindre son destinataire et non quelqu'un d'autre possédant un nom de domaine similaire. Il vous permet également de taper «*www.nameshield.net*» sans avoir à saisir une longue adresse IP et d'accéder au site Web approprié.

Pour ces opérations ce sont principalement deux types de serveurs qui sont utilisés.
Le Serveur faisant autorité : serveur DNS qui connait le contenu d'un domaine. (Les serveurs de l'AFNIC qui connaissent ce qu'il y a dans .Fr et peuvent répondre).
Résolveur ou serveur récursif : serveur DNS qui ne connait rien mais pose des questions aux serveurs faisant autorité et mémorise les réponses. (Chez le FAI, ou sur le réseau local).

La résolution D.N.S. – Les différents niveaux

Lorsqu'un internaute saisit une adresse dans son navigateur, c'est donc un serveur DNS qui traduit cette adresse humainement compréhensible, en une adresse IP, compréhensible par les ordinateurs et les réseaux. L'adresse www.nameshield.net est ainsi traduite en 81.92.80.11.

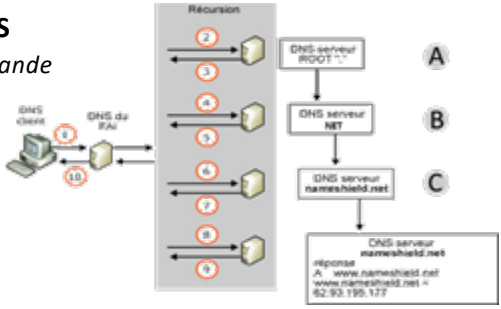
On appelle cela la "**résolution DNS**".

Ce temps est d'autant plus faible que le serveur est performant : CPU (processeur), accès disque, et RAM (mémoire) doivent être correctement dimensionnés.

Le système des serveurs racine répond à plus de 100.000 requêtes par seconde !

Le même principe s'applique pour trouver un site web ou un serveur de messagerie si le nom de domaine comporte un «enregistrement MX» (une adresse email).

Comprendre une requête D.N.S
(Quand l'internaute envoie sa demande de recherche d'un site)



L'architecture logique du DNS est calquée sur la structure hiérarchique des noms de domaine.
Le DNS d'un niveau hiérarchique donné «délègue» au niveau inférieur le soin de traiter le sous-domaine suivant, jusqu'au dernier niveau qui, lui, connait l'adresse IP correspondant au nom de domaine demandé.

Les différents niveaux du D.N.S.

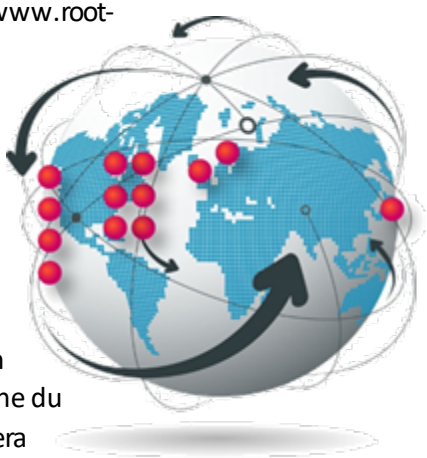
A. **Le niveau le plus haut du DNS est appelé la «racine» («root»).** Au nombre de 13, les serveurs nommés de a.root-servers.net à m.root-servers.net, sont placés sous la responsabilité de l'ICANN. Ils contiennent l'adresse des serveurs DNS et connaissent tous les TLD existants et peuvent donc router la demande de résolution vers le DNS de niveau inférieur traitant le TLD considéré (com, net, org, fr...).
B. **Niveau «TLD»** : Les serveurs DNS de premier niveau sont placés sous la responsabilité du «Registre» gérant le TLD considéré. Il y en a plusieurs par domaine ("com", "net", "fr"...). Ils connaissent l'adresse des serveurs DNS de chacun des sous-niveaux. Ainsi, les serveurs DNS du domaine "com" connaissent l'adresse des serveurs DNS qui gèrent microsoft.com, apple.com.
C. **DNS de second niveau :** Ce DNS est appelé «DNS Autorité» pour ce nom de domaine. Il connaît l'ensemble des noms de domaine relatifs à ce domaine et peut alors fournir l'adresse IP correspondant du nom de domaine. Il est placé sous la responsabilité du Registrant, c'est-à-dire le titulaire du nom de domaine considéré. Celui-ci peut déléguer cette responsabilité en la confiant à un prestataire technique de son choix (un registrar).

L'architecture et le cache

L'ARCHITECTURE D.N.S.

L'architecture physique est très complexe et implique de nombreux prestataires techniques.

Il y a 13 serveurs racine, mais grâce à des fonctionnalités avancées de routage (appelées anycast), plusieurs centaines de serveurs (plus de 500) peuvent se partager une même adresse IP. Il y a donc physiquement des centaines de serveurs qui gèrent la racine, mais "seulement" 13 IP différentes. (Six serveurs sur la côte Est des Etats-Unis, 4 sur la côte Ouest, deux en Europe (au Royaume-Uni et en Suède) et un au Japon (http://www.root-servers.org)



Il y a aussi plusieurs serveurs de premier niveau à chaque fois pour chaque Domaine, et plusieurs serveurs DNS pour un domaine, ce qui permet au système de continuer à fonctionner en cas de panne de l'un d'eux. Il y a donc toujours au moins un serveur DNS principal (primaire) et un serveur secondaire contacté en cas de panne du premier. Si un serveur ne répond pas, il sera toujours possible de contacter d'autres serveurs qui possèdent la même information.

L'architecture de chaque maillon est donc constituée de machines réparties et redondantes, pouvant se secourir mutuellement.

Chaque niveau hiérarchique du DNS doit être architecturé pour respecter une continuité de fonctionnement sans faille car si un maillon du DNS s'arrête, c'est tout une partie de l'Internet qui est injoignable. Mais si la «racine» s'arrête, il n'y a plus d'Internet !
Tout est mis en œuvre pour un fonctionnement optimum et très protégé.

LE MECANISME DE CACHE

Plus on est proche de la racine, plus le nombre de requêtes augmente. Le système distribué permet de gérer cet énorme trafic, mais s'il fallait faire toutes ces opérations à chaque fois qu'un utilisateur lance une requête, cela générerait un trafic important et des temps de requête très longs.

Afin de limiter ce problème, des mécanismes de «cache» ont été introduits pour retrouver rapidement les adresses IP de certains noms de domaine souvent demandés sans avoir à «remonter» jusqu'à la «racine».

Les fournisseurs d'accès à internet (FAI) des internautes fournissent des serveurs DNS. Lorsque votre ordinateur doit résoudre une requête DNS, c'est donc le serveur DNS du FAI qui est contacté. Le serveur DNS du FAI est un serveur intermédiaire. Il garde temporairement en mémoire les dernières résolutions de noms de domaines pour ne pas contacter systématiquement tous les serveurs derrière.
Ainsi, si deux utilisateurs du même FAI demandent à aller sur www.nameshield.net, le serveur DNS ne fera pas ces opérations deux fois. Il donnera immédiatement la réponse qu'il a conservée en cache.

Le système D.N.S.

LE MECANISME DE CACHE

L'architecture DNS mondiale est basée sur un système de cache : lorsqu'un serveur a effectué une première fois une résolution, il la garde en mémoire un certain temps pour pouvoir répondre plus rapidement aux nouvelles requêtes.

La zone DNS est la base de données qui contient l'ensemble des enregistrements pour un nom de domaine. Elle permet de définir les services liés à votre domaine.

La mise en cache sur un serveur DNS peut durer de quelques secondes à plusieurs jours. C'est pour cela que, lorsqu'on change l'adresse IP associée à un nom de domaine, tous les internautes ne voient pas le changement immédiatement. Il faut qu'ils attendent que les serveurs DNS de leur FAI aient mis à jour leur cache pour prendre en compte la nouvelle adresse IP associée au domaine.

Le réglage des TLL (Time to Live) accessibles dans le fichier zone DNS permet de remédier à cet inconvénient. C'est pourquoi pour chaque enregistrement un TTL (Time To Live) est défini. Plus le TTL est bas plus la consultation des serveurs DNS va être élevée. (Pas d'info dans le cache donc j'interroge le serveur suivant ou root).

Le Time To Live est le temps pendant lequel une information doit être gardée en cache.

Un TTL global pour l'ensemble de la zone est également défini. Il est pris en compte si aucun TTL n'est défini au niveau de l'enregistrement. La valeur d'un TTL est défini en secondes (600 secondes sont égales à 10 minutes).

LA ZONE DNS

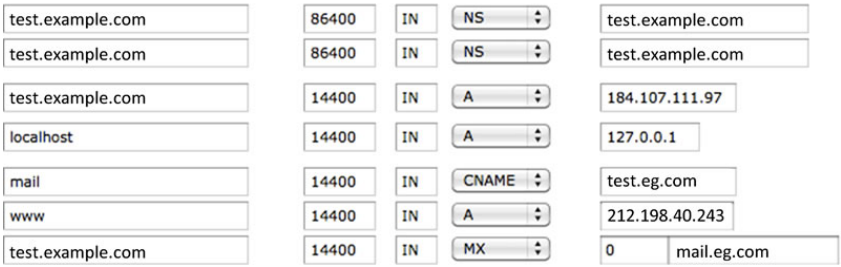
Les connexions sont possibles grâce au protocole DNS. Encore faut-il que la base de données zone qui permet de définir les services liés à votre domaine soit correctement configurée. Les informations contenues dans ce fichier zone vont vous permettre de faire «fonctionner» votre nom de domaine en indiquant l'adresse d'un site, l'adresse email… La configuration de la zone est donc particulièrement importante.

Les fichiers de zones DNS, sont les fichiers de configuration présents sur le serveur DNS contenant toutes les associations "nom de domaine / adresse IP". Ils permettent le fonctionnement du nom de domaine.

Une zone DNS est une base de données contenant des enregistrements, appelés RR (Resource Records). Seules sont concernées par ces informations les personnes responsables de l'administration du domaine, le fonctionnement des serveurs de noms étant totalement transparent pour les utilisateurs.

La lecture d'une zone DNS

Bien que ces informations soient réservées aux administrateurs de noms de domaine, il est intéressant de connaître les différents types de record possibles.



D'une manière générale, un enregistrement DNS comporte les informations suivantes :

Nom de domaine : le nom de domaine doit être un nom FQDN, c'est-à-dire être terminé par un point. Si le point est omis, le nom de domaine est relatif, c'est-à-dire que le nom de domaine principal suffixera le domaine saisi.

TTL : En raison du système de cache permettant au système DNS d'être réparti, les enregistrements de chaque domaine possèdent une durée de vie, appelée TTL (Time To Live), permettant aux serveurs intermédiaires de connaître la date de péremption des informations et ainsi savoir s'il est nécessaire ou non de la revérifier.

Classe : In pour internet.

Les principaux types de record spécifiant le type de ressource décrit par l'enregistrement sont :

A : il s'agit du type de base établissant la correspondance entre un nom canonique et une adresse IP. Par ailleurs il peut exister plusieurs enregistrements A, correspondants aux différentes machines du réseau (serveurs).

AAAA record ou IPv6 address record qui fait correspondre un nom d'hôte à une adresse IPv6 de 128 bits distribués sur seize octets.

CNAME (Canonical Name) : il permet de faire correspondre un alias au nom canonique. Il est particulièrement utile pour fournir des noms alternatifs correspondant aux différents services d'une même machine.

MX (Mail eXchange) : correspond au serveur de gestion du courrier. (Lorsqu'un utilisateur envoie un courrier électronique à une adresse (utilisateur@domaine), le serveur de courrier sortant interroge le serveur de noms ayant autorité sur le domaine afin d'obtenir l'enregistrement MX.)

NS : correspond au serveur de noms ayant autorité sur le domaine.

PTR : un pointeur qui associe une adresse IP à un enregistrement de nom de domaine, aussi dit «reverse» puisque il fait exactement le contraire du A record.

SOA (Start Of Authority) : le champ SOA permet de décrire le serveur de noms ayant autorité sur la zone, l'adresse électronique du contact technique, différentes durées dont celle d'expiration, le numéro de série de la zone.

TXT : permet à un administrateur d'insérer un texte quelconque dans un enregistrement DNS.

(sous-) domaine	TTL	Classe	Type de record	Valeur
domaine ou sous-domaine	"Time To Live" réfère au rafraichissement en seconde de l'entrée	IN veut dire "Internet"	A, MX, TXT, CNAME	nom web, IP ou autre valeur pertinente.

Qui gère Internet ?

Les principaux acteurs

Aucun individu, personne, entreprise, organisation ou gouvernement unique ne dirige internet. Internet est en soi un réseau d'ordinateurs répartis à l'échelle mondiale comprenant de nombreux réseaux autonomes volontairement interconnectés.

Les intervenants travaillent en coopération selon leurs fonctions respectives pour créer des politiques et des normes partagées entretenant ainsi le fonctionnement mondial d'Internet pour le bien public.

En effet, il existe une multitude d'intervenants qui s'occupent d'Internet et interviennent sur des domaines très divers comme :

Politiques et normes (les principes, les normes, les règles, les procédures de prise de décisions et les programmes partagés…). Les normes Internet facilitent le fonctionnement des systèmes entre eux sur internet, en définissant des protocoles, des formats de messages, des schémas et des langues.

Opérations et services : Les opérations d'Internet couvrent tous les aspects matériels, logiciels et infrastructurels requis pour faire fonctionner Internet. Les services couvrent l'éducation, l'accès, la navigation web, le commerce en ligne, les réseaux sociaux, etc. Les parties prenantes sont multiples : la société civile et les utilisateurs internet, le secteur privé, les organisations nationales et internationales, les gouvernements, la recherche, les communautés

académiques et techniques… tous ont leur mot à dire concernant le fonctionnement d'internet …

Outre **l'ICANN**, (Internet Corporation for Assigned Names and Numbers) organisme le plus connu interviennent :

- IANA (Internet Assigned Numbers Authority)
- IAB (Internet Architecture Board),
- IETF (Internet Engineering Task Force), l'IGF (forum sur la gouvernance d'Internet),
- IRTF (Internet Research Task Force),
- ISOC (Internet Society),
- les registres Internet régionaux,
- le W3C (World Wide Web Consortium)

...

Sécurité pour se doter des moyens pour protéger les identifiants uniques d'internet et en empêcher l'utilisation abusive.

Stabilité avec la capacité à garantir que le système fonctionne conformément aux prévisions et à faire en sorte que les utilisateurs des systèmes d'identification uniques lui fassent confiance.

Résilience – capacité du système d'identificateurs uniques à supporter/ tolérer / survivre de manière efficace aux attaques malveillantes et à d'autres éléments perturbateurs sans interrompre ou arrêter le service.

Le rôle de l'ICANN

Internet n'appartient à aucune entreprise ou gouvernement, les américains en assumaient de «manière unilatérale» la gestion technique par l'intermédiaire de l'ICANN. L'organisation internationale de droit californien à but non lucratif a obtenu son indépendance le 1er Octobre 2016.

Créée en 1998, l'ICANN (Internet Corporation for Assigned Names and Numbers) est une organisation internationale de droit californien à but non lucratif, dont le siège social est à San Diego, en Californie.

