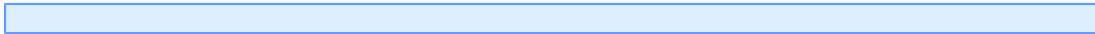


Marketing alternatif ou Black marketing : Techniques et prévention

par Maxime Biasutti ([Marketing alternatif ou black marketing : techniques et prévention](#))

Date de publication : 21 janvier 2009

Dernière mise à jour :



I - Introduction.....	3
II - Qu'est-ce que le black marketing?.....	3
III - Le black marketing, une technique offensive !.....	3
IV - Quelques techniques du black marketing.....	3
IV-A - La désinformation.....	3
IV-A-1 - Comment procéder ?.....	4
IV-A-2 - Exemple.....	4
IV-B - Les darksites.....	4
IV-B-1 - Exemple.....	4
IV-C - Espionnage.....	4
IV-C-1 - Comment procéder ?.....	5
IV-D - L'attaque DoS (Deny Of Service).....	5
IV-D-1 - Comment s'en prévenir ?.....	5
IV-E - Spam bombing/Mail bombing.....	5
IV-E-1 - Une variante possible.....	5
IV-E-2 - Comment éviter le spam ?.....	5
IV-F - Spam sur les forums et les blogs.....	6
IV-G - Farmlinks (Fermes de liens).....	6
IV-H - Génération de faux trafic.....	6
IV-H-1 - Comment s'en prévenir ?.....	6
IV-I - Les splogs.....	6
IV-J - Les pages satellites.....	6
IV-J-1 - Exemple.....	7
IV-K - Le cloaking.....	7
IV-K-1 - Comment détecter une page cloakée ?.....	7
IV-L - Le referer cloaking.....	7
IV-M - Keyword stuffing.....	7
IV-M-1 - Comment ces listes de mots clés ou portions de textes sont-ils cachés ?.....	8
IV-N - Phishing.....	8
IV-N-1 - Comment s'en prévenir ?.....	8
IV-O - Exploitation des failles XSS (Cross Site Scripting).....	8
IV-O-1 - Qu'est-ce qu'une faille XSS ?.....	8
IV-O-2 - La faille XSS persistante.....	8
IV-O-3 - La faille XSS non persistante.....	8
IV-O-4 - Comment s'en prévenir ?.....	9
IV-P - Page HiJacking.....	9
IV-P-1 - Comment procéder ?.....	9
IV-P-2 - Comment s'en prévenir ?.....	9
V - Que risque-t-on à employer de telles techniques ?.....	9
VI - Conclusion.....	10
VII - Liens utiles.....	10

I - Introduction

Attention, l'article suivant a pour but d'avertir les développeurs et webmasters de certaines techniques, parfois et même souvent illégales, permettant à un site (une entreprise) d'augmenter ses visites (son chiffre d'affaire) et non d'inciter à utiliser des techniques illégales susceptibles de conduire à des poursuites judiciaires. Cependant, même si ces techniques sont expliquées, vous ne trouverez pas le moyen direct (code, ou autre) permettant de les mettre en oeuvre ou encore d'exploiter certaines failles de sécurité.

Il est conseillé de lire tous les articles et tutoriels sur le webmarketing afin de mieux comprendre le contenu qui va suivre. (cfr: Pied de page)

II - Qu'est-ce que le black marketing?

Nous connaissons tous de près ou de loin le fonctionnement du marketing : Faire la promotion d'un produit ou d'un service, via la publicité, les médias, le bouche à oreille. Trouver de manière innovante le moyen de faire connaître un produit ou un service au public en impliquant directement ou non le consommateur?

Aujourd'hui, vu l'ampleur incroyable du web et de son évolution incessante, il est impératif pour les entreprises d'être présentes sur la toile, de vendre leurs produits et/ou services en ligne (sites d'e-commerce), de toucher le public d'une autre manière en exploitant le web (publicité web, adWords google, emailing, buzz, etc).

Malheureusement il est fastidieux, long et bien souvent très coûteux d'avoir une bonne visibilité sur le web. Dès lors, on remarque que beaucoup trop de sites web doivent fermer à cause d'un mauvais positionnement sur les moteurs de recherches (particulièrement Google) suite au