



## Détournement de nom

Pour plus de sécurité, adoptez les réflexes CASES !

Quand les utilisateurs d'Internet sont induits en erreur ou victimes

Qu'ont en commun Julia Roberts, Scarlett Johansson, Sting, Google et Microsoft ? Leur nom a été usurpé par des cybercriminels. Mauvaise nouvelle : personne n'est à l'abri. Même les internautes luxembourgeois, qu'ils soient particuliers ou entreprises. Bonne nouvelle : il est possible de se protéger.

Julia Roberts n'en a pas cru ses yeux : le site Internet juliaroberts.com est tombé entre les mains de cybercriminels. Ils ont utilisé le nom de domaine et la notoriété de l'actrice pour détourner des internautes crédules vers un site douteux et gagner de l'argent.

La vedette de « Pretty Woman » n'est pas la première personnalité à être victime de cybersquatteurs, c'est-à-dire des détenteurs de noms de domaine : Madonna, Eminem, Sting, Pierce Brosnan et Bill Clinton ont aussi dû se protéger contre ces squatteurs. Il est rare que ces actions aient une issue heureuse : Sting a



dû essayer une défaite, le nom de domaine sting.com ne lui ayant pas été reconnu. Même Bill Clinton a dû renoncer à posséder pas mal de noms de domaine comme williamclinton.com ou williamjclinton.com.

Des firmes connues comme Google et Microsoft ont dû se débattre avec le typosquatting. Un groupe de pirates Internet s'est par exemple approprié le nom de domaine googlek.com. Bon nombre de personnes ayant consulté ce site ont été infectées par un virus dangereux. Suite à un arrêté de justice, ce site est

désormais redirigé vers google.com.

L'accaparement de noms de domaine, le « domaingrabbing », la réservation d'adresses Internet, aussi appelée le « domainsquatting », ainsi que le piratage de marques, aussi connu sous le nom « brandjacking », ont été ces dernières années des pratiques très en vogue auprès des cybercriminels. Selon une enquête de la Commission européenne, près d'un quart des propriétaires de marque ou de domaine interrogés ont déjà été victimes de cybersquatting.

MarkMonitor, une société spécialisée dans la surveillance de marques sur Internet, recensait en 2008 quelque 1,7 million d'utilisations abusives de marques dans des noms de domaine, soit une progression de 18 % en un an. L'OMPI, l'Organisation Mondiale de la Propriété Intellectuelle, faisait état en mars 2009 de 2329 plaintes déposées, notamment par le club de football anglais Arsenal, la société agroalimentaire Nestlé et l'actrice américaine Scarlett Johansson.

Un nom de domaine – par exemple « cases » dans [www.cases.lu](http://www.cases.lu) – constitue le cœur d'une adresse Internet. Il peut se composer de lettres, de chiffres et de caractères spéciaux comme un trait d'union. Un bon nom de domaine dans le monde numérique est généralement aussi précieux qu'une adresse 1A dans le monde réel. Certaines adresses Internet valent donc beaucoup d'argent. L'adresse [business.com](http://business.com) a par exemple été vendue pour 7,5 millions de dollars.

Lorsque de grosses sommes sont en jeu, différentes astuces sont utilisées. Les cybersquatteurs remplissent un nom de domaine qu'ils ont acheté pour quelques euros de contenus à connotation négative sur l'offre de la

### **Conseil de sécurité : contrôler les contenus actifs**

Protégez-vous contre les sites douteux. Dans le navigateur Mozilla Firefox, il est possible de marquer les points suivants sous Outils/Options/Sécurité : avertir lorsque des sites essaient d'installer des modules ; afficher une alerte si le site visité est considéré comme un site attaquant ; afficher une alerte si le site visité est considéré comme frauduleux. Les attaques drive-by download sont particulièrement dangereuses. Même si un utilisateur ne télécharge rien d'Internet, il peut être victime d'un piège rien qu'en surfant sur des sites manipulés. Les pirates ajoutent des contenus actifs sur des sites non suspects mais mal protégés ou manipulent les contenus actifs déjà présents comme ActiveX, Java et Flash. Vous pouvez vous protéger en contrôlant l'autorisation de contenus actifs via le navigateur. Mozilla Firefox permet en outre via <https://addons.mozilla.org/de/firefox/addon/722> d'installer l'extension NoScript.

personne concernée ou l'entreprise. Ils espèrent ainsi que les victimes achètent le nom de domaine à prix supérieur pour se débarrasser de ces opinions nuisibles.

### **Enregistrement à des fins malveillantes**

Les internautes doivent savoir que certains noms de domaine ne sont enregistrés qu'à des fins malveillantes. Le but est de tromper les utilisateurs ou de leur nuire. Un cas classique de duperie d'internautes est l'enregistrement par des cybercriminels de noms ressemblant à celui de

sociétés réputées afin de diriger les victimes vers un site falsifié proposant une gamme de produits comparable ou des articles pouvant être confondus avec des produits de marque. Les victimes sont essentiellement les commerces virtuels et les clients. Les sites d'enchères sont eux aussi concernés par ces duperies. Par exemple, le nom [eay.de](http://eay.de) ne dirige pas vers le célèbre portail d'enchères eBay mais vers un concurrent.

