# Cybersquatting: Attention aux attaques homographiques !

**Categories :** Noms de domaine, WebInlex

**Date :** lundi 1 avril 2019

Comme les titulaires de marques et les spécialistes en noms de domaine le savent si bien, les fraudeurs et les cybersquatteurs peuvent être imaginatifs et trouvent sans cesse de nouveaux moyens de porter atteinte aux marques et aux consommateurs en réservant et en utilisant des noms de domaine de manière frauduleuse.

### ***Cybersquatting* et *typosquatting***

Ces pratiques, communément appelées ***cybersquatting***, consistent notamment à enregistrer des noms de domaine reproduisant des marques. Ceux que l'on appelle *cybersquatteurs* vont ensuite soit tenter de vendre ces noms de domaine aux titulaires des marques concernées, soit porter atteinte à la réputation et à la visibilité de ces marques ou encore en tirer indûment profit par le biais de ces noms de domaine.

L'une des formes les plus connues de *cybersquatting* consiste à réserver des noms de domaines très proches de marques ou de noms de domaine existants et comportant des fautes de frappe ou d'orthographe. Baptisée ***typosquatting***, cette pratique repose principalement sur les fautes que pourraient commettre les internautes en entrant directement une adresse URL dans leurs navigateurs.

*Exemples : au lieu de , ou au lieu de*

Par le biais de ces techniques, les fraudeurs ont pour objectif d'exposer les internautes à des messages publicitaires non sollicités, des virus ou les amener sur ce que l'on appelle des sites d'hameçonnage (*phishing websites).* En effet, le *typosquatting* est fréquemment utilisé dans le cadre d'opérations d'hameçonnage (*phishing*), une technique visant à piéger les internautes afin d'obtenir leurs données personnelles, les amener à télécharger des virus sur des faux sites ou leur envoyer des emails frauduleux en usurpant l'identité d'une société.

### Noms de domaine internationalisés (IDN) et attaques homographiques

Il y a plusieurs années déjà, l'internationalisation constante de l'Internet a rendu possible de réserver ce que l'on appelle des noms de domaines internationalisés (IDN : *Internationalized*

*domain names*). Il s'agit de noms de domaine qui contiennent en tout ou partie des caractères accentués ou appartenant à d'autres alphabets (Arabe, Chinois, Cyrillique…).

Inutile de dire que l'émergence des noms de domaine internationalisés (IDN) a offert des possibilités quasi-infinies aux *cybersquatteurs*, qui peuvent jouer sur les similitudes entre des caractères de différents alphabets et les mixer afin de réserver des noms de domaine plus ressemblants que jamais aux marques et noms de domaine préexistants. Cette pratique est communément appelée **attaque homographique**.

Ces atteintes sont possibles du fait que certains caractères non latins (*tels que ceux des alphabet Grec ou Cyrillique*) sont similaires à s'y méprendre aux caractères latins : c'est ici que réside l'astuce pour réserver des noms de domaine frauduleux reproduisant de façon quasi-identique des droits antérieurs.

S'il est possible de réserver des noms de domaine internationalisés depuis plusieurs années maintenant, ces attaques homographiques connaissent un forte recrudescence ces dernières années, et ont visé plusieurs grandes sociétés mondiales. Quelques exemples :

- (*utilisé dans le cadre d'une arnaque massive au début de l'année 2018*), , réservés en fraude des droits la compagnie aérienne française Air France ;
- , , réservés en fraude des droits des réseaux sociaux WhatsApp and Instagram;
- réservé en fraude des droits du groupe allemand BMW;
- réservé en fraude des droits de la société néerlandaise IKEA;
- réservé en fraude des droits de la chaîne de supermarchés française E. LECLERC…

**Ce qu'il faut retenir**

Le *cybersquatting* connaît de nombreuses variations, qui illustrent la grande agilité et l'imagination sans fin des cybercriminels.

Les conséquences des attaques homographiques et des attaques de cybersquatting en général, en particulier celles impliquant des tentatives d'hameçonnage (*phishing*), peuvent être graves pour les sociétés en termes d'activité et d'image, celles-ci pouvant occasionner une perte de confiance des consommateurs ainsi que des pertes financières.

Par ailleurs, les *cybersquatteurs* ne visent pas seulement les grandes sociétés mondiales mais peuvent également s'attaquer à n'importe quelle société en s'immisçant en interne ou auprès de ses fournisseurs, distributeurs…. par la réservation de noms de domaine proches de marques ou de dénominations sociales qui servent à envoyer des emails frauduleux avec pour objectif ultime de détourner des fonds.

**Cela souligne l'importance de surveiller sa marque sur Internet, et particulièrement parmi les noms de domaine, afin de détecter rapidement et neutraliser efficacement tout nom de domaine portant atteinte à un titulaire de droits.**

Notre cabinet reste à votre disposition pour vous accompagner dans la protection de vos marques parmi les noms de domaine et vous assister dans les problématiques de *cybersquatting*.

Lucie PRUNIERES, *Juriste en Propriété Industrielle*

INLEX IP EXPERTISE