5/ DNS, l'annuaire d'internet

Le protocole TCP/IP permet d'associer des noms en langage courant, appelés « adresses symboliques » aux adresses numériques (adresses IP) grâce à un système appelé DNS (Domain Name System). Il traduit les noms de domaines des URL (Uniform ressource locator) en adresses IP ; c'est un composant essentiel au développement des réseaux.

Application :
Utilisez un moteur de recherche pour vous rendre sur le site de la mairie de L'Isle-Jourdain à la page consacrée au lycée.
a- Notez l'adresse qui se trouve dans la barre d'adresse du navigateur web :

Cette adresse peut-être décomposée en trois parties :
- la partie "https" (HyperText Transfert Protocol) sera étudiée dans le module sur le web ;

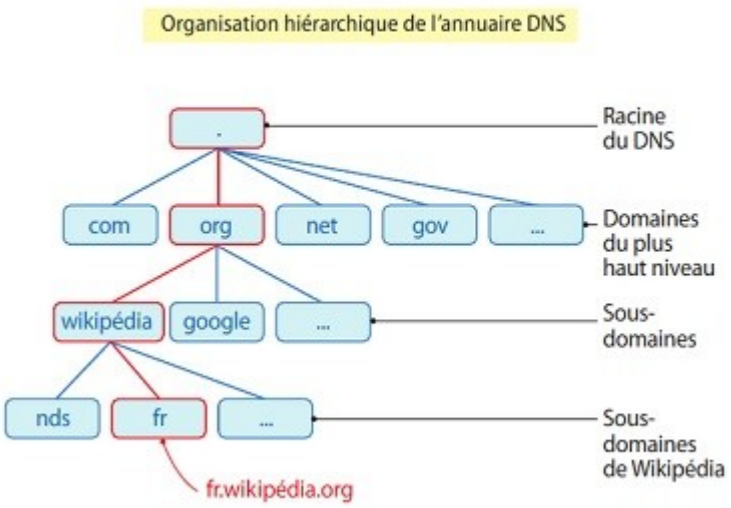
- "mairie-islejourdain.com" est un nom de domaine
  "com" est le premier niveau du nom de domaine
  "mairie-islejourdain" le second niveau du nom de domaine (voir ci-dessous) ;

- la partie "/lycee" désigne l'emplacement de la page HTML "lycee".

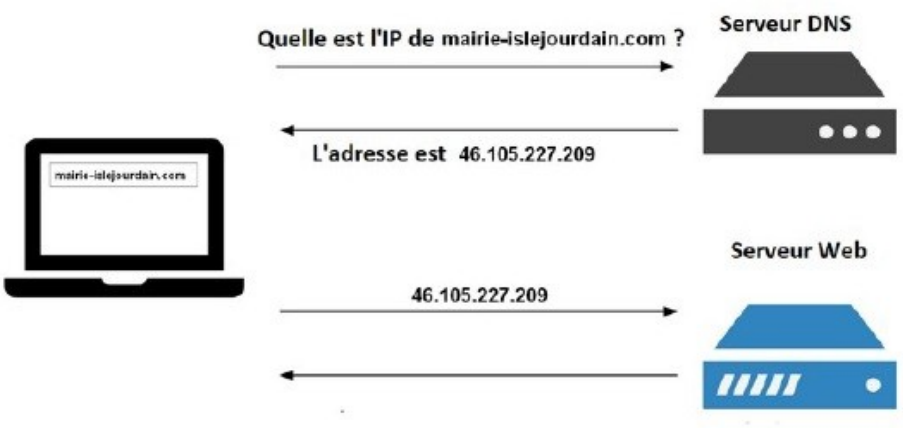
Concrètement, "mairie-islejourdain.com" désigne un serveur sur le réseau, celui sur lequel est installé le site de la mairie. Or, jusqu'à présent nous avons vu que c'est une adresse IP (des chiffres) qui permet de reconnaître une machine sur internet, pas une combinaison de mots.

DOC 1 **L'adresse symbolique, plus facile à retenir**

Pour un être humain, l'adresse IP d'une machine est difficile à retenir. On l'associe donc à une adresse symbolique : un texte compréhensible et facile à mémoriser. La correspondance entre adresse IP et adresse symbolique est enregistrée dans un annuaire, le *Domain Name System* (**DNS**). Il est organisé en **domaines** et sous-domaines, chacun correspondant à des ensembles et sous-ensembles d'adresses gérées en commun. Ainsi dans « wikipédia.org », « wikipédia » est un sous-domaine de « .org ». « wikipédia.org » correspond à l'IP d'une machine.



En utilisant un convertisseur DNS ➔ IP tel que http://domaintoipconverter.com ou http://fr.dns2ip.info/, retrouvez l'adresse IP du serveur "mairie-islejourdain.com" ; notez-la ici :
Le DNS permet de traduire les adresses IP en adresses symboliques et vice versa… est-ce si sûr ? En utilisant le même



convertisseur, **essayer maintenant d'obtenir l'adresse symbolique à partir de l'adresse IP** ; que constate-t-on ?

Entrer l'adresse IP dans le navigateur pour ouvrir la page ; que constate-t-on ?

Quand on envoie une requête pour se connecter au site « https://www.mairie-islejourdain.com/ », le serveur DNS fait le lien entre cette adresse symbolique et l'adresse IP du serveur, comme le schématise la figure.