Les internautes sont aussi induits en erreur par de prétendus sites d'entreprise qui se révèlent être des sites de commentaires négatifs ou d'appel au boycott. On a longtemps retrouvé dans cette catégorie le site

elf.de qui exerçait une pression sur un groupe pétrolier.

Le cybersquattage de réseaux sociaux fait partie des nouvelles formes de duperie. Des utilisateurs de Twitter réservent des adresses Twitter d'entreprise pour diffuser ensuite des stupidités sur l'entreprise en se faisant passer pour des membres du personnel. Cet « account grabbing » se retrouve aussi sur Facebook. Depuis le 13 juin, il est possible de personnaliser des pages avec son propre nom selon le principe « facebook.com/votre nom ». Dès les premiers jours, cette possibilité a donné naissance à des abus.

Une autre astuce de criminels, certes pas nouvelle mais très efficace, consiste à enregistrer des noms ressemblant au nom de domaine de grandes banques. Par cette combine, ils espèrent obtenir des informations sensibles comme le numéro PIN du titulaire du compte via le phishing. En Allemagne, on peut citer le cas d'escrocs qui, au nom de la Volksbank, ont invité les clients à une « harmonisation des données pour le compte ». Le nom de domaine frauduleux était volksbank-datenabgleich.de.

Dans certains cas, les fautes de frappe dans l'adresse de sites destinés aux enfants conduisent à des contenus pornographiques. En 2008, la

chaîne de télévision Cartoon Network a été concernée : ici, les criminels ont enregistré 327 domaines différents avec erreurs typographiques. Un nom de domaine peut aussi être utilisé pour diffuser des milliers de spams.

Une autre forme de nuisance pour les internautes est l'enregistrement de noms de domaine soi-disant dérivés. On retrouve dans cette catégorie l'exemple de eBay-members.com. Le site utilise le même design et le même style que le site eBay officiel de sorte que l'utilisateur a l'impression qu'il s'agit réellement du site des membres d'eBay. Mais ce site a été enregistré par des pirates.

Le cas de skype.at est aussi entré dans les annales. Ce site n'était pas la présence autrichienne de Skype sur Internet (un logiciel permettant de téléphoner à bon compte via Internet) même si l'adresse le laissait penser. Avec la promesse de pouvoir téléphoner gratuitement sur Internet via Skype, les utilisateurs étaient invités à entrer leurs données d'adresse pour télécharger le logiciel. Les utilisateurs ont été sournoisement abusés. En communiquant ses données personnelles, l'utilisateur concluait un contrat et s'engageait à verser 192 EUR au prestataire pour deux ans. Avant d'envoyer le formulaire, l'utilisateur devait renoncer à son droit de rétractation légal.

Nombre d'utilisateurs n'ont remarqué le piège que lorsqu'ils ont reçu la facture.

### **Réflexes de protection pour les utilisateurs, les entreprises et les organisations**

Pour se protéger des différentes formes d'attaque sur les noms de domaine, il convient d'observer quelques règles et d'appliquer quelques réflexes de sécurité. Les utilisateurs d'Internet doivent faire preuve de prudence surtout sur les sites de banques ou d'enchères. Ils ne devraient jamais cliquer sur un lien dans un e-mail. Ce lien peut s'avérer faux et conduire à un site complètement différent de celui annoncé dans l'e-mail.

Lorsqu'il saisit un nom de domaine, l'utilisateur doit toujours vérifier l'orthographe. S'il tombe sur quelque chose d'inhabituel ou de suspect sur le site, il doit immédiatement contrôler l'orthographe du nom de domaine dans la barre d'adresse du navigateur.

Les organisations et entreprises devraient se protéger de toutes parts pour ne pas laisser d'angle d'attaque aux cybercriminels. Ces mesures englobent aussi l'enregistrement de toutes les variantes de domaine pour les marques, entreprises et produits. Pour renforcer encore la protection de noms importants, il convient de vérifier l'entrée dans le

registre de marques du Benelux (Office Benelux de la propriété intellectuelle) ou dans le registre de marques européen. Un avocat spécialisé dans les marques peut donner toutes les informations nécessaires.

Pour se prémunir du typosquattage, les plus grosses organisations et entreprises devraient vérifier si l'enregistrement de quelques noms de domaine avec erreur typographique pourrait être judicieux. Les

organisations et firmes devraient en outre éviter d'envoyer des e-mails à partir d'un prestataire libre, c'est-à-dire gratuit. Il peut arriver ici qu'en dehors du domaine d'influence du prestataire, le nom de domaine soit détourné pour l'envoi de spams.

Il est également recommandé de garder un œil sur les noms qui ressemblent dangereusement à ceux de ses propres marques, à l'entreprise et à ses produits

actuels ou en projet. Pour cela, les responsables peuvent utiliser la fonction « Google Alerts » ou consulter régulièrement des registres de marques et le serveur WHOIS. Ils devraient aussi s'informer via le site Wipo.org ou un moteur de recherche sur le droit des domaines, des noms et des marques.

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

[www.cases.lu](http://www.cases.lu)