Le rôle premier de l'ICANN est d'allouer l'espace des adresses de protocole internet, d'attribuer les identificateurs de protocole (IP), de gérer le système de nom de domaine de premier niveau pour les codes génériques (gTLD), d'attribuer les codes nationaux (ccTLD), et d'assurer les fonctions de gestion du système de serveurs racines.

L'Icann coordonne l'opération et l'évolution des serveurs racine du DNS.

L' ICANN décide de l'ouverture de toute nouvelle extension, gère la liste des Top Level Domain (TLD) comme le .com, .net, .org, .fr, .uk…, confie la gestion technique de TLD à un organisme (appelé registre) qui lui-même délègue la gestion commerciale à un registrar.

L'ICANN a en outre pour mission de préserver la stabilité opérationnelle d'internet, de promouvoir la concurrence, d'assurer une représentation globale des communautés internet.

L'ICANN ne contrôle pas le contenu publié sur Internet. Elle ne peut mettre fin au spam et ne gère aucunement l'accès à Internet. Mais de par son rôle de coordination au sein du système d'attribution de noms sur internet, elle exerce une influence non négligeable sur le développement et l'évolution d'Internet.

L'ICANN est donc un organisme stratégique qui dispose d'un pouvoir économique certain, la création de nouvelles extensions permettant de générer de nouvelles richesses et de nouveaux actifs numériques.

La sécurité est au cœur du travail de l'ICANN pour faciliter la coordination technique mondiale des systèmes d'identifiant unique d'Internet.

Le rôle du registre

L'ICANN délègue la gestion aux registres

L'ICANN délivre un droit de délégation sur la vente des noms de domaine à différentes organisations réparties dans différents pays, **les registres**.

Les registres ont pour mission de faciliter la commercialisation des extensions par l'intermédiaire d'un réseau de distributeurs agréés, les **registrars**, également appelés **bureaux d'enregistrement**.

Ce sont eux les registrars accrédités qui attribuent les noms de domaine aux déposants.

Comprendre le fonctionnement entre les acteurs de l'internet : ICANN—Registre—Registrar—Registrant

LE REGISTRE

Un registre ou NIC (Network Information Center) est une entité (association, société, ...) chargée de gérer la base de données qui regroupe des noms de domaine par catégorie, d'un TLD ou des adresses IP pour une région définie.

L'ICANN passe des contrats avec chaque registre. Elle gère également un système d'accréditation pour les registrars.

Le registre de noms de domaines désigne également une base de données contenant des informations sur les sous-domaines (ou domaine de second niveau) d'un domaine de premier niveau.

Exemples de registres de domaines de premier niveau
VeriSign, Inc. : *.com, .net, .name*
Afilias : *.org , .info*
CIRA : *.ca*
DENIC : *.de*
Neulevel : *.biz*
EURid : *.eu*
Nominet : *.uk*
...

Le registre est en charge de :

- la gestion de la base de données de noms de domaine et sous leurs extensions respectives,
- la mise à disposition et l'entretien d'un whois.
- la définition des conditions d'attribution des noms de domaine dans leur(s) zone(s) à charge.

En effet, les registres sont chargés de déterminer les règles et modalités d'attribution qui sont souvent désignées par le terme de charte de nommage. Ces règles varient d'une extension à l'autre en fonction du marché ou d'éventuelles contraintes imposées par les pouvoirs publics. La complexité de ces règles est totalement maîtrisée par les professionnels comme les registrars accrédités par l'ICANN. **L'AFNIC est le registre du .fr** (www.afnic.fr).

Le rôle du registrar

LE REGISTRAR (ou bureau d'enregistrement)

Un **registrar** (terme anglais désignant un bureau d'enregistrement de noms de domaine) est une société privée qui se charge des démarches administratives et techniques d'enregistrement d'un nom de domaine auprès des registres concernés.

Le **registrar** est en contact direct avec le client final. Il joue le rôle d'intermédiaire entre le "Registrant" et le "Registre"; Il est inscrit auprès des divers registres de noms de domaine en fonction des extensions qu'il souhaite commercialiser (il paye pour cela une redevance annuelle).

Les **registrars** qui souhaitent par exemple commercialiser le .fr, s'inscrivent auprès de l'AFNIC.

Un « **Registrar** » **unique** est recommandé pour faciliter la gestion du portefeuille de noms de domaine d'une entité.
Le **registrar** retenu doit être reconnu pour son sérieux et son professionnalisme.
Il doit être **accrédité.**

Chaque fois qu'un nom de domaine est réservé, le registrar reverse au registre responsable de l'extension une somme (en général fixe). Il en va de même à chaque transfert ou renouvellement de nom de domaine.

Chaque registre de noms de domaine a sa propre politique de prix, de conditions, etc. Les registres gérés par le gouvernement des États-Unis, comme **Verisign** pour le .com, obligent leurs registrars à se faire accréditer par l'ICANN et par le registre.

LE ROLE DU REGISTRAR

Le registrar est responsable de la maintenance de la base de données des noms de domaine réservés auprès de lui, ainsi que de la mise à jour de la base de données des registres qu'il représente.

De ces mises à jour dépendent le fonctionnement du système DNS.

Choisir un registrar n'est pas un acte anodin.

Un « Registrar » unique est recommandé pour faciliter la gestion du portefeuille de noms de domaine d'une entité. Le registrar retenu doit être reconnu pour son sérieux et son professionnalisme.

Il doit être accrédité.

Enfin, un registrar peut proposer de nombreux services à ses clients, comme :

- enregistrement du nom de domaine
- hébergement de site sur ses serveurs,
- gestion DNS et configuration technique
- gestion d'adresses électroniques personnalisées,
- gestion de négociation pour l'achat d'un nom de domaine,
- accompagnement dans les procédures UDRP,
- assistance aux démarches administratives,
- etc.

Le choix du registrar sera fonction de vos besoins, du niveau de services recherché et des moyens dont vous disposez.

Les extensions de noms de domaine

Informations générales

A la fin 2013, il existait :

- **22 extensions** dites **génériques** de premier niveau gTLDs *(.com / .org / .net …)*
- **280 extensions pays** ccTLDs

La barre des 326 millions de noms de domaine enregistrés dans le monde a été franchie en mai 2016 soit près de :

127 millions de noms de domaine enregistrés .**com**
16 millions de noms de domaine enregistrés .**net**
16 millions de noms de domaine enregistrés .**de**
5.6 millions de noms de domaine enregistrés .**info**
2,9 millions de noms de domaine en .**fr** enregistrés auprès de l'AFNIC

S'ajoutent depuis 2014 les nouvelles extensions

Un peu plus de 17 millions de noms de domaine déposés dans les newgTLDS comme :

2.7 Millions de noms de domaine enregistrés .**xyz**
2.1 millions de noms de domaine enregistrés .**top**

Les extensions les plus utilisées en France sont le .com (près de 46 % des noms) et le .fr (plus de 32 % des noms)
39,5% des noms de domaine .fr sont déposés par des particuliers.

Les « TOP LEVEL DOMAINS » ou extensions de premier niveau

Les « Top Level Domains » (ou « TLD » ou « extensions ») sont définis par l'IANA (« Internet Assigned Numbers Authority) qui dépend de l'ICANN depuis 1998. (www.internetassignednumbersauthority.org/)

L'ICANN / IANA sont en charge d'allouer l'espace des adresses de protocole Internet (IP), d'attribuer les identificateurs de protocole et de gérer le système de nom de domaine de premier niveau, c'est-à-dire les "Top Level Domains".

Les TLD sont classés en 2 catégories :

- les « gTLD » ou « TLD génériques »
- les « ccTLD » ou « TLD géographiques », « cc » signifiant « country code »),

Et une nouvelle catégorie de générique (gTLD), les nouvelles extensions …

Liste complète des TLD sur : www.iana.org/domains/root/db

Nombre de noms enregistrés

Toutes extensions confondues : 326.000.000
.com et .net : 143.424.000
ccTLDs : 141.700.000

Les génériques gTLDs

(Avant 2014)

Les extensions génériques ou gTLDs
Vous avez le choix entre une vingtaine de TLD génériques.

Les extensions génériques gTLD (genericTLD), composées de 3 lettres ou plus, représentent plutôt un thème, un domaine.

Les gTLDs accessibles à tous

.com pour un site à caractère commercial.
.org pour une organisation à but non lucratif
.net pour une activité sur le Net
.info pour un site d'information

Les gTLDs soumis à des critères d'admissibilité

.biz réservé aux entreprises.
.name pour les personnes physiques / individuels
.pro pour les professions libérales

Les gTLDs limités aux personnes ou entités appartenant à une communauté

.edu (écoles sup ou universités)
.travel (voyage)
.asia (région Asie pacifique)
.museum (musées)
.cat (Catalogne)
.xxx (sites adultes)
.aero (aéronautique)
.jobs (sites offres d'emplois)
.mobi (mobiles)
.coop (coopératives)
.info (site d'information)

Et encore les génériques réservés...

.gov gouvernement des états unis.
.mil organisme militaires des états unis
.int organismes internationaux établis par traités international

C'est le registrar qui est en charge d'informer le registrant sur les critères de validation d'un enregistrement.

Par exemple pour enregistrer un .coop, une entité doit être une coopérative agréée, ou pour le **.aero** il faut être un professionnel, une association du secteur de l'aviation.
Si l'enregistrement dans l'un des gTLD restreints peut s'avérer plus coûteux, en partie en raison des coûts de vérification il apporte une meilleure visibilité et permet de démontrer votre niveau de qualification, votre spécificité. De plus, il est vérifié par une instance officielle.

Un domaine générique « ouvert » n'impose pas de règles aux utilisateurs.

Les extensions country code ccTLDs

Les extensions country code ou ccTLDs

Les extensions de type ccTLD (country code TLD), sont associées à une identification géographique ou pays répertorié par l'ISO (International Standards Organization) qui attribue les codes pays.

Si l'Iana gère l'attribution des ccTLDs, il ne lui appartient pas en revanche de décider si telle ou telle région est un pays ou non, ni de définir les lettres des codes pour représenter un pays donné. L'Iana utilise la liste de code à deux lettres neutre, tenue à jour par l'ISO.

La définition des politiques et des responsabilités juridiques des ccTLDs relève des juridictions nationales et les statuts des registres ccTLD diffèrent selon les pays.

Dans certains pays, les ccTLDs sont liés par un contrat, ou bien par un accord avec un Etat, ou encore selon des mécanismes juridiques et de contrôle, ou enfin, ils sont gérés par les gouvernements. Dans d'autres cas, la relation entre le ccTLD et le gouvernement est très informelle.

Il existe des particularités singulières :

Des domaines qui diffèrent de la norme ISO 3166-1 : .**uk** (royaume uni), .**ac** (ascension), .**eu** (europe), .**tp** (timor oriental), .**yu** (yougoslavie).

Des domaines de complaisance : .**ad** (andorre), .**am** (Arménie), .**fm** (Micronésie), .**cd** (république du Congo), .**nu** (Niue), .**tv** (Tuvalu), .**je** (jersey).

Les domaines de complaisance sont des domaines qui sont utilisés pour des applications commerciales, la plupart du temps en-dehors de leur pays, parce que leur nom a un deuxième sens comme par exemple

le : **.am** (Arménie) et **.fm** (Micronésie) utilisés par des radios AM et FM ; ou **.tv** (Tuvalu) utilisé par des sites en relation avec la télévision et par des sites de vidéos.

Les sLDs, domaine de second niveau

Certaines extensions n'autorisent pas l'enregistrement des noms de domaine directement sous le premier niveau (nom de domaine.tld), mais sous un niveau inférieur (nom de domaine.sld.tld).

C'est par exemple l'Australie (.au) qui a donc choisi de refuser l'enregistrement de noms sous le format company.au et imposent aux entités des sLDs spécifiques (.com.au pour le commerce ou .edu.au pour l'éducation, etc.).

Cette approche tend malgré tout à disparaître. Par exemple, l'extension nationale du Royaume-Uni est maintenant accessible à tous ceux disposants d'une adresse postale au Royaume-Uni.

Quelques ccTLDs

- **.fr** (France)
- **.be** (Belgique)
- **.de** (Allemagne)
- **.it** (Italie)
- **.re** (Ile de la Réunion)
- **.eu** (Europe)*

Le ccTLD « .eu » (Union Européenne) ne correspond pas à un code pays ISO mais est classé dans les ccTLD.

Les IDNs

LES IDN ou Internationalized Domain Name

L'internet est victime de son succès. En moins de 15 ans le nombre d'internautes aura été multiplié par 10, passant de 300 millions d'internautes en 2000 à probablement plus de 3.04 milliards en 2015 soit près de 42% de la population.

Aujourd'hui 57% des internautes n'utilisent pas nativement l'alphabet latin (chinois et japonais, arabe, cyrillique).

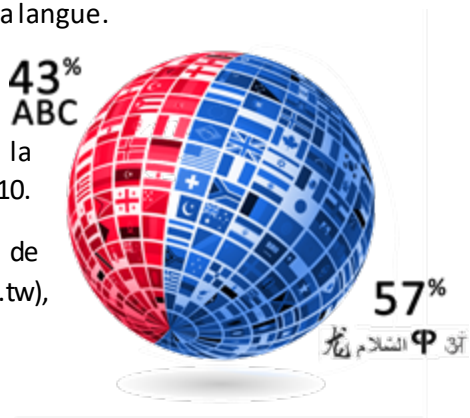
Le multilinguisme est un concept fondamental pour la diversité culturelle et la participation de tous les groupes linguistiques sur internet.

C'était un risque énorme pour l'ICANN de voir émerger une nouvelle norme concurrente.

L'ICANN a donc pris la décision de s'ouvrir à d'autres alphabets. Les IDN sont lancés.

Définition des IDN : Aussi appelé "nom de domaine multilingue", c'est un nom de domaine comportant des caractères autres que des lettres anglophones, des chiffres ou des tirets. Il s'agit de noms de domaine qui peuvent s'écrire avec des caractères différents du Code américain pour l'échange d'information (ASCII) contenant 94 caractères.

Vous pouvez par exemple enregistrer un nom de domaine en IDN avec des accents (éléctricité.fr) ou avec des caractères non latins (россия.рф, l'équivalent en cyrillique, de russie.ru). C'est le pendant technique de la représentation des spécificités culturelles de chaque région du monde sur Internet par la langue.



Exemples : **.рф** (Российская Федерация) est un domaine national de premier niveau pour la Fédération russe, lancé en mai 2010.

台灣 est un domaine national de premier niveau pour Taïwan (.tw), lancé en juillet 2010.

Un préfixe a été choisi en 2003 pour identifier ces noms de domaines internationalisés, il s'agit de « **xn--** ».

L'IDN fait appel à une technologie récente, sans pour autant remplacer l'actuelle infrastructure mondiale du DNS. Pour que le nom de domaine soit résolu sur Internet, c'est donc le système du client qui doit s'adapter pour être compatible **IDN**.

C'est pourquoi, les noms de domaine latin sont transformés suivant un algorithme réversible appelé **Punycode** qui à partir de la version **Unicode** du nom de domaine va produire une version dite ACE ("ASCII Compatible Encoding") ne comportant que des caractères LDH.