Faites le test avec les sites ci-dessous :
- conversion,
- puis recherche du site à partir de l'adresse IP dans un navigateur ; est-ce que cela fonctionne à chaque fois ?
- pour les sites de Météo France, les 2 sites (.fr / .com) sont-ils identiques ? quelle(s) différences constatez-vous ?

Adresse symbolique	***Adresse IP***
google.fr	
meteofrance.com	
meteofrance.fr	
mon-ent-occitanie.fr	
lemonde.fr	
wikipedia.fr	

Piratage du DNS :

L'internet est l'un des grands enjeux géostratégiques d'aujourd'hui car il permet de diffuser des informations ciblées par toujours vraies (complotisme, par exemple) ou au contraire un pays peut décider de bloquer certains types d'informations sur son sol. A l'heure de la mondialisation et des câbles optiques sous-marins qui ne connaissent pas les frontières, il faut une parfaite maîtrise de l'outil et de son fonctionnement. Internet constitue aussi un outil de surveillance des citoyens.

En ce qui concerne les serveurs DNS, ce sont des bases de données qui mémorisent la relation entre adresse symbolique et adresse IP. Chaque fournisseur d'accès a ses propres serveurs DNS (ce sont des routeurs) qui sont utilisés par défaut par les ordinateurs des abonnés. Les pirates peuvent exploiter les failles de sécurité de ce système, remplacer un serveur du FAI ou le pirater pour que l'internaute ne soit pas dirigé vers le bon site mais vers un site pirate, copie du vrai site ciblé, qui recueillera des identifiants, des informations « sensibles » (bancaires notamment), pouvant ainsi nuire à l'utilisateur.
Une autre forme de piratage du DNS passe par les virus ou le wifi. Tous les systèmes d'exploitation, y compris sur mobile, incluent une base de données locales qui contient certaines correspondances entre adresses IP et noms de domaines ; cette base de données locales permet notamment aux développeurs de tester localement des outils (ou sites) avant de les mettre en ligne, ou de bloquer l'accès à certains sites. Les pirates peuvent y ajouter un virus qui dirigera l'utilisateur vers un faux site, ou un cheval de Troie (téléchargé naïvement ou à son insu par l'utilisateur) qui prendra le contrôle de tout ou partie de l'appareil, créera des failles de sécurité, espionnera l'activité de l'utilisateur et récupérera des informations confidentielles.
Les serveurs DNS utilisés par défaut par les appareils de l'internaute sont ceux fournis avec la connexion internet (par le FAI). Certains pirates optent donc pour une technique très simple : ils proposent un accès wifi gratuit qui leur évite de recourir à des failles de sécurité ou à des virus. Il leur suffit de créer leurs propres serveurs DNS pour cette connexion, qui renvoient vers leurs faux sites.

Se protéger :

Si on est obligé d'utiliser le wifi public, il est fortement recommandé d'obtenir un VPN (réseau privé virtuel) où le terme « virtuel » concerne la méthode de connexion utilisée pour protéger le trafic et les données web privées lors de la connexion à internet. Cet petit utilitaire cache l'adresse IP de l'appareil et empêche l'espionnage.

Les spécialistes de la sécurité conseillent de vérifier régulièrement le nom de domaine du site et la présence du petit cadenas vert à gauche de l'URL du site sur le navigateur pour être certain que la connexion est sécurisée, avant d'entrer ses identifiants. Cela fonctionne contre l'hameçonnage, mais se révèle inutile contre le piratage DNS. En effet, l'adresse du site correspond bien, puisqu'elle a été détournée, et les criminels ayant pris le contrôle du nom de domaine peuvent recréer des certificats de sécurité.

Il est aussi possible de changer le mot de passe administratif (qui donne accès aux paramètres) de son propre routeur, et de mettre régulièrement à jour son routeur.

Recommandations de l'ICANN :
Dans un communiqué de presse publié vendredi 22 février 2019, l'Icann (Internet Corporation for Assigned Names and Numbers) invite les registrars du monde entier à mieux sécuriser le système d'adressage DNS en ayant recours au DNSSEC (l'extension de sécurité idoine). L'organisme nord-américain de gestion des noms de domaine (qu'on présente aussi souvent comme l'annuaire central d'Internet) souhaite ainsi encourager les gestionnaires de DNS à ne pas passer outre cette étape importante qui permet de mieux sécuriser l'infrastructure du web.

En résumé, utiliser un serveur DNS alternatif permet d'éviter le piratage via une connexion wifi. Utiliser un bon logiciel antivirus à jour devrait éviter le piratage par un virus. Si la présentation d'un site web semble suspecte, vérifiez sur les réseaux sociaux si d'autres utilisateurs rencontrent des problèmes. Une recherche sur Twitter permet souvent de voir le problème avant même que les propriétaires des sites ne s'en rendent compte.

Sources :
https://www.futura-sciences.com/tech/questions-reponses/securite-video-tout-ce-vous-devez-savoir-piratage-dns-10938/
https://www.avg.com/fr/signal/what-is-dns-hijacking
https://www.lesnumeriques.com/vie-du-net/non-icann-a-pas-ete-pirate-mais-encourage-usage-dnssec-n84309.html