



CASES articles

Le World Wide Web – son fonctionnement repose sur les adresses Internet

Les noms de domaine - tout le monde les utilise, mais de quoi s'agit-il ?

Pour plus de sécurité, adoptez les réflexes CASES !

Les noms de domaine sont également ciblés par les pirates

Ebay.com, facebook.com ou amazon.com – des millions d'utilisateurs d'Internet les connaissent : ces noms de domaine permettent l'accès au site d'enchères en ligne Ebay, au portail social Facebook et au site de vente en ligne Amazon. Les noms de domaine ont été créés afin de faciliter la navigation des utilisateurs, mais de nombreuses questions restent en suspens concernant leurs fonctions. Ainsi la différence entre .com et .net n'est pas souvent faite. Pourtant, une connaissance plus approfondie du système d'adressage permet de mieux comprendre l'Internet. Certaines formes d'attaque seraient ainsi plus facilement détectables par l'utilisateur.

Avant la création des noms de domaine, les utilisateurs ne voyaient que l'adresse réelle d'une page Internet, c'est-à-dire une suite de chiffres. Il est indéniable que l'adresse <http://194.154.200.74> est nettement plus difficile à mémoriser que le nom de domaine correspondant : <http://www.etat.lu>.

Chaque ordinateur relié à l'Internet peut être identifié à l'aide d'une longue suite de chiffres. Ces chiffres n'étant toutefois pas faciles à mémoriser, un nom commun a été introduit : le nom de domaine. Un nom de domaine aisément mémorisable peut donc désormais être attribué à chaque suite de chiffres.

Tout comme les marques ou les logos, les noms de domaine revêtent une importance stratégique et exercent, pour de nombreuses sociétés, un effet sur la concurrence. Ils sont donc souvent dotés d'une grande



valeur marchande et peuvent également devenir la cible des cybercriminels.

En jargon spécialisé, l'adresse Internet est dénommée URL (ou Uniform Resource Locator) et rend possible l'accès à des pages Internet. La structure de ces adresses sera décrite à l'aide de l'exemple : <http://www.cases.lu/de/publications/dossiers/index.html>.

Structure d'une adresse Internet

L'adresse Internet est composée de plusieurs parties : le protocole, le nom de l'ordinateur, le nom d'hôte, le domaine de premier niveau (ou top level domain) et le lieu de stockage.

Le protocole

« http » désigne le langage de communication. Il s'agit d'un protocole

établissant précisément les règles de communication sur Internet. La plupart des internautes utilisent l'« HyperText Transfer Protocol », ou http, pour accéder aux pages web. C'est ce protocole qui est utilisé dans notre exemple.

D'autres protocoles, tout aussi importants, sont également employés, par exemple en liaison avec des serveurs de fichiers. Un serveur de fichiers a pour vocation de mettre à disposition de l'espace de stockage pour de grandes quantités de données. Les données sont en outre accessibles à plusieurs utilisateurs et peuvent être téléchargées. Le protocole de communication alors utilisé est le protocole « ftp » ou « File Transfer Protocol ». Dans notre exemple d'une adresse Internet, la dénomination du protocole « http » serait ainsi remplacée par « ftp ». Chaque protocole met en œuvre des méthodes spécifiques pour la communication et l'adressage de ressources.

Le nom d'hôte

Le nom d'hôte constitue la partie principale d'une adresse Internet. Dans notre exemple, www.cases.lu constitue le nom d'hôte. Ce nom d'hôte est composé de trois éléments :

« www » représente le nom de l'ordinateur, lequel dépend habituellement du service mis à disposition par le serveur. Dans notre exemple, il s'agit ainsi d'un serveur web. Dans le jargon spécialisé, cet élément est également appelé sous-domaine ou « subdomain ».

Le nom de domaine « cases » constitue l'élément principal de l'adresse. Il se rapporte généralement à l'organisation à laquelle appartient la page Internet. Le nom de domaine peut être composé de lettres, de chiffres et de caractères spéciaux, comme le trait d'union par exemple. Le nombre de combinaisons possibles pour un nom de domaine est par conséquent gigantesque.

« lu » représente le domaine de premier niveau ou top level domain (TLD). Il y a deux sortes de domaines de premier niveau : ceux qui permettent une différenciation par pays, et ceux qui permettent une différenciation par service ou branche d'activité. Dans notre exemple « lu » correspond au Grand-duché de Luxembourg.

Le lieu de stockage de la ressource souhaitée

L'élément

« /de/publications/dossiers/index.html » indique le lieu de stockage de la ressource souhaitée. Le signe « / » permet de décrire l'arborescence des répertoires successifs menant à un fichier spécifique, par exemple un texte.

Attaques sur les noms de domaine

Le nom de domaine est un outil important lorsqu'il s'agit d'obtenir l'accès à des informations sur Internet. Vu le nombre très important d'utilisateurs, l'Internet est devenu un marché inté-

Comment l'archipel de Tuvalu gagne de l'argent

De nombreuses organisations considèrent leur nom de domaine comme une marque. Elles sont donc très créatives lorsqu'il s'agit de créer leur adresse Internet. Le domaine de premier niveau .tv est par exemple très volontiers utilisé par les chaînes de télévision. L'introduction de ce top level domain par Tuvalu s'est ainsi révélé être une nouvelle source de revenus très lucrative pour cet archipel du Pacifique, et les noms de domaines .tv se vendent à prix d'or. Un autre domaine de premier niveau s'est révélé très lucratif : il s'agit de « .fm », qui intéresse en particulier les stations de radio. Celui-ci est attribué par les États fédérés de Micronésie. Le site <http://data.iana.org/TLD/tlds-alpha-by-domain.txt> permet de consulter tous les top level domains actuels.