Exemple pour **www.caféetthé.fr**

Unicode : www.caféetthé.fr
ACE : www.xn--cafetth-dyae.fr

Les nouvelles extensions

Enjeux et opportunités

Le contexte

Compte-tenu de l'importance croissante de l'Internet dans le monde économique, social et culturel, l'ICANN a lancé une large consultation afin d'introduire de nouveaux gTLDs de premier niveau pour répondre aux demandes pressantes de certaines organisations et groupes représentatifs.

En complément des 22 extensions génériques et des 280 extensions pays existantes, l'ICANN a décidé d'autoriser en 2013 la création de plus de 1300 nouvelles extensions !

Objectif : choix pour le consommateur et compétition pour le secteur des noms de domaine.

Les nouvelles extensions forment trois groupes

1. **Les extensions fermées, pour les entreprises** qui déposent leur propre nom en tant qu'extension. (.nike, .loreal, .audi, …)
2. **Les extensions ouvertes :**
   - Extensions en caractères non latins,
   - Extensions géographiques (.paris, .bzh, etc.) reliées à un lieu, ville ou région,
   - Extensions sectorielles fondées sur des termes génériques qui indiquent un métier, une activité, un service.
     Tous les thèmes sont abordés : Villes, Régions, Alimentation, Finance, Loisirs, Eduction, Santé, Technologie, Religion, Sport…

3. **Les extensions réservées à une cible spécifique** (ex : « .banque, .archi.... »)

Les extensions fermées, pour les entreprises

Les sociétés pourront donc spécifier leur secteur d'activité dans leur adresse web en déposant leur propre nom en tant qu'extension et en s'en réservant l'utilisation exclusive.

Les entreprises seront plus facilement identifiables par leurs clients et prospects, gagneront en termes de visibilité et de communication, sans compter sur la diminution du cybersquatting...

Ils ont candidaté : .ALSTOM, .APPLE, .BNPPARIBAS, .GOOGLE, .MICROSOFT, .MCDONALDS, .INTEL, .TOTAL, .TOYOTA, .BMW, .ORACLE, .AMERICANEXPRESS, .NIKE, .ZARA, .GUCCI, .LOREAL, .AUDI, .AXA, .XEROX, .HERMES, ...

Ces extensions «société» s'adressent avant tout aux marques internationales car le ticket d'entrée pour postuler est de l'ordre de 185 000 dollars au minimum.

Par ailleurs le candidat doit répondre à 50 questions issues d'un guide du candidat (350 pages), choisir un opérateur de registre, apporter des garanties financières, proposer un plan de commercialisation. Une procédure lourde d'environ un an.

Cette possibilité offerte aux entreprises est le plus profond changement depuis la création d'internet !

Les extensions ouvertes :

Extensions en caractères non latins: Malgré les contraintes précédemment exposées, des acteurs comme les organismes internationaux, pourraient être intéressés car il sera possible de demander des extensions en caractères non latins.

Ce type d'extension est bien représenté dans le programme des nouvelles extensions (116) et l'on trouve même dans le premier tour un dossier .catholique en caractères chinois déposé par le Vatican. Pour les utilisateurs d'alphabets chinois, arabes, cyrilliques ou autres, ces nouvelles extensions en caractères non latin sont une excellente nouvelle.

Extensions géographiques reliées à un lieu, ville ou région, (.paris, .bzh, .corsica, .aquitaine, .berlin, .melbourne, ...)

Si ces noms de domaines géographiques sont demandés depuis longtemps, c'est principalement pour donner à une zone géographique une identité numérique qui permet de véhiculer une image de marque.

C'est la possibilité pour une entreprise, d'afficher son attachement ou son origine locale et pour les professionnels du tourisme de disposer d'un formidable outil de communication !

Pour le .paris, la Ville de Paris a souhaité proposer un Programme pionniers afin de promouvoir son TLD.

L'objectif **du programme pionniers** consiste à sélectionner 100 entreprises sur la qualité de leur projet digital et prêtes à utiliser ce nouvel outil pour partager et diffuser, avant les autres, l'esprit d'initiative et d'innovation de la ville de Paris.

Les 100 ambassadeurs du .paris, qui ont porté en avant-première l'extension .paris pendant 6 mois, sont par exemple :

- Citroën pour dsworld.paris,
- Bercy pour BercyArena.paris,
- RATP pour metro.paris,
- Aéroports de Paris pour airports.paris
- …

Le site : http://bienvenue.paris

.PARIS :
Ouverture le 02/12/2014
6000 noms vendus en 2h
7000 noms enregistrés par des particuliers

Les enjeux et opportunités

Quel intérêt de posséder son propre point ? Quelle visibilité pour les entreprises ? Comment protège-t-on les marques ? Quelles sont les opportunités ? Comment s'y retrouver avec tous ces nouveaux territoires numériques ?

Quel intérêt de posséder son .société ?

Concernant le .brand, bon nombre d'entreprises mettent en avant les avantages techniques et sécurité inhérents au fait de gérer sa propre extension. Plus besoin de dépendre de tiers opérant une extension. Avoir sa propre infrastructure Internet basée sur sa propre extension permet d'accélérer les accès et les échanges en interne. Enfin, d'un point de vue marketing c'est un atout de pouvoir communiquer sur son nom.

Quelle visibilité pour les entreprises, pour les marques ?

Avec les new gTLDs c'est tout d'abord davantage de choix, de concurrence, c'est une nouvelle façon de trouver des informations, produits et services, de se repérer sur internet. C'est une nouvelle opportunité de communication pour les entreprises, les marques qui pourront segmenter leur communication et communiquer sur des produits (immo, golf), des services (credit, training) des évènements (events, club, etc.) cette nouvelle approche touche les marques, les activités, les communautés ...

C'est une opportunité pour les marques de renforcer ou créer leur(s) communauté(s).

En effet, les newgTLDs permettent de choisir un nom de domaine plus pertinent, plus précis en offrant un meilleur ciblage des contenus, plus de précision sur des thèmes : géographiques (.paris, .bzh, etc.), sectorielles (.hotel, .immo, etc.), et communautaires (.gay, .catholic, etc.)

Enfin, les **extensions en caractères non latins** (chinois, arabe, hébreux, thaï ...) permettront l'utilisation de l'internet par des communautés non anglophones. Pour les marques, il y a de nouvelles opportunités de business à saisir sur de nouveaux territoires.

Vos objectifs prioritaires doivent être :
visibilité, référencement et protection.

Comment va-t-on surfer demain ? Comment s'y retrouver avec tous ces nouveaux territoires numériques ? Ce sont principalement les moteurs de recherche qui vont s'adapter à ces nouvelles extensions. Certains sont en avance comme Bing, Yahoo, d'autres seront prêts comme Google, qui est l'un des candidats aux nouvelles extensions les plus prolifiques avec une centaine de dossiers déposés à l'ICANN.

Pour les marques, il y a de nouvelles opportunités de business à saisir.

Pour les internautes de nouvelles habitudes à acquérir ...

Classement des 35 nouvelles extensions à MAI 2016.

17 Millions de noms de domaine déposés dans les New gTLDs

Classement	Extension	Nombre de noms de domaine enregistrés en Mai 2016 (*)	Progression % / classement précédent Mars 2016
1	.xyz - (NewgTLD)	2 785 798	5,76
2	.top (NewgTLD)	2 129 379	25,84
3	.wang - (NewgTLD)	1 071 592	0
4	.win (NewgTLD)	911 656	8,97
5	.club - (NewgTLD)	766 628	4,23
6	.link - (NewgTLD)	392 368	15,2
7	.site (NewgTLD)	369 769	11,92
8	.bid - (NewgTLD)	354 835	12,17
9	.science (NewgTLD)	349 918	1,29
10	.xin (NewgTLD)	323 633	113,49
11	.red - (NewgTLD)	308 373	-0,84
12	.ren (NewgTLD)	299 419	2,81
13	.online (NewgTLD)	265 832	29,69
14	.party (NewgTLD)	240 492	3,07
15	.loan (NewgTLD)	237 073	16,64
16	.click (NewgTLD)	236 333	7,56
17	.date (NewgTLD)	187 166	6,17
18	.website - (NewgTLD)	168 407	5,56
19	.space (NewgTLD)	154 479	10,69
20	.kim - (NewgTLD)	125 408	13,58
21	.tech (NewgTLD)	104 788	27,31
22	.work (NewgTLD)	104 280	1,86
23	.lol (NewgTLD)	92 669	1,02
24	.webcam - (NewgTLD)	91 677	3,97
25	.review (NewgTLD)	80 942	13,77
26	.trade - (NewgTLD)	80 057	36,42
27	.nyc - (NewgTLD)	76 706	0,32
28	.realtor (NewgTLD)	74 846	0,42
29	.news (NewgTLD)	74 316	6,19
30	.download (NewgTLD)	67 789	43,35
31	.rocks - (NewgTLD)	66 899	3,13
32	.london - (NewgTLD)	64 337	0,4
33	.guru - (NewgTLD)	63 378	-6,48
34	.berlin - (NewgTLD)	58 709	-1,63
35	.email - (NewgTLD)	57 897	3,24

La Trademark-clearingHouse

La TMCH Trademark-clearinghouse

Si le lancement des 1400 nouvelles extensions offre un plus grand choix d'adresses web aux entreprises et aux marques, c'est aussi pour chaque TLD lancé, autant d'occasions pour les cybersquatteurs d'en profiter, et de risques pour la propriété intellectuelle.

La question de la protection des marques et droits de propriété intellectuelle antérieurs se pose inévitablement. L'ICANN, a donc étudié un mécanisme, une base de données mondiale, afin de protéger les détenteurs de droit des marques existantes, dans le cadre de ce lancement.

Ainsi la TradeMark-ClearingHouse (TMCH) est née.

Il s'agit grâce à la TMCH de permettre aux titulaires de marques d'enregistrer des informations relatives à leur marque dans une base de données centralisée à la condition que la marque soit au préalable enregistrée auprès d'un office d'enregistrement (par exemple INPI en France).

La mise en œuvre de la TMCH a été confiée au tandem IBM pour la gestion technique, et Deloitte pour la gestion juridique.

Infos sur la trademark-clearinghouse : http://www.trademark-clearinghouse.com/content/what-trademark-clearinghouse

Opportunités et risques

La création de plusieurs centaines de nouvelles extensions de premier niveau au cours des prochains mois va induire de nouvelles problématiques pour les détenteurs de marques et en premier lieu pour les sociétés titulaires de larges portefeuilles.

L'apparition de ces nouvelles extensions apporte des enjeux positifs indéniables. Elles devraient permettre notamment :

- d'accroitre la visibilité des marques sous des extensions génériques à fort pouvoir d'attractivité,
- de mieux combattre le cybersquatting par le regroupement des marques sous une même extension-société.

A contrario, l'arrivée massive de plusieurs centaines de nouvelles extensions va :

- accroître la complexité de la protection des marques sur Internet ;
- renchérir inexorablement le coût de protection, tant par les dépôts préventifs que par les procédures de contentieux.

C'est sur ce dernier point que l'ICANN a souhaité s'engager auprès des détenteurs de marques avec la mise en place de la TMCH.

Enregistrer votre marque dans la TMCH c'est bénéficier de l'enregistrement en période de sunrise et d'alertes en cas de dépôts par un tiers.

Les trois promesses de l'ICANN

L'ICANN a souhaité délivrer trois promesses fortes vis-à-vis des détenteurs de marques :

1. **Obtenir une procédure prioritaire d'enregistrement de ses marques dans les 30 jours précédant le lancement d'un new Gtld.**

Avant l'ouverture officielle d'une nouvelle extension, une période de 30 jours appelée Sunrise Period, permettra aux titulaires de marques enregistrées dans la TMCH, d'enregistrer les noms de domaine correspondants sur cette nouvelle extension.

De par l'enregistrement préalable des marques dans la TMCH, des codes d'authentification (Sunrise Codes) permettent au détenteur d'une marque, d'enregistrer un nom de domaine identique au sein de la nouvelle extension.

2. **Etre prévenu de l'enregistrement de noms de domaine par des tiers** et portant éventuellement atteinte aux marques enregistrées dans la TMCH.

Durant la **Claims Period** qui se déroule sur une période de 90 jours avant la phase d'ouverture générale de l'extension, le propriétaire d'une marque est informé si sa dénomination est déposée par un tiers sur cette nouvelle extension.

La personne (tiers) qui dépose un nom protégé, c'est-à-dire une marque préalablement enregistrée dans la TMCH, est informée de ce dépôt préalable et doit certifier qu'elle en prend connaissance et qu'il y a un risque de contentieux ultérieur.

3. **Bénéficier d'un système de résolution des litiges simplifié :** U.R.S. (Uniform Rapid Suspension System) permettant une gestion efficace des conflits avec une procédure de règlement de litige rapide et simple est disponible.

PROCEDURE U.R.S.

Dans le cadre du dépôt par un tiers d'un nom de domaine, faisant l'objet préalable d'une protection par la TMCH, ce n'est pas moins de 5 acteurs distincts qui pourront être impliqués avant l'envoi d'une alerte auprès du détenteur de la marque. Ce dernier sera alors libre d'engager ou non une procédure de règlement rapide de litige (URS).

A noter: après la période de claims seul le titulaire de la marque sera notifié.

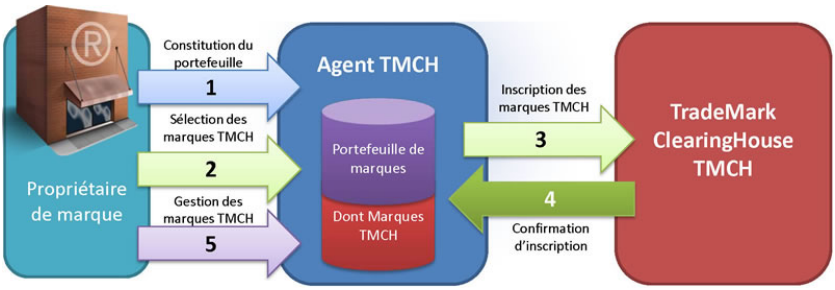
Pour saisir ces opportunités et être le premier à déposer il faut préalablement que vous puissiez indiquer que vous être détenteur d'une marque valide et exploitée, et vous enregistrer dans la **TradeMark-ClearingHouse** (TMCH).

Quelles sont les conditions pour inscrire une marque dans la Clearinghouse ?

La Trademark-ClearingHouse a pour mission première de protéger les marques préalablement et dûment enregistrées auprès des offices, à savoir :

- les marques verbales nationales ou régionales enregistrées auprès d'un office de marques (cf. INPI / OMPI / OHMI /...) ;
- les marques verbales reconnues à la suite d'une décision de justice
- les marques protégées par les lois et traités en vigueur ;
- toutes autres marques constituant un droit de propriété intellectuelle.

Le simple dépôt d'une marque étant insuffisant, l'enregistrement est requis.



Process d'enregistrement d'une marque dans la clearinghouse

N'importe quel détenteur d'une marque commerciale, particulier ou entreprise peut soumettre sa marque à la Clearinghouse en répondant à ces conditions :

- comparaison entre les informations fournies et celles disponibles dans les bases de données des offices.
- pièces justifiant pleinement les droits du détenteur
- preuves d'usage : documents classiquement demandés par les tribunaux dans le cadre des procédures d'opposition fondées sur l'antériorité comme : étiquette, emballage, support publicitaire / marketing (ex : brochure, catalogue, manuel, tract, dépliants, affiche, impression d'écran, présence marketing sur les réseaux sociaux...)

Les marques soumises à la TMCH font l'objet d'une authentification scrupuleuse.

Toutes les informations sur :
http://newgtlds.icann.org/ en/about/trademark-clearinghouse/faqs

Le process de lancement

Le process de lancement des TLD

Les nouvelles extensions sont lancées en plusieurs fois et chaque nouvelle extension a sa propre date de lancement et différentes périodes d'enregistrement permettant à des groupes différents d'enregistrer leur nom de domaine.

La phase de Sunrise

Réservée aux détenteurs de marques, correspond à la phase d'ouverture de l'enregistrement pour une nouvelle extension. Cette phase est commune à toutes les nouvelles extensions et dure en général 60 Jours.

Cette période est exclusivement réservée aux détenteurs de marques enregistrées auprès de la Trademark-Clearinghouse, ce qui leur permet d'enregistrer prioritairement un nom de domaine correspondant à leur marque et ainsi de la protéger.

La phase de Landrush

La phase de Landrush est la première opportunité pour les non-détenteurs de marques d'essayer et d'enregistrer le nom de domaine de leur choix, peu importe les droits relatifs aux marques. Cette phase dure en général 30 jours, les candidats à qui les noms de domaine sont attribués seront désignés et informés à la fin de cette phase.

En cas d'applications similaires, une enchère sera organisée avec les candidats en question.

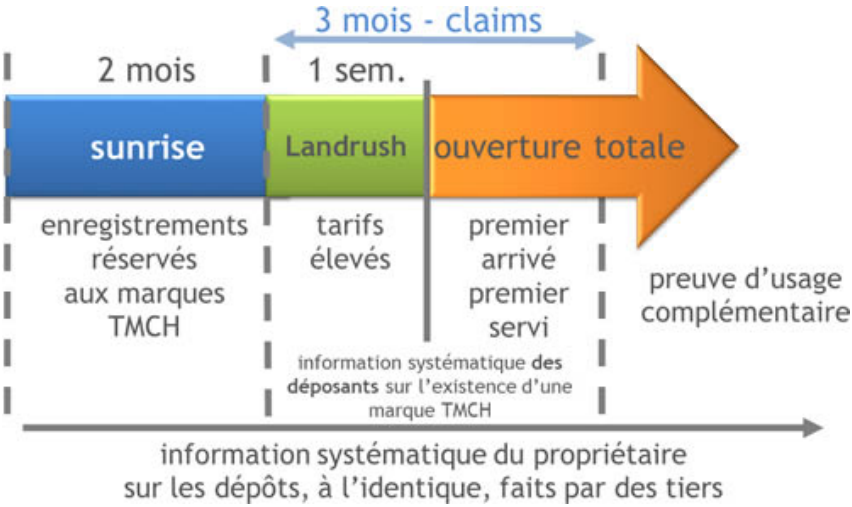
La phase ouverture totale

Après la phase de Landrush, c'est au tour de la phase dite de disponibilité générale de commencer. Cette phase correspond à la période où l'enregistrement est ouvert à tous.

Si l'ouverture totale est ouverte à tous, elle favorise aussi les dépôts de nombreux cybersquatteurs …

Chacun peut enregistrer le nom de domaine qu'il veut, sous réserve qu'il soit disponible. Pendant cette période, les enregistrements de domaine sont attribués sur le principe du premier arrivé-premier servi et en temps réel.

En fonction de votre objectif en termes de visibilité et protection vous choisirez la période correspondante …



La procédure de défense U.R.S.

Comme expliqué précédemment, en prévision des litiges à venir à l'encontre des noms de domaine réservés dans ces nouvelles extensions (cyber-squatteur, typo-squatteur…), l'ICANN a impulsé une nouvelle procédure de résolution des conflits : la procédure URS (Uniform Rapid Suspension / Système Uniforme de Suspension Accélérée).

L'URS ne traite uniquement que les newgTLDs et complète l'UDRP en offrant des coûts plus réduits et en fournissant une aide rapide (21 jours) aux détenteurs de droits en cas d'infractions incontestable. Elle présente toutefois une différence importante.

La procédure URS permet de bloquer (suspendre) l'utilisation d'un nom de domaine, pas de le récupérer pour l'exploiter en retour. Le nom de domaine ne sera pas transférable, on ne pourra pas modifier les DNS, ni le rediriger vers un autre site. Au final il sera bloqué jusqu'à ce qu'il retombe dans le domaine public.

Pour déposer une plainte URS, il faut démontrer les 3 points suivants :

- Le plaignant doit disposer d'une marque enregistrée ou d'un nom commercial identique/similaire au nom de domaine litigieux
- Le titulaire du nom de domaine n'a pas de droit ou d'intérêt légitime.
- Le nom de domaine a été enregistré de mauvaise foi. (La preuve d'enregistrement abusif doit être évidente.)
  La plainte devra être rédigée en anglais exclusivement.

L'inscription de la marque dans la TMCH permet de justifier facilement le droit de marque (fichier SMD) même si cette inscription n'est pas obligatoire pour le recours à l'URS).

Cette procédure a été créée aux fins de satisfaire deux objectifs principaux :

- La célérité d'une part, puisque la procédure URS ne concerne que les atteintes flagrantes aux droits de marque et se caractérise par des délais courts (décision en moins d'un mois),
- l'économie d'autre part, puisque les taxes de l'ICANN ne sont pas être très élevées (Environ 500€)

La procédure U.R.S. permet seulement de bloquer l'utilisation d'un nom de domaine, pas de l'utiliser.

Quel choix entre : URS ou UDRP ?

La procédure URS doit être envisagée uniquement dans le cas où l'on ne souhaite pas utiliser le nom de domaine. S'il s'agit de récupérer un nom de domaine, la procédure UDRP sera pertinente.

Le centre d'arbitrage (National Arbitration Forum) qui a examiné de nombreuses plaintes a rendu dans plus de 85 % des cas, des décisions favorables en faveur du demandeur...

La protection D.P.M.L.

Le programme D.P.M.L.

Certains registres (Donuts, Rightside) ayant en gestion un grand nombre d'extensions proposent une offre de protection nommée D.P.M.L. (Domains Protected Marks List) sur l'ensemble de leur TLDs en gestion.

Les offres DPML ont été introduites pour permettre aux titulaires de marques de les protéger à l'identique ou au contenant, en bloquant les noms de domaine associés dans l'ensemble des nouvelles extensions gérées par ces registres.

Elles protègent à moindre coût (environ 2500€ pour 5 ans chez Donuts et sur la base de la liste complète proposée par le registre) les titulaires de marques contre le cybersquatting, au regard de ce qu'il en serait via des enregistrements défensifs pour chaque nom de domaine …..

Le fonctionnement de la DPML

La marque doit obligatoirement être enregistrée au sein de la TMCH pour être éligible à ces solutions. Une fois inscrite dans une DPML, l'ensemble des noms de domaine reprenant cette marque sera bloqué dans toutes les extensions gérées par le registre. La période initiale de protection est de 5 ans, renouvelable par la suite.

La protection correspond à la marque déposée telle qu'elle est enregistrée dans la TMCH.

Points importants :

Un domaine bloqué par la DPML n'est pas fonctionnel, Il s'agit uniquement d'un blocage pour qu'un tiers ne cybersquatte pas la marque inscrite. L'activation de l'adresse internet n'est pas possible par le titulaire de la marque (il ne peut être utilisé pour créer une URL, une adresse e-mail, un compte FTP…).

Si ce dernier souhaite finalement débloquer un nom de domaine, il devra s'acquitter de frais d'activation d'un peu de moins de 100 dollars par nom de domaine puis payer les frais annuels de l'extension.

A tout moment, une personne ayant une marque identique (et non similaire) pourra outrepasser le blocage de la DPML et demander l'enregistrement du domaine correspondant au terme bloqué.

Les extensions de Donuts : .CAMERA, .CLOTHING, .LIGHTING, .SINGLES, .VOYAGE, .GURU, .HOLDINGS, .EQUIPMENT, .BIKE, .ESTATE, .CONTRACTORS, .PLUMBING, .LAND, .GRAPHICS, .TECHNOLOGY, .GUIDE, .GALLERY, .EMAIL, .CAB, .BUSINESS, .CENTER, .MANAGEMENT, .SYSTEMS, .ACADEMY, .CAREERS, .DIAMONDS, .PHOTOGRAPHY, .DIRECTORY, .TODAY, .KITCHEN...
La liste complète sur http://www.donuts.co/tlds/

Les extensions de Rightside : .ACTOR, .CONSUTLING, .DANCE, .DEMOCRAT, .ENGINEER, .FUTBOL, .HAUS, .IMMOBILIEN, .KAUFEN, .MODA, .NINJA, .PUB, .REPUBLICAN, .REVIEWS, .ROCKS, .SOCIAL, .AIRFORCE, .ARMY, .GIVES, .NAVY, .REHAB.

Les fraudeurs et les attaques

Le cybersquatting

LES OBJECTIFS DES FRAUDEURS

Les fraudeurs les plus prolifiques ne décident pas arbitrairement de déposer un NDD. Leurs pratiques répondent à un comportement adopté délibérément et qu'ils reproduisent dans le but de dégager les meilleurs profits et ce, le plus rapidement possible.

OMPI
ORGANISATION MONDIALE DE LA PROPRIÉTÉ INTELLECTUELLE

La majorité des fraudeurs n'investissent pas dans les dépôts de NDD pour se constituer un patrimoine. Leur objectif est de gagner de l'argent le plus vite possible en misant peu. La violation de marques est une activité commerciale dans laquelle les enjeux juridiques et éthiques représentent un coût relativement dérisoire par rapport aux bénéfices qu'ils peuvent en tirer.

2585 plaintes déposées suivant le principe UDRP en 2013 à l'O.M.PI.

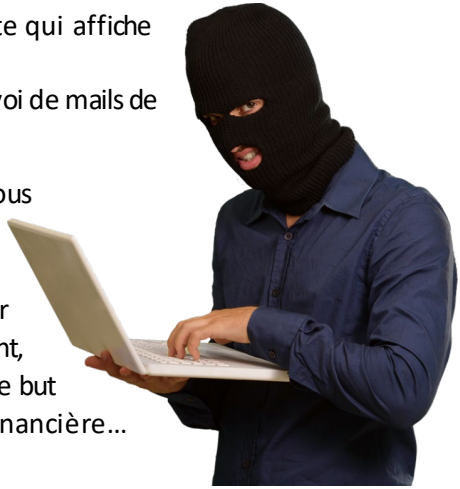
Depuis le lancement des principes UDRP, en décembre 1999, le Centre a été saisi de plus de 25 500 litiges au titre des principes UDRP portant sur quelque 47 000 noms de domaine dans les domaines génériques de premier niveau et les domaines de premier niveau qui sont des codes de pays (gTLD et ccTLD).

Les différentes atteintes aux marques sur internet

Le cybersquatting ou « Cybersquat » en français est une pratique consistant à s'accaparer , en le déposant, un nom de domaine, reprenant ou évoquant une marque, un nom commercial, un patronyme ou tout autre dénomination sur laquelle le déposant n'a aucun droit et ce afin de tirer un profit matériel ou moral de sa notoriété présente ou à venir.

Les objectifs des cybersquatteurs peuvent être différents comme :

- revendre ou marchander le nom de domaine auprès de la marque légitime,
- bloquer l'accès au nom, à la marque,
- nuire à l'image de la marque ou de la société légitime, en associant par exemple au nom de domaine à un site pornographique,
- profiter de la notoriété de la marque pour drainer du trafic sur le site web en utilisant le nom de domaine,
- associer le nom de domaine à un site web frauduleux utilisé pour une attaque en "phishing" ou pour crédibiliser une arnaque diffusée par spam,
- associer le nom de domaine à un site qui affiche des produits de contrefaçon,
- utiliser le nom de domaine pour l'envoi de mails de spam.



Certains cybersquatteurs mettent sous surveillance automatique les noms de domaine de sociétés notoires, en espérant qu'elles oublient de renouveler leur nom de domaine. Ces noms seront, bien entendu, aussitôt redéposés dans le but d'engager une éventuelle négociation financière…

Le typosquatting et slamming

LE TYPOSQUATTING

Forme de cybersquatting consistant à enregistrer un nom de domaine très proche d'un nom de domaine généralement fort connu et qui se fonde sur les fautes de frappes ou d'orthographe commises par les internautes au moment de la recherche permettant ainsi d'aiguiller l'internaute vers un autre site que celui recherché.

Exemples : credit-abricole.fr, creditmuuel.fr, le boncoim.fr, ...

Le typosquatting qui représente près de 15% des litiges emmène souvent l'internaute vers des sites contenant des "liens commissionnés" vers d'autres sites. Si l'internaute clique sur un de ces liens, le propriétaire du site intermédiaire touche une commission du propriétaire du site final.

Plus grave, on commence à constater l'utilisation de noms typosquattés pour aiguiller l'internaute vers un site contenant une page "malicieuse" destinée à infecter son PC avec un "malware".

Le typosquatting, des objectifs variés :

- vendre des bandeaux publicitaires sur la page d'accueil,
- proposer des produits ou services concurrents ou complémentaires à ceux du site d'origine
- renvoyer vers des sites concurrents.

Attention, cette technique permet de détourner, grâce aux fautes d'orthographes ou de frappes, une partie des mails adressés par la clientèle du titulaire du nom de domaine d'origine.

Les effets peuvent être particulièrement graves lorsque le client communique par email des informations confidentielles (banque, santé, assurance..).

LE SLAMMING

Le Slamming, il en existe de deux types:

La fausse facture de renouvellement : cette pratique consiste à envoyer un avis d'expiration du nom de domaine qui est, en réalité, une demande de transfert du nom de domaine vers un autre prestataire.

Si le titulaire du nom de domaine ne vérifie pas et répond positivement à cet avis, son nom de domaine sera transféré au nouveau prestataire.

Autre pratique, **le chantage à l'enregistrement :** une société reçoit un **mail d'un Registrar** l'informant qu'un nom de domaine la concernant ou proche, est sur le point d'être enregistré par un tiers. Le registrar lui propose alors la priorité pour l'enregistrement immédiat du dit nom, moyennant un coût en général plus élevé que la moyenne bien sûr.

C'est, dans la plupart des cas, une arnaque !

Le phishing et la corruption du whois

LE PHISHING

Ne sous estimez jamais les attaques possibles de serveurs et leurs conséquences.

Certainement la technique la plus connue de tous.

La technique du phishing est une technique d'« ingénierie sociale » c'est-à-dire consistant à exploiter non pas une faille informatique, mais la « faille humaine » en dupant les internautes par le biais d'un courrier électronique semblant provenir d'une entreprise de confiance, typiquement une banque ou un site de commerce.

Le mail envoyé par ces pirates usurpe l'identité d'une entreprise (banque, site de commerce électronique, etc.) les invite à se connecter en ligne par le biais d'un lien hypertexte et à mettre à jour des informations les concernant dans un formulaire d'une page web factice, copie conforme du site original, en prétextant par exemple une mise à jour du service, une intervention du support technique, etc.

Les fraudeurs récupèrent ainsi des renseignements personnels tels que : mot de passe, numéro de carte de crédit, date de naissance, etc. C'est une forme d'attaque qui peut se faire par courrier électronique, par des sites web falsifiés ou autres moyens électroniques comme les sms (smishing).

On peut encore citer le dotsquatting (réservation d'un nom de domaine comprenant l'adresse « www » sans le point, accolé directement au nom de la marque), le tldsquatting, etc. Ces atteintes ont toutes le même objectif de détourner le trafic des sites Internet

des titulaires de marques, vers des sites concurrents, via des sites « parking ».

On peut citer également les atteintes aux marques par le **biais des username sur les réseaux sociaux** assimilables au cybersquatting.

Dans le cas le moins grave, le username sera associé à un compte n'ayant aucun rapport avec la marque et l'entreprise, mais il arrive souvent que le compte soit exploité par un contrefacteur usurpant l'identité du titulaire de la marque et mettant tout en œuvre pour créer un risque de confusion !

La corruption d'entrée « Whois »

Un pirate arrive à se faire passer auprès du Registrar pour un des contacts associés au nom de domaine. Il peut alors modifier les informations enregistrées, par exemple l'adresse du serveur « DNS Autorité ». Il déroute ainsi tout le trafic destiné à ce domaine vers un serveur sous son contrôle et peut procéder à toutes sortes de malversations.

La place désormais donnée aux commentaires sur les marques par les consommateurs sur Internet conduit également à des atteintes relatives à l'e-réputation de plus en plus fréquentes. Les critiques négatives reprises en boucle sur les réseaux sociaux peuvent générer un grave préjudice d'image pour la marque.

Le DNS Cache Poisoning et l'attaque DDOS

L'empoisonnement du cache DNS ou pollution de cache DNS est une technique permettant de leurrer les serveurs DNS afin de leur faire croire qu'ils reçoivent une réponse valide à une requête qu'ils effectuent, alors qu'elle est frauduleuse.

Pour mener à bien une attaque par empoisonnement de cache, l'attaquant exploite une vulnérabilité du serveur DNS qui accepte alors des informations incorrectes. Si le serveur ne valide pas les informations reçues et qu'il ne vérifie pas qu'elles proviennent d'une source fiable, alors il stockera dans son cache ces informations erronées. Il les transmettra par la suite aux utilisateurs qui effectuent la requête visée par l'attaque.

Ce type d'attaque permet, par exemple, d'envoyer un utilisateur vers un faux site dont le contenu peut servir à du phishing (Dans le cas du DNS, on parle de pharming) ou comme vecteur de virus et autres applications malveillantes. Un ordinateur présent sur Internet utilise normalement un serveur DNS géré par le fournisseur d'accès. Ce serveur DNS est la plupart du temps limité aux seuls utilisateurs du réseau du fournisseur d'accès et son cache contient une partie des informations rapatriées par le passé. Une attaque par empoisonnement sur un seul serveur DNS du fournisseur d'accès peut affecter l'ensemble de ses utilisateurs, soit directement ou indirectement si des serveurs esclaves s'occupent de propager l'information.

L'attaque par DDOS (Denial of Service ou DoS)

Une attaque par déni de service est une attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser.

Il peut s'agir de :

- l'inondation d'un réseau afin d'empêcher son fonctionnement ;
- la perturbation des connexions entre deux machines, empêchant l'accès à un service particulier ;
- l'obstruction d'accès à un service à une personne en particulier.

L'attaque par déni de service peut ainsi bloquer un serveur de fichiers, rendre impossible l'accès à un serveur web ou empêcher la distribution de courriel dans une entreprise.

Les premières attaques n'étaient perpétrées que par un seul « attaquant » avec des ressources limitées et attirés par l'exploit et la renommée.

Aujourd'hui, avec la forte augmentation du nombre d'échanges commerciaux sur Internet, le nombre de chantages au déni de service a très fortement progressé, des attaques plus évoluées sont apparues, impliquant une multitude de « soldats », aussi appelés « zombies ». On parle alors de DDoS (distributed denial of service attack).

Ces attaques sont en fortes progression et visent les grandes entreprises accompagnées d'une demande de rançon pour arrêter l'attaque.

Les procédures de défense

Comment lutter contre le cybersquatting

Un rappel sur les critères qui définissent la détection de cas de cybersquatting (et typosquatting).

Ma dénomination sociale et/ou ma marque :

- ont été réservées comme nom de domaine par un tiers
- sont repris à l'identique au sein d'un nom de domaine en association avec une autre marque ou un autre terme, souvent dénigrant
- sont reprises avec une modification (une ou deux lettres modifiées) au sein d'un nom de domaine réservé par un tiers (le typosquat)
- un nom de domaine reprenant ma marque est exploité et renvoie sur une page internet vierge ou avec des liens commerciaux (site parking)

La stratégie de récupération

La stratégie de récupération d'un nom de domaine détenu par un tiers dépend essentiellement des droits antérieurs dont vous disposez sur le terme. Ces droits seront indispensables si vous comptez utiliser la procédure UDRP, à savoir

- Identité ou la similarité entre la marque et le nom de domaine
- Absence de droits et d'intérêts légitimes sur le nom de domaine
- Enregistrement ou utilisation de mauvaise foi du nom de domaine

De manière générale il appartient au requérant de prouver qu'il dispose d'un intérêt à agir et que le nom de domaine objet du litige est susceptible de porter atteinte à des droits de propriété intellectuelle ou de la personnalité.

En cas de détection d'un cas de "cybersquatting" ou "typosquatting" plusieurs solutions sont possibles et fonction du dommage stratégique occasionné et du niveau de défense souhaité par l'entreprise.

Si l'URL ne conduit nulle part ou conduit sur un site sans danger, sans risque pour l'entreprise ; il est juste conseillé de mettre en place une surveillance afin de s'assurer qu'aucun changement futur ne rende ce site dangereux pour la marque.

L'url pointe vers un site préjudiciable pour la marque

Si la marque considère que l'URL pointe sur un site, qui lui est préjudiciable, il faut engager une action.

Cette action peut avoir deux objectifs distincts : la non utilisation du nom de domaine par son détenteur, soit sa libération.

Dans ce dernier cas, le nom devenant ainsi libre, il pourra être redéposé ultérieurement. Il faudra donc surveiller et détecter ce nouveau dépôt pour engager une action.

Dans le cas d'une nouvelle extension on n'hésitera pas à user de la procédure URS qui permet de bloquer le nom de domaine, sans toutefois pouvoir l'utiliser.

La procédure UDRP

Le rachat d'un nom de domaine

Cette action de récupération ne peut être engagée qu'en cas de constat d'un "cybersquatting". Si l'entreprise considère que le nom de domaine doit devenir sa propriété, il faut la tenter.

Si le tiers détenteur est de bonne foi, cette approche peut aboutir, bien souvent avec une compensation financière même minime. Il est aussi possible que le tiers ne réponde pas malgré les relances.

La procédure U.D.R.P

Si les actions précédemment citées n'ont pas abouti et que vous remplissez les critères de droit décrits à la rubrique « stratégie de récupération » vous pouvez alors faire appel à un centre d'arbitrage par l'intermédiaire de votre registrar pour déclencher une procédure extra judiciaire dite U.D.R.P. (Uniform Domain-name dispute-Resolution Policy).

La procédure UDRP est simple, se fait par envoi de **documents électroniques, sans plaidoirie et se réalise en cinq étapes**

- dépôt de plainte du requérant,
- présentation des observations du défendeur
- constitution d'une commission d'experts,
- décision, et enfin exécution de cette décision.

Chaque "Registre" peut désigner un centre d'arbitrage devant statuer pour les litiges concernant son TLD. En effet Il existe dans la grande majorité des cas

une procédure de résolution de litige par extension pays. Chaque Registre fixant lui-même sa mise en place.

(Une extension ne bénéficiant pas d'une procédure de résolution de litige doit être considérée comme à risque. Ex: .de (Allemagne) ou .ru (Russie))

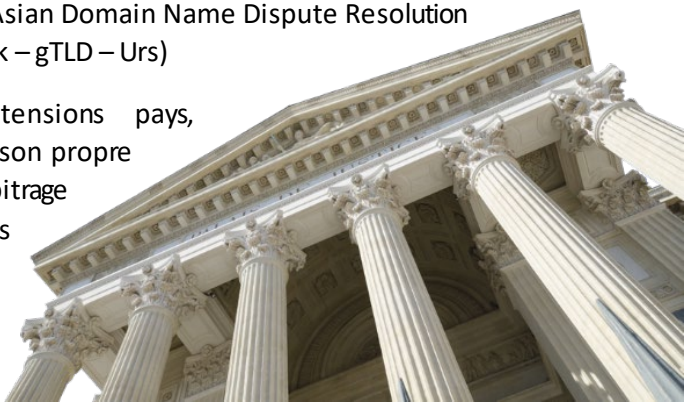
Une procédure simple

Il n'y a qu'un seul échange d'argumentaire et de pièces pour les parties. Aucune audience en personne n'est prévue. Aucun dédommagement n'est possible, si le défendeur condamné ne saisit pas la justice, le registrar exécute automatiquement la décision de transfert ou de radiation du nom de domaine.

Les centres d'arbitrage

- OMPI - WIPO's Arbitration and Mediation Center for the resolution of domain name disputes (CH – gtld)
- NAF (National Arbitration Forum) (us- gTLD – Urs)
- CAC (Czech Arbitration Court) (eu – gTLD -cz)
- AFNIC (.fr domain name registry) (FR)
- ADNDRC (Asian Domain Name Dispute Resolution Center) (Cn – hk – gTLD – Urs)

Pour les extensions pays, chaque pays a son propre centre d'arbitrage avec ses propres règles.



La procédure UDRP et SYRELI

LA PROCEDURE U.D.R.P

Coût d'une procédure UDRP

Le coût d'une procédure UDRP dépend du nombre de domaines sur lesquels porte le litige et du nombre d'experts amenés à rendre un jugement. Avant d'engager une telle procédure, il faut savoir que, comme pour une décision de justice, le résultat n'est jamais acquis d'avance, même si la bonne foi du requérant semble évidente.

89% de noms transférés sur 1843 décisions rendues par l'O.M.P.I en 2013

Une procédure (UDRP) n'exclut pas une action en justice et n'implique aucune renonciation aux droits des parties d'entrer en justice. En effet, le titulaire de la marque, ou le détenteur du nom de domaine, a la possibilité de porter le litige devant les tribunaux, que ce soit avant ou après la procédure extra-judiciaire.

Le recours auprès des Tribunaux.

C'est le dernier recours, à n'utiliser que dans les cas très graves ou en l'absence de procédure UDRP. Il doit être mis en œuvre par des juristes spécialisés. La procédure étant longue et coûteuse, et son résultat étant aléatoire, il faut peser le pour et le contre avant d'engager cette procédure et, là encore, prendre conseil auprès de sociétés spécialisées.

LA PROCEDURE SYRELI pour la France

Cette procédure permet d'obtenir une décision de suppression ou de transmission d'un nom de domaine dans un délai de deux mois à compter du dépôt de la demande. (Le nom de domaine doit avoir été créé ou renouvelé postérieurement au 1er juillet 2011.)

L'AFNIC statue sur chaque demande au vu des seules pièces et écritures déposées par les deux parties, dans le respect du règlement SYRELI, et ne procède à aucune recherche. Cette procédure est exclusivement en français ce qui signifie que toutes les pièces produites devront être traduites et certifiées par un traducteur assermenté.

Cette obligation peut avoir pour les requérants étrangers, des répercussions importantes sur le coût de la procédure qui au contraire se veut abordable et accessible à tous.

Les conditions d'accès sont identiques à la procédure UDRP.

L'Afnic registre du .fr gère également les extensions suivantes :

- .TF est l'extension géographique destinée aux Terres australes et antarctiques françaises
- .RE est un domaine internet de premier niveau désignant l'espace territorial de l'île de la Réunion,
- .WF domaine de premier niveau officiel de Wallis et Futuna, territoire d'outremer français.
- .PM domaine national de premier niveau réservé à Saint-Pierre-et-Miquelon.
- .NC domaine national de premier niveau réservé à la Nouvelle Calédonie
- .YT est l'extension nationale de Mayotte.

Protection : 4 mesures simples et efficaces

LA DOUBLE AUTHENTIFICATION

Cette procédure permet de renforcer la sécurité en proposant aux utilisateurs de se connecter à leur compte (une interface…) en saisissant un code chiffré de validation envoyé sur un téléphone portable en complément de leur nom d'utilisateur et de leur mot de passe.

Cette validation en deux étapes contribue à protéger le compte d'un utilisateur contre les accès non autorisés au cas où un tiers parviendrait à obtenir son mot de passe.

Même si une personne malveillante parvient à dérober votre mot de passe, elle ne pourra se connecter que si elle dispose des informations de validation supplémentaires de l'utilisateur.

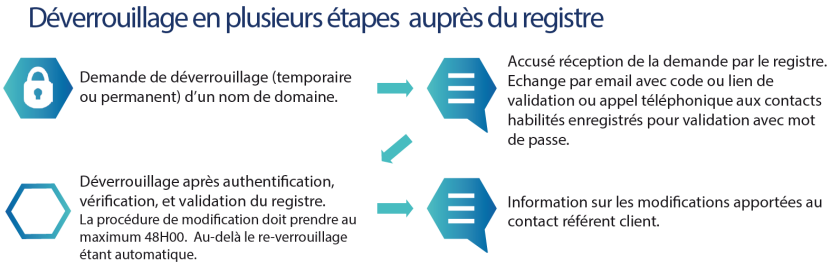
Ces dernières se présentent sous la forme de codes que seul l'utilisateur peut obtenir via son mobile ou via une signature chiffrée contenue dans une clé de sécurité.

Au final si quelqu'un veut se connecter sur votre compte, il faudra qu'il vous vole votre mot de passe ET votre téléphone !

Le registry lock

Les cybercriminels s'attaquent régulièrement aux sites des grandes entreprises et tentent de pirater, de paralyser ou de détourner le trafic des sites web en accédant frauduleusement aux données d'enregistrement du nom de domaine.

Ils peuvent ainsi en modifier les éléments, notamment le site web de résolution du domaine. Les conséquences sont importantes et le préjudice peut s'avérer particulièrement élevé.
Pour faire face à ces attaques, un principe simple et sécurisé existe : le Registry lock.



Ce service permet à un titulaire de nom de domaine d'indiquer au registre qu'il désire le verrouillage des informations relatives à son nom de domaine.
Le déverrouillage est exécuté après une authentification du titulaire appelé « contact authentifié ».
Le Registry lock permet de bloquer un nom sur différentes opérations comme la modification de serveur DNS, la modification de contact, le transfert et la suppression d'un nom de domaine.
Ce mécanisme de sécurité, mis en œuvre pour protéger les noms de domaine, s'exécute par le biais de procédures fortement sécurisées.
Les registres ne proposant pas tous ce service de Registry lock, cette solution peut être proposée au niveau du registrar (Registrar lock).

Le DNS premium

Le DNS (Domain Name System) est l'élément central de la disponibilité de vos services Internet (sites – messagerie – VPN – etc.). La résolution DNS est donc primordiale.

Ce dispositif particulièrement robuste fonctionne sans problèmes majeurs depuis les années 80. Il reste néanmoins vulnérable par certains aspects liés à sa conception et au développement de nouvelles formes d'attaques.

Dans certains cas, les attaques visent les infrastructures proprement dites, donc les serveurs sur lesquels sont installés les noms de domaine. Dans d'autres cas, les agresseurs cherchent à exploiter les possibilités offertes par les logiciels pour créer des situations anormales dont ils espèrent tirer profit.

Les stratégies peuvent être subtiles, mais reposent souvent sur des schémas relativement bien identifiés.

Il est donc indispensable que vos noms de domaine les plus stratégiques soient gérés au minimum avec le DNS Premium, ce qui vous permettra :

- **D'assurer un temps de réponse optimal à vos sites**
  Grâce à notre réseau « Anycast », bénéficiez d'un temps de réponse optimisé de la part des serveurs les plus proches de vos visiteurs.

- **Assurer la disponibilité de vos services Internet**
  Un réseau DNS Anycast assure une disponibilité à 99,999%.

- **Sécuriser vos services Internet**
  Via une plateforme en SaaS dédiée et son système d'authentification par ACL, sécurisez la gestion de vos DNS.

- **Protéger vos sites contre les attaques DDoS**
  Grâce à un filtrage anti DDoS et un réseau Anycast qui assure la disponibilité des sites, même en cas d'attaque.

- **Assurer une fiabilité de structure optimale**
  Grâce à un réseau Anycast puissant et robuste, et des points de présence mondiaux.

Les certificats SSL

Vous avez sécurisé votre nom de domaine avec le Registry lock et vous utilisez le DNS Premium sur votre nom de domaine stratégique qui supporte votre site marchand. Avez-vous pensé aux certificats SSL ?

Un certificat SSL est un fichier de données qui lie une clé cryptographique aux informations d'une organisation. Installé sur un serveur, le certificat active le cadenas et le protocole «https» dans les navigateurs, afin d'assurer une connexion sécurisée entre le serveur web et le navigateur.

Généralement, le SSL est utilisé pour sécuriser les transactions bancaires, le transfert de données et des informations de connexion.

Une connexion sécurisée par SSL offre deux avantages :

- Elle garantit que le serveur est bien celui qu'il prétend être (authentification du propriétaire).
- Elle permet de chiffrer les données pendant leur transit, ce qui permet de se prémunir contre une interception des données "en clair" en cours de route.

Cette solution permet de répondre aux attaques comme le phishing, et permet de garder des données personnelles et/ou bancaires confidentielles lors d'un achat en ligne sur un site de e-commerce.

L'organisation qui souhaite installer le certificat SSL sur son serveur web afin d'initialiser des sessions sécurisées avec les navigateurs devra auparavant se soumettre à une vérification auprès d'une autorité de certification.

Les autorités de certifications

GeoTrust thawte Symantec

Une fois le certificat SSL installé sur un site, une connexion « https » indiquera au serveur qu'il doit établir une connexion sécurisée avec le navigateur.

Lorsque la connexion sécurisée est établie, l'ensemble du trafic entre le serveur et le navigateur sera sécurisé.

Les noms de domaine

La valeur de la marque

LA RELATION MARQUE et NOM DE DOMAINE

Définition: La MARQUE EST UN SIGNE DISTINCTIF apposé sur des produits ou des services par une entreprise et destinée à les distinguer

des produits ou services similaires proposés par une autre entreprise.

Elle a pour fonction de rallier et fidéliser une clientèle aux produits ou services offerts par une entreprise dans un environnement concurrentiel. Pour être protégée la marque doit être enregistrée pour des produits et/ou services précis qui sont répertoriés dans une classification internationale :

- 34 classes de produits
- 11 classes de services

Il est tout à fait possible de déposer une marque à l'identique mais dans une classe de Nice différente. Exemple : Chesterfield (collants / tabac).

Le développement du marché national, européen et international conduit à faire de la marque un instrument majeur de la politique commerciale des entreprises. Économiquement, la marque sert à la

fois à individualiser un produit ou service, à le nommer, mais assure surtout en elle-même une fonction marketing.

La marque est donc un actif de valeur car elle va permettre au consommateur de distinguer et de choisir tel produit ou tel service en raison de l'image qu'il se fait de la marque.

Cependant, si la marque peut devenir l'actif principal d'une entreprise, elle n'en demeure pas moins fragile.

La marque est un bien précieux, un élément indispensable de votre stratégie industrielle et commerciale. Si vous ne la protégez pas, vous offrez à vos concurrents la possibilité de s'en emparer et de bénéficier de vos efforts à bon compte.

Pourquoi dépose-t-on une marque ?

- Pour se créer un droit
- Pour agir en contrefaçon contre les marques identiques /similaires
- Pour agir à l'encontre des cybersquatteurs (plaintes UDRP...)
- Pour accéder à la Trademark-clearingHouse (TMCH)
- Pour étendre sa protection à l'étranger
- Pour enrichir ses actifs immatériels

Où déposer sa marque ?

En France, dépôt auprès de l'INPI
Pour l'union européenne, auprès de l'OHMI
Le système de Madrid est une solution unique pour l'enregistrement et le renouvellement des marques dans le monde entier auprès de l'OMPI.

La valeur de la marque (suite)

Pour être recevable une marque doit être distinctive – licite – disponible

Marque Verbale	Marque figurative	Marque semi figurative
Wanadoo, Twingo, Guy Degrenne, Decaux, Ushuaia, Côte d'Or, ...	Guy Degrenne	Perrier

Une marque distinctive : la marque ne doit pas être générique ni descriptive, c'est-à-dire que l'on ne peut pas déposer un terme qui, dans le langage commun ou professionnel, sert à la désignation du produit et du service en question, par exemple, un vendeur de cuisine ne peut pas déposer comme marque le nom de site www.cuisine.com

Une marque licite : c'est-à-dire que la marque ne doit pas être contraire à l'ordre public et aux bonnes mœurs, la marque ne doit pas tromper le public sur le caractère du produit (ne pas faire croire qu'il s'agit d'un organisme d'état ou officiel) - conditions examinées par l'INPI.

Une marque disponible : au moment où l'on dépose le signe, il faut que le signe déposé ne fasse pas l'objet d'un droit légitime qui appartient à un tiers dans le même secteur d'activité (un nom de domaine libre n'est pas nécessairement une marque disponible et inversement).

Vous devez vérifier la disponibilité de votre marque internet dans toutes les activités et dans les pays concernés.

Cette étape relève de votre responsabilité puisque l'INPI n'est pas habilité à vérifier la disponibilité de votre marque.

Ne prenez pas de risque car si votre marque n'est pas disponible, elle pourra être contestée à tout moment par les propriétaires de ces droits.

Exploitez votre marque

Sachez que si le droit de marque naît du dépôt d'un signe à un office, ce droit ne sera réellement efficace qu'à la condition que le signe soit exploité :

- il convient de faire vivre votre marque,
- de l'apposer sur des produits ou services
- d'en assurer la promotion afin de justifier le monopole résultant du dépôt.

Protégez votre marque

Comme toutes les marques, vous devez faire face, aujourd'hui, à une double problématique :

1. Protéger vos marques, dans le monde physique
2. Protéger vos marques sur Internet

Mettez en place des surveillances et :

- Repérez rapidement les dépôts de marque /réservations de noms de domaine contrefaisants ou les usages litigieux,
- Réagissez rapidement à l'encontre d'un usage contrefaisant par la procédure la mieux adaptée,
- Renouvelez vos marques et noms de domaine en temps utile.

Choisir un nom de domaine

MARQUE ET NOM DE DOMAINE

Le nom de domaine n'est qu'un signifiant textuel de la marque (une adresse électronique), qui fait référence à la présence double de la société sur le marché : son adresse physique et son adresse virtuelle.

Marque et nom de domaine = la synergie

Marques et noms de domaine sont liés ; ils constituent tous les deux des signes distinctifs, ce sont tous les deux des actifs immatériels et ils doivent faire l'objet d'une réflexion conjointe en matière de dépôt et de protection.

Si les marques et les noms de domaine bénéficient chacun de leurs propres règles, ils peuvent interférer souvent les uns avec les autres. Si une marque peut constituer un obstacle juridique (antériorité) à l'enregistrement d'un nom de domaine sachez que l'inverse est également vrai.

La sélection et le choix d'un nom de domaine doivent se faire en amont dans le cadre d'un projet et en parallèle du dépôt de marques.

Posez-vous les bonnes questions avant de déposer un nom de domaine :

- Mon nom de domaine sera-t-il utilisé en tant que site web actif ? Où sera t– il un nom de domaine défensif ?
- Servira-t-il à la gestion des adresses de messagerie ?
- Quel est l'élément qui doit primer dans la communication : le nom ? la marque ? le service? le produit... ?
- Quelles valeurs à associer : quels mots-clés peuvent être intégrés au nom de domaine ?

- Quelle est la cible (public concerné) : internationale, nationale, locale ?
- Quelle extension (gTLD, new gTLD) permet de communiquer sur un service, une activité, un évènement, et permettra le meilleur référencement ?
- Quel choix valider IDN ou ccTLDs ?
- Quelle variantes syntaxiques avec et sans tiret, phonétiques, au pluriel et au singulier…

Voici les règles de dépôts qui vous permettront de choisir votre nom de domaine :

Ce qui est autorisé :

- Les lettres de A à Z
- Les chiffres de 0 à 9
- Les accents
- Les tirets « - » à l'intérieur du nom

Ce qui n'est pas autorisé :

- Les tirets « - » comme premier ou dernier caractère
- Les signes de ponctuation (hors .extension)
- Le signe espace
- Les caractères spéciaux

Choisir son nom de domaine

Lorsque vous recherchez le nom de domaine pour votre site, votre préoccupation doit être de supprimer le plus de sources de confusion possibles pour votre audience.

- Utilisez votre nom de marque pour développer votre notoriété
- Choisssez un nom court, facile à mémoriser, pertinent (éviter les tirets)
- Enregistrez différentes variantes de votre nom de domaine (avec /sans tiret, pluriel, singulier)
- Réservez plusieurs extensions (.fr, .com…) et dans les extensions à risques (.de, .at, .ru, …)

Pourquoi déposer un nom de domaine ?

Pour affirmer son identité sur internet:

- Noms, marques, produits
- Avec des extensions locales, européennes, mondiales, thématiques.

Si vous êtes une société, choisissez le nom de celle-ci, qui vous permettra d'être facilement identifié et mémorisé par vos clients et prospects.
Les adresses mail s'appuient aussi sur les noms de domaine et il est recommandé de n'utiliser qu'un seul nom de domaine de messagerie : le nom de domaine principal de l'entité.

La bonne stratégie de dépôt d'un nom de domaine c'est trouver le bon équilibre entre la visibilité et la protection

Pour anticiper le développement d'une nouvelle stratégie

Stratégie commerciale ou produit, et déposer des noms de domaine et les garder en réserve pour de futures utilisations.

Pour déposer en préventive des noms pour empêcher un tiers de l'utiliser *(cybersquatting, typosquatting)*

Dans ce cas il est conseillé d'enregistrer les noms de domaine proches du vôtre au niveau de l'orthographe (avec ou sans tiret, singulier/pluriel, fautes d'orthographe courantes, etc.), ceci afin

d'éviter le typosquatting et de rediriger les clients qui ne taperaient pas la bonne adresse.
Les variantes possibles à partir d'un nom de domaine officiel sont nombreuses et il est impossible de toutes les prévoir et, à fortiori, de toutes les déposer. Mais il s'agit avant tout de trouver le bon équilibre afin d'en déposer pour capter du trafic, ou pour se prémunir d'attaques futures.

Pour améliorer sa visibilité

- Être en adéquation domaine et contenu
- Pointer systématiquement vers un site pertinent
- Utiliser des emails sur carte de visite

Pour des opérations commerciales, institutionnelles à caractère provisoire (évènement, anniversaire, opération spéciale….), il est fréquent de créer un site web dédié (événementiel) et un nom de domaine officiel à communiquer. C'est une opportunité de communiquer au moindre coût.

Pour capter du trafic

- Optimisation des mots clés et utilisation des extensions
- Double accès domaine et sous domaine

Exemple : www.nameshield.com/blog
Sous domaine : blog.nameshield.com

Pour développer une stratégie de sous domaines

- Expression thématique (voyage...)
- Expression d'activité ou fonctionnalité (blog, boutique...)
- Expression ciblage communauté (vip, intranet...)

L'utilisation de sous-domaines est un moyen simple pour créer plusieurs sites internet appartenant à une même marque. Le sous-domaine ne demande aucune procédure d'enregistrement préalable, juste une simple activation technique pour le rendre disponible sur internet.

Une marque peut créer autant de sous-domaines que de besoin pour ses nouveaux sites :

Par exemple, si Auchan (adresse de site « www.auchan.fr ») veut créer un site dédié à l'automobile, il vaudra mieux lui donner l'adresse « www.autos.auchan.fr » (avec création d'un sous-domaine précédant le domaine « auchan.fr ») que « www. autos-auchan.fr » (ce qui impliquerait l'enregistrement d'un nouveau nom de domaine). Il faudra tout de même se poser la question avec les nouvelles extensions telles que le « .auto » (www.auchan.auto).

L'utilisation de sous-domaines améliore le référencement dans les moteurs de recherche lors des recherches sur la marque contenue dans le nom de domaine principal.

La recherche de disponibilité

Une étape essentielle

Lorsqu'une marque est jugée stratégique elle doit faire l'objet d'un dépôt de marque auprès des offices (INPI pour le France, OHMI, OMPI…). Il est alors recommandé d'enregistrer et de déposer dans le même temps un nom de domaine associé afin de la protéger.

La majorité des noms de domaines étant disponibles sur la base du « premier arrivé, premier servi », comme pour une marque, il vous faut vérifier que le nom de domaine choisi n'existe pas déjà et faire une recherche d'antériorité.

Que permet une recherche d'antériorité ?

Une recherche d'antériorité permet de vérifier à l'instant « T », si une personne ou une société a déjà déposé un nom de domaine qui serait identique ou phonétiquement identique à une de vos marques ou à l'appellation d'un de vos produits.

Vous pouvez vérifier la disponibilité du nom que vous avez choisi sur le site Web du registrar qui vous permettra de rechercher sur plusieurs TLD génériques et codes pays.

https://www.nameshield.net

La notion d'antériorité

Aujourd'hui les noms de domaine sont de véritables signes distinctifs à l'instar des marques

Le conflit entre nom de domaine et marque résulte notamment dans l'absence de lien entre les systèmes d'enregistrement de marque et de nom de domaine. Si la marque est administrée par une autorité publique, le nom de domaine est lui administré par une ONG (ICANN) et bénéficie d'une présence mondiale.

La recherche d'antériorité pour le dépôt de marques et de noms de domaine est donc fondamentale, doit se faire bien en amont des dépôts et ce, afin d'éviter des litiges qui peuvent coûter très cher à l'entreprise en terme financier mais aussi en terme marketing s'il s'agit de produits ou services.

Cette recherche d'antériorités a un double objectif :

- Eviter des litiges avec des tiers qui sont titulaires de ces marques / noms de domaine déjà déposés,
- Eviter de voir des titulaires de ces marques/noms de domaine, profiter (quelque fois involontairement) de la notoriété (visibilité, communication, trafic…) de l'entreprise autour de termes très proches ce qui s'apparente à du typosquatting…

En matière de recherche d'antériorité, prenez conseil auprès de registrars ou de cabinets de propriété intellectuelle

Il existe plusieurs types d'antériorités :

L'antériorité de marque vis-à-vis de nom de domaine

En cas de litige entre le titulaire d'un nom de domaine et celui d'une marque identique, si la marque a été déposée avant le nom de domaine, dans la plupart des cas l'antériorité donnera raison aux titulaires de la marque.

Le titulaire du nom de domaine peut essayer de se défendre et prouver sa bonne foi en cas d'absence de préjudice surtout si la marque a été déposée dans une classe n'ayant aucun rapport avec l'activité de la marque du titulaire.

L'antériorité de noms de domaines vis-à-vis d'autres noms de domaine

Ce type d'antériorité doit être faible si les recherches ont été faites. Cette antériorité est essentielle en amont de projets tels que la création d'un nouveau produit d'un nouveau service d'une société.

L'antériorité de noms de domaine vis-à-vis des marques

Ce peut être le cas pour une marque déposée involontairement ou consciemment (fraudeurs) qui peut porter préjudice à un nom de domaine existant.

Le nom de domaine ayant moins de « droits » que la marque, la restitution de celui-ci ne sera pas automatique surtout si le nom de domaine est exploité de bonne foi, visible et ce depuis plusieurs années. Le titulaire d'un nom domaine peut aussi tout à fait attaquer le déposant d'une marque correspondant au nom de domaine et déposée après lui.

Le choix du registrar

Un registrar est une société accréditée par l'ICANN qui traite votre enregistrement pour le nom de domaine souhaité, si celui-ci est disponible. Pour ce faire, le registrar utilise le registre, c'est-à-dire l'entité qui maintient la base de données qui fait autorité pour le nom de domaine que vous avez sélectionné.

Choisir un registrar n'est pas un acte anodin. N'oubliez pas que le nom de domaine est l'adresse de votre site, de votre boite mail. Il doit être sécurisé. Aujourd'hui, les noms de domaine peuvent être enregistrés auprès de nombreuses sociétés qui sont concurrentes et qui proposent différemment des prix, des services d'expertise, du service client et un environnement sécurisé.

Attention si vous recherchez avant tout « un prix », vous n'aurez probablement pas de service support ou alors un service payant.

Les services

Hébergement, surveillance, solution de messagerie, solution DNS, prestations d'audit et de nommage, prestations juridiques, il peut y avoir beaucoup de prestations annexes à vos noms de domaine. Le choix dépendra de vos besoins en termes de visibilité, de sécurité et sera, au final, fonction de l'importance stratégique de votre portefeuille…

Quelques registrars sont sortis de leur métier de simple technicien de l'enregistrement, pour se tourner vers le conseil. C'est avant tout un accompagnement de proximité pour protéger et valoriser vos actifs

identitaires et une réflexion stratégique conjointe sur la protection et la sécurité des noms de domaine qu'ils proposent aujourd'hui.

La notoriété du registrar

Accréditations, services support, localisation, présence sur le marché, références… autant d'éléments qui doivent vous permettre d'évaluer le professionnalisme du registrar.

La sécurité

La sécurité doit être un élément important dans le choix d'un registrar. Voici quelques recommandations. Choisissez un registrar qui :

- propose un Registry lock, ou verrou de niveau registre, (une authentification des demandes entre le Registrar et le Registre.)
- offre un mécanisme d'authentification journalisée et renforcée, par exemple grâce à deux facteurs d'authentification et un filtrage des accès à l'interface d'administration.
- met en place une procédure de sauvegardes régulière des données contenues dans les zones DNS.

Enfin choisissez un bureau d'enregistrement et un registre soumis à la législation française ou européenne et dont la procédure de règlement des litiges fait référence à une langue et à un système juridique maîtrisé par le titulaire.

Les données WHOIS

C'est un service de recherche fourni par les registres de noms de domaine permettant d'obtenir des informations sur une adresse IP ou un nom de domaine.

Ces informations ont des usages très variés, comme par exemple :

- pour trouver des informations utiles pour résoudre des problèmes de propriété d'un enregistrement comme les dates de création et d'expiration, l'identité du titulaire du nom de domaine...
- pour contacter les gestionnaires Web afin de résoudre des problèmes techniques liés à un nom de domaine.
- pour obtenir l'identité réelle, la localisation et l'information de contact de toute organisation présente en ligne.
- pour contacter le titulaire d'un nom de domaine dans le but de discuter et de négocier une transaction liée au nom de domaine enregistré.
- pour notifier au titulaire d'un nom de domaine qu'il a l'obligation de veiller à l'exactitude de ses informations d'enregistrement.
- ...

LE WHOIS (contraction de l'anglais who is?, signifiant « qui est ? ») est indispensable pour assurer le bon fonctionnement du DNS.

Lors de l'enregistrement d'un nom de domaine, le déposant doit fournir au registrar des informations de contact qui seront associées au nom de domaine (le Whois).

Le WHOIS est un répertoire public et gratuit contenant les informations techniques et de contact des titulaires de noms de domaine enregistrés.

Tous ceux qui souhaitent savoir qui est derrière le nom de domaine d'un site Internet peuvent obtenir ces informations à l'aide de l'annuaire WHOIS.

Les informations sont collectées et mises à disposition par les bureaux d'enregistrement et les opérateurs de registre, conformément aux dispositions prévues dans les contrats conclus avec l'ICANN.

Les titulaires de noms sont tenus de mettre à jour en temps opportun (dans un délai de sept jours suivant tout changement) les données WHOIS d'un nom de domaine enregistré. Le bureau d'enregistrement est à son tour obligé de mettre à jour les données WHOIS dans les plus brefs délais.

Les informations délivrées par un whois

Lorsque l'on effectue une requête Whois, diverses informations concernant le nom de domaine sont fournies, on pourra trouver :

- **Le bureau d'enregistrement – Registrar :**
Organisme qui a enregistré le nom de domaine.
- **Le propriétaire - owner – registrant :**
Personne physique ou morale possédant officiellement le nom de domaine.

En tant que registrant, vous devez fournir à votre registrar des coordonnées précises et fiables, mais aussi rapidement corriger et mettre à jour ces informations le cas échéant, notamment votre nom complet et votre adresse postale, ainsi que le nom, l'adresse postale, l'adresse électronique, le numéro de téléphone et le numéro de fax des contacts techniques et administratifs répertoriés.

- **Le contact administratif - Administrative Contact :**
Personne physique, représentant le propriétaire. le contact administratif a les droits pour modifier tous les paramètres du nom de domaine et en charge de répondre aux questions légales au sujet du domaine.

WHOIS LOOKUP

```
%%
%% This is the AFNIC Whois server.
%%
%% complete date format : DD/MM/YYYY
%% short date format : DD/MM
%% version : FRNIC-2.5
%%
%% Rights restricted by copyright.
%% See http://www.afnic.fr/afnic/web/mentions-legales-whois_en
%%
%% Use '-h' option to obtain more information about this service.
%%
%% [161.58.53.64 REQUEST] >> nameshield.fr
%%
%% RL Net [##########] - RL IP [#########.]
%%

domain: nameshield.fr
status: ACTIVE
hold: NO
holder-c: EM2504-FRNIC
admin-c: JPB660-FRNIC
tech-c: DT1958-FRNIC
zone-c: NFC1-FRNIC
nsl-id: NSL98860-FRNIC
registrar: NAMESHIELD
Expiry Date: 25/03/2016
created: 25/03/2008
last-update: 18/09/2014
source: FRNIC

ns-list: NSL98860-FRNIC
nserver: ns4.perf1.de
nserver: ns1.perf1.com
nserver: ns2.perf1.fr [81.92.87.76 2a01:c8:1:107::76]
nserver: ns3.perf1.eu
nserver: ns5.perf1.asia
source: FRNIC

registrar: NAMESHIELD
type: Isp Option 1
address: 7 rue de Caumartin
address: PARIS
country: FR
phone: +33 2 41 18 28 28
fax-no: +33 2 41 18 28 29
e-mail: registrar@nameshield.net
website: http://www.nameshield.net
anonymous: NO
registered: 01/01/1998
source: FRNIC

nic-hdl: EM2504-FRNIC
type: ORGANIZATION
contact: NAMESHIELD
address: 27, rue des arenes
address: 49100 Angers
country: FR
phone: +33 2 41 18 28 28
e-mail: registrar@nameshield.net
registrar: NAMESHIELD
changed: 19/04/2012 nic@nic.fr
anonymous: NO
obsoleted: NO
eligstatus: ok
eligsource: REGISTRY
eligdate: 19/04/2012 15:40:42
source: FRNIC

nic-hdl: JPB660-FRNIC
type: PERSON
contact: Jean Paul Bechu
address: NAMESHIELD
address: 27, rue des arenes
address: 49100 Angers
country: FR
phone: +33 2 41 18 28 28
fax-no: +33 2 41 18 28 29
e-mail: registrar@nameshield.net
registrar: NAMESHIELD
changed: 15/06/2009 nic@nic.fr
anonymous: NO
obsoleted: NO
source: FRNIC

nic-hdl: DT1958-FRNIC
type: PERSON
contact: Department Technical
address: NAMESHIELD
address: 27, rue des arenes
address: 49100 Angers
country: FR
phone: +33 2 41 18 28 28
fax-no: +33 2 41 18 28 29
e-mail: technical@nameshield.net
registrar: NAMESHIELD
changed: 12/06/2009 nic@nic.fr
anonymous: NO
obsoleted: NO
source: FRNIC
```

- **Le contact technique - Technical Contact :**

Généralement de l'hébergeur du site correspondant au nom de domaine. Le contact technique peut modifier les adresses des serveurs DNS du domaine.

- **Le contact de facturation - Billing contact :**

Personne qui reçoit les factures du registrar et qui doit donc les payer.

- **Les serveurs de nom - Name server - DNS :**

Machines chargées de la conversion domaine->IP. Tous les registrars réclament au minimum 2 serveurs DNS (un primaire et un secondaire).

Le whois est une source d'informations gratuite qui permet de trouver le nom du titulaire d'un nom de domaine... et bien d'autres informations !

- **La date de création - Record created on :**

Il s'agit de la date à laquelle le nom de domaine a été enregistré.

- **La date d'expiration - Record expires on :**

Date jusqu'à laquelle il a été réservé. Elle est mise à jour à chaque renouvellement.

Les opérations sur les noms de domaine

Enregistrement : création d'un nouveau nom de domaine

La durée de validité d'un nom de domaine : La durée de souscription est généralement choisie par le Registrant lors de l'enregistrement du nom de domaine. Elle peut varier de 1 à 10 ans. Un nom de domaine enregistré doit impérativement être renouvelé avant la fin de cette durée. Sinon, il redevient libre et peut être déposé par quelqu'un d'autre.

Changement de délégation : changement de bureau d'enregistrement (registrar). Le titulaire (registrant) du nom de domaine reste identique. Il s'agit simplement d'un transfert de nom de domaine. En général, le client informe son prestataire actuel afin d'obtenir le code d'autorisation (auth info) pour le transfert. C'est le nouveau prestataire qui procédera au changement de bureau d'enregistrement.

Changement de délégation avec transfert de propriété : changement de bureau de registrar avec transmission du nom de domaine au profit d'un nouveau titulaire (registrant)

La transmission volontaire d'un nom de domaine (en cas d'acceptation par les 2 parties.) équivaut à un changement de propriété du nom de domaine. Il peut y avoir transmission d'un nom de domaine en application d'une décision de règlement extrajudiciaire des litiges, ou d'une décision de justice.

Abandon : suppression du nom de domaine auprès du registre. Le nom redeviendra disponible.

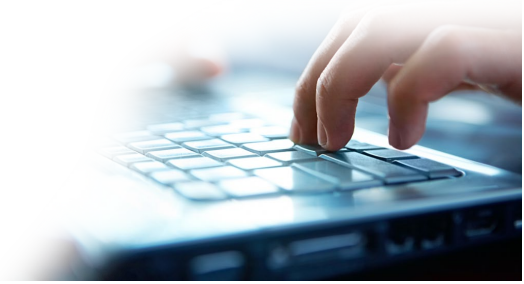
Renouvellement : renouvellement de l'enregistrement du nom de domaine auprès du registrar avec nouvelle date d'échéance

Le non renouvellement d'un nom de domaine avant sa date d'expiration est une cause très fréquente de problèmes. Certains pirates surveillent les retombées des noms de domaine dans le domaine public pour les enregistrer à leur nom. Ils proposent ensuite aux titulaires légitimes de les racheter (cher !) Soyez prévoyant et choisissez un renouvellement automatique……

La migration de portefeuille lors du changement de registrar : migration des noms de domaine en fonction de leur date d'expiration chez le registrar actuel ou migration en masse sur des critères propres au client sans souci de date d'expiration : plutôt telle filiale, tel métier, tel registrar…

Il est impératif de vous renseigner sur la méthode et le process utilisés par le nouveau registrar pour gérer une migration sans risque comme :

- La coupure du site internet ou du service mail si les informations de zone n'ont pas été correctement communiquées, ou modifiées en cours de transfert sans avertissement,
- La perte de nom de domaine en cas de non renouvellement du nom de domaine par le registrar,
- L'échec de la migration (société dissoute, adresse e-mail erronée, procédure non validée, etc.).

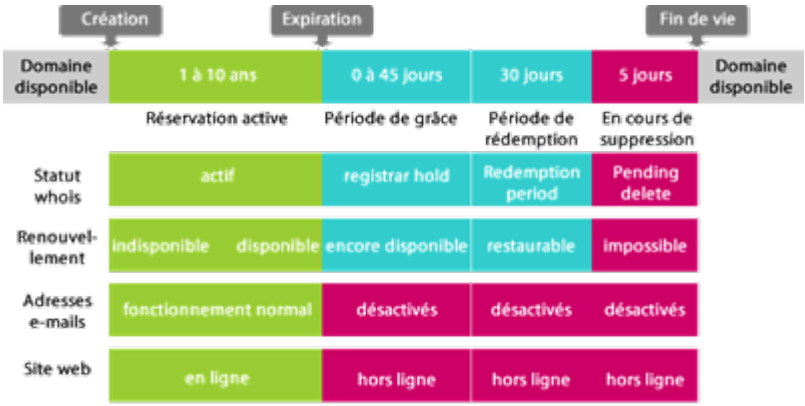


Les étapes de vie d'un nom de domaine

Journée 0 à -45 : période de grâce

Si le nom de domaine a expiré, il se retrouve dans une période de grâce pendant 45 jours. Le haut de la page Web pourrait afficher un message de rappel de renouvellement durant les trois jours suivant la date d'expiration.

Pendant la période de grâce, le nom de domaine est encore considéré comme la propriété du propriétaire actuel et les informations WHOIS continue d'afficher les informations du propriétaire actuel (ou la confidentialité relative au service WHOIS, le cas échéant).



Le domaine est encore disponible au renouvellement par le propriétaire actuel du nom de domaine pendant 40 jours suite à l'expiration du nom de domaine.

Journée -45 à -70 : période de rédemption

Après la période de grâce de 45 jours, si le nom de domaine n'a pas été renouvelé, il sera mis en attente de suppression et finalement abandonné ou vendu aux enchères. Durant cette période, si le nom de domaine n'est pas mis en vente aux enchères (ce qui signifie que personne n'a montré un intérêt dans le domaine), le nom de domaine est encore considéré comme la propriété du propriétaire actuel du nom de domaine. Les informations WHOIS affichent des informations de contact confidentielles.

Les frais de récupération de nom de domaine sont d'environ 120$ et incluent le renouvellement du domaine.

Important : Une fois que le nom de domaine est en attente pour être mis en vente aux enchères, il ne peut pas être racheté par le propriétaire d'origine. Cela signifie que la seule façon de récupérer le nom de domaine est de faire une offre pour le nom de domaine pendant la vente aux enchères.

Journée -70 à -75 : libération du nom de domaine

Après la période de rédemption, si le nom de domaine n'a pas été vendu aux enchères et acquis par une tierce partie, il est libéré et rendu disponible pour un réenregistrement. Quiconque désire enregistrer le nom de domaine devra communiquer directement avec un registrar comme on le fait pour n'importe quel nouveau nom de domaine.

Avant et après les nouvelles extensions

Internet est victime de son succès. Son expansion sans précédent fait surgir de nouvelles opportunités comme de nouvelles menaces. En moins de 15 ans le nombre d'internautes aura été multiplié par 10, passant de 300 millions en 2000 à plus de 3 milliards d'internautes en 2015.

En Octobre 2016 nous comptons plus de 24 millions de noms de domaine enregistrés dans les nouvelles extensions.

Le nom de domaine n'est plus seulement une ressource technique qui permet aux internautes d'accéder aux sites web. L'explosion de l'Internet grand public, puis du commerce électronique, le développement des objets connectés, l'arrivée des nouvelles extensions et la possibilité pour les entreprises de devenir leur propre registre ..., font aujourd'hui du nom de domaine un actif numérique recherché et disputé.

Demain plus encore qu'aujourd'hui, le nom de domaine devra faire l'objet d'une réflexion en matière de choix, d'exploitation optimisée et de sécurité.

Si les marques et les noms de domaine sont aujourd'hui régis par des règles spécifiques, la création de la Trademark-ClearingHouse permet de définir un « nouveau cadre de protection » pour les marques internet. La prolifération de nouvelles extensions apporte un large choix de noms de domaine accompagné de la nécessité de mettre en place des surveillances afin de protéger ses actifs.

Les entreprises vont devoir réagir. Elles qui , bien souvent, ont constitué d'importants portefeuilles de manière empirique, sans véritable stratégie, doivent aujourd'hui prendre conscience qu'il est non seulement important de détenir et d'exploiter des noms de domaine en lien avec la marque, les produits, les services de l'entreprise, mais plus encore que la mise en place de surveillances et de protections efficaces et pérennes dans le temps face à l'afflux massif de dépôts est totalement indispensable.

Dans ce contexte, l'élaboration d'une stratégie de nommage, assortie d'une charte d'organisation entre les différents services (direction, marketing, juridique, technique…) est plus que d'actualité pour toute entreprise qui souhaite se construire une présence sur Internet solide et efficace.

L'arrivée de plus de 1400 nouvelles extensions est certainement le plus profond bouleversement depuis la création des noms de domaine. Gageons que les entreprises sauront profiter de ces nouvelles opportunités et que l'internaute saura modifier ses habitudes de navigation pour s'approprier ce nouvel internet.

L'optimisation de portefeuille

Les objectifs d'une gestion optimisée

Face à aux bouleversements considérables observés sur Internet, les entreprises doivent être en mesure de saisir de nouvelles opportunités, de protéger efficacement leur patrimoine identitaire que sont leurs marques et noms de domaine.

Dans cet environnement aussi concurrentiel, il est primordial que l'entreprise fasse **un état des lieux (audit)** de son portefeuille et définisse ensuite un périmètre de nommage en adéquation avec ses besoins : c'est **la stratégie de nommage**.

Une stratégie de nommage ne se limite pas à des précautions prises a priori. Elle s'envisage sur la continuité et doit évoluer en fonction des nouveaux enjeux (nouvelles extensions, nouveaux produits, nouveaux marchés, ...).

Cette stratégie dépend fondamentalement des besoins et des objectifs de l'entreprise en termes de communication, de développement, et du niveau de protection attendu.

Trois règles s'appliquent dans l'élaboration d'une stratégie de nommage efficace :

- Le responsable de cette étude doit avoir une connaissance parfaite des activités, des services, des métiers, des projets, des marques, des stratégies…de l'entreprise.
- Il doit impliquer l'ensemble des intervenants et parties prenantes (juridique, marketing, informatique, achats…) dans ce projet et autour d'une vision claire des besoins.
- Il ne doit pas travailler qu'à posteriori et définir des règles souples et évolutives afin de pérenniser la méthode.

Les bénéfices obtenus sont nombreux tels que :

- Une stratégie partagée par tous les acteurs de l'entreprise (direction, juridique, marketing…),
- Une forte cohérence et une rationalisation dans la gestion des marques et noms de domaines,

- Une optimisation des dépenses à travers une validation des process,
- Un meilleur équilibre entre la stratégie de visibilité et la stratégie de protection.
- …

La stratégie de nommage facilitera la mise en place d'actions pour **valoriser et sécuriser vos marques** sur votre territoire internet afin de renforcer la visibilité de votre portefeuille et de le **sécuriser** avec des enregistrements défensifs, des enregistrements préventifs, une harmonisation administrative.

L'audit de portefeuille

Objectifs de l'audit / état des lieux est de prendre connaissance de votre portefeuille de marque et noms de domaine dans le détail, d'identifier et de classer les informations pour chaque marque, chaque nom de domaine.

L'audit de votre portefeuille en trois étapes :

Etats des lieux de vos marques

Sur la base de votre portefeuille de marques, identifier :

- Les marques Françaises / Communautaires / Mondiales / US, vous appartenant,
- Les marques appartenant à vos filiales,
- Les déposants et mandataires - Le statut et les dates de renouvellement - Cartographie.

Etat des lieux de vos Noms de domaine et ceux de vos filiales

- Identifier les noms de domaine vous appartenant et appartenant à vos filiales,
- Identifier les noms de domaine attachés à un site web actif,
- Tester les urls associées aux noms de domaine (page blanche, dns, parking,…),
- Identifier les contacts et organismes détenteurs des droits,
- Lister les DNS associés à chaque nom de domaine.

Etat des lieux des noms de domaine appartenant à des tiers (légitimes & illégitimes)

- Lister les noms de domaine déposés contenant vos marques principales ET détenus par des tiers,

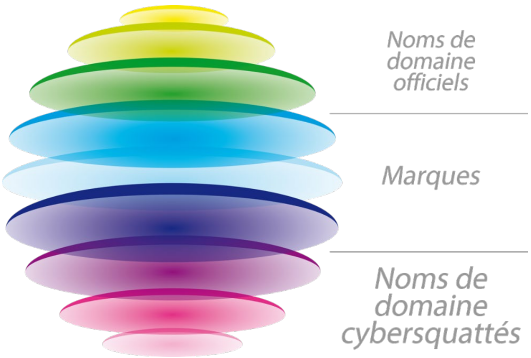
- Fournir les données d'enregistrement (titulaire, contacts administratif et technique),
- Indiquer les DNS utilisés,
- Indiquer la présence éventuelle d'un site actif,
- Fournir la description de la page web,
- Indiquer les dates de dépôt et de renouvellement.

Bénéfices de l'audit

Identification du portefeuille de noms de domaine détenu par catégorie :

- détenus par des partenaires (distributeurs, licenciés),
- détenus par des concurrents,
- détenus par des tiers non autorisés (revendeurs non autorisés, cybersquatteurs, contrefacteurs).

Et l'utilisation qui est faite de ces noms de domaine (parking pub, vente en ligne, blog, page ebay,…)



La stratégie de nommage

La phase d'audit vous permettra une première analyse complète des lacunes de votre portefeuille, de valider les premières pistes pour l'optimisation de votre portefeuille avec des actions de valorisations, des actions correctives, des sources d'économie…et de prendre les premières décisions avec les abandons possibles, les enregistrements défensifs, …..

Vous pouvez donc passer à la phase dite de stratégie de nommage
La stratégie de nommage permet à une entreprise de savoir comment gérer son portefeuille de noms de domaine dans le temps pour déposer, exploiter, conserver et abandonner au bon moment ses noms de domaine.
Seule une approche croisée marques / noms de domaine et une analyse du cybersquatting, permet de définir une stratégie de nommage gagnante.

Une stratégie de nommage en quatre étapes

Etape 1. Phase d'identification et de qualification des besoins de l'entreprise (analyse précise de l'entreprise, de ses activités et compétences et de ses projets de développement)

- **Métiers et secteurs d'activités :** présence entreprise, filiale…
- **Points de présence :** implantation, zone géographique, type de présence (direct, distribution, production, ...)
- **Noms commerciaux, enseignes, marques :** modes de distribution (direct, indirect, …) association avec couverture géographique, phase dans le cycle d'exploitation,

- **Etablissement d'un classement stratégique :** Marques stratégiques, Marques supports, Marques défensives.

A l'issue de cette étape, l'entreprise doit pouvoir aisément identifier quels sont ses marchés stratégiques suivant le croisement de critères tels que Marques / activité / Pays.

Etape 2. Etude des dénominations, termes autour desquels l'entreprise va déposer ses NDD. Cette étude sera réalisée principalement sur les vocables, les extensions et les graphies, sans oublier les nouvelles extensions …

- **Les vocables :** Marques support de communication de l'entreprise, variante vocables, (tirets, accents, fautes d'orthographes…), termes génériques désignant les activités (produits, services…).
- **Les extensions classées** suivant plusieurs critères du type stratégiques spéculatives (lutte contre les cybersquatting, ...)
- **Les graphies** possibilité de déposer un nom de domaine en IDN sous certaines extensions
- **Les nouvelles extensions** et les opportunités pour l'entreprise de communiquer sur les produits les services, les évènements…

La stratégie de nommage *(suite)*

La prochaine étape , certainement la plus importante va vous permettre de définir votre stratégie à un instant T, mais également de mettre en place des règles de nommage vous permettant de faire évoluer votre portefeuille tout en restant cohérent.

Etape 3. Le périmètre de nommage opérationnel

- Noms de domaine stratégiques (utilisés ou à utiliser)
- Liste des noms de domaine en support de communication
- Liste des marchés devant être optimisés (marques actuelles ou futures)
- Liste des marchés avec objectif de protection
- Croisement des dépôts avec les contraintes (langue, présence locale…).
- Abandon des noms de domaine à faible valeur ajoutée
- Cohésion des portefeuilles éclatés, (filiales, distributeurs…)
- Eventuelles procédures à lancer (UDRP, URS, Rachats ...)

Les règles de nommage en perpétuel mouvement, ajouté à cela les nouvelles extensions génériques, le développement des IDN... rendent impossible le risque zéro en matière de cybersquatting.

Deux précautions permettent de limiter les risques :

- L'isolement des noms de domaine stratégiques pour lesquels les enregistrements en termes de communication et de protection seront quasi systématiques
- La mise en place de surveillances automatisées permettant de disposer d'information si un tiers venait à déposer un nom de domaine à l'identique ou proche d'un vocable de l'entreprise.

Les surveillances

Etape 4. La mise en place de surveillances

Il n'est pas nécessaire de surveiller toutes les dénominations. Il faudra donc s'intéresser aux dénominations stratégiques pour mettre en place ces surveillances.

Plusieurs types de surveillance au contenant, à l'approchant d'une dénomination, d'une marque, d'un vocable sur les extensions génériques ou pays sont proposés :

- Surveillance de dépôts de marques
- Surveillance de dépôts de noms de domaine
- Surveillance de contenu
- Surveillance de retombée dans le domaine public
- Surveillance d'une Url

Mettre en place des surveillances permet bien souvent d'éviter des procédures onéreuses.

Indépendamment de l'aspect budgétaire, le choix des surveillances sera fonction du niveau stratégique de votre marque et du niveau de protection attendu.

Il ne vous reste plus qu'à communiquer sur votre stratégie de nommage et les bonnes pratiques (mécanismes et procédures) et à veiller au maintien de la cohérence de votre portefeuille !

Conclusion

La révolution du nommage est lancée avec les nouvelles extensions qui s'ouvrent à un rythme soutenu depuis décembre 2013 dépassant les 3 millions d'enregistrements en Janvier 2014.

Avec le développement de l'internet cette révolution est incontournable et positionne plus encore le nom de domaine comme un actif immatériel. Comme la marque, cet actif doit être exploité et protégé.

Ce défi offre l'opportunité, ou plutôt rend indispensable pour l'entreprise de repenser sa stratégie en matière de gestion de portefeuille de noms de domaine avec pour objectif de le rationaliser, de profiter des nouvelles extensions pour augmenter encore plus sa visibilité sur internet et de mettre en place des solutions de surveillance pertinentes.

Ce document a pour objectif de vous apporter des informations claires, de vous plonger dans les subtilités de la gestion des noms de domaine et de vous permettre de prendre conscience des enjeux internet de demain.

Sachez vous approprier ce nouvel internet !

A propos de Nameshield group

Fondé en 1994, le groupe Nameshield bénéficie aujourd'hui d'une véritable expertise en protection des marques sur Internet ...

Avec plus de 20 ans d'expérience à défendre les marques sur le web, le groupe Nameshield est reconnu comme une véritable référence en matière de gestion de portefeuille de noms de domaine, protection de la marque et gestion des risques sur le web.

Les équipes Nameshield comptent plus de 80 collaborateurs répartis sur 6 pays européens.

Ce qui fait notre différence

- Les clients sont au centre de nos préoccupations et bénéficient d'une haute qualité de service,
- Une large gamme de solutions pour une gestion complète de votre portefeuille : audit, stratégie de nommage, services de surveillance et de protection, etc.
- Professionnalisme, expertise et fiabilité,
- Solutions adaptées aux entreprises, aux revendeurs et aux particuliers.

« J'ai fondé Nameshield il y a plus de 20 ans afin d'aider les propriétaires de marques et les particuliers à construire et protéger leur présence en ligne. Notre activité s'est largement accrue, cependant notre mission reste inchangée. »

Jean-Paul BECHU
Fondateur et dirigeant,
Nameshield group

Nameshield group

27 rue des Arènes - 49100 Angers
37 boulevard des Capucines - 75002 Paris

Tél. +33 2 41 18 28 28
commercial@nameshield.net
www.nameshield.net