Conseil CASES : enregistrement d'un nom de domaine

Conformément aux dispositions régissant l'attribution des noms de domaine, ceux-ci doivent être déposés auprès d'un bureau d'enregistrement officiel. Seul ce dernier est habilité à réserver et à vendre des noms de domaine. La page Internet <http://www.internic.net/index.html> propose une liste des bureaux d'enregistrement officiels répertoriés.

La disponibilité d'un nom de domaine ainsi que les droits annuels à acquitter peuvent être vérifiés auprès de l'un de ces bureaux d'enregistrement. Si le nom de domaine est disponible, il est possible de déterminer la période de réservation de celui-ci. Pour l'enregistrement, diverses données (en fonction du pays) telles que le nom, l'adresse postale et une adresse e-mail sont requises. Dans le cadre de cette procédure, l'identité de la personne physique procédant à l'enregistrement du nom de domaine est déterminée, le but étant de limiter la marge de manœuvre des cybercriminels concernant l'utilisation abusive des noms de domaine.

Dès que le nom de domaine est attribué, les informations relatives au propriétaire de celui-ci peuvent être consultées dans une base de données.

Les procédures utilisées par un bureau d'enregistrement devraient être examinées avant le dépôt d'une demande auprès de celui-ci. Celles-ci peuvent en effet varier en fonction du bureau d'enregistrement et du pays d'établissement de celui-ci. Il convient de préciser que les pays dont les bureaux d'enregistrement appliquent une procédure de vérification d'identité stricte ou qui émettent des prescriptions tout aussi strictes lorsqu'il s'agit de modifier un nom de domaine sont bien moins touchés par l'utilisation abusive des noms de domaine par des cybercriminels.

Définition : protocole

Un protocole établit des règles précises de communication sur Internet. L'« HyperText Transfer Protocol » ou http est, par exemple, très souvent utilisé pour accéder à des pages web.

Définition : serveur

Le serveur est un programme communiquant avec d'autres programmes. Sa vocation est de permettre à ces autres programmes d'accéder à des services spécifiques.

ressant pour les cybercriminels. Les pirates attirent par exemple leurs victimes sur des pages Internet contrefaites. Les méthodes permettant ce genre de détournement sont nombreuses.

Ce détournement se fait souvent à l'insu de l'utilisateur ou grâce à la manipulation du domaine de premier niveau décrit précédemment. Afin de se protéger de cette forme d'attaque en tant qu'utilisateur d'Internet, il

convient de connaître la méthode employée.

L'enregistrement d'un nom de domaine se fait selon le principe du « premier arrivé, premier servi ». Une forme d'attaque dénommée « cybersquatting » consiste à enregistrer un nom de domaine en premier, à condition que celui-ci puisse être assimilé à une société connue, une tendance actuelle ou tout autre événement d'actualité. Les cybersquatteurs espèrent ainsi se procurer des noms de domaine dont la valeur connaîtra une forte hausse à échéance assez brève. Lorsqu'une entreprise constate que le nom de domaine qu'elle souhaite déposer est déjà enregistré, elle sera peut-être prête à payer une forte somme d'argent pour l'obtenir. Le cybersquatteur est ensuite bien sûr tout disposé à céder le nom de domaine correspondant contre une importante rétribution.

Le cybersquatting, une pratique courante en particulier au cours du boom de l'Internet pendant les années 90, est désormais puni par la loi et les cybersquatteurs doivent souvent céder les noms de domaine ainsi déposés.

La durée d'enregistrement d'un nom de domaine étant limitée dans le temps, les cybersquatteurs sont toujours à l'affût de délais arrivés à échéance et enregistrent tout nom de domaine qui n'est plus protégé. Les cybersquatteurs sont également immédiatement sur les rangs lorsque de nouveaux domaines de premier niveau sont introduits. Ainsi, lors de l'introduction du top level domain « .mobi », de nombreuses entreprises renommées sont arrivées trop tard.

Le « typosquatting » est une autre forme d'attaque reposant sur les erreurs de frappe que pourrait faire un utilisateur lorsqu'il saisit une adresse Internet ou sur l'introduction d'un nom de domaine erroné. Les typosquatteurs enregistrent les noms de domaine ne se différenciant que très peu des noms connus. Ils tablent par exemple sur les erreurs de frappe générées par la proximité des touches sur le clavier. Une autre approche consiste à utiliser les ressemblances phonétiques de certains noms, les typosquatteurs espérant alors exploiter les éventuelles erreurs des utilisateurs d'Internet.

Ce sont souvent les sites pornographiques ou encore les casinos en ligne qui utilisent le typosquatting. Ils tentent ainsi d'attirer des clients sur leurs pages. Il n'est d'ailleurs pas rare de voir le concurrent direct d'une entreprise essayer de détourner les clients de celle-ci sur son propre site. Dans certains cas, le typosquatting peut également être qualifié d'enregistrement abusif d'un nom de domaine. Il est alors, tout comme le cybersquatting, passible de poursuites judiciaires.

Une forme modifiée du typosquatting consiste à enregistrer des noms de domaine ressemblant à ceux d'organisations dignes de confiance. Les cybercriminels utilisent cette méthode par exemple afin d'obtenir les mots de passe ou les données bancaires des utilisateurs.

Il est recommandé aux utilisateurs d'Internet de vérifier le nom de domaine après sa saisie. Si l'utilisateur remarque quelque chose de suspect ou d'inhabituel sur une page Internet, il convient toujours de vérifier l'orthographe du nom de domaine dans la barre d'adresse du navigateur.

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

www.cases.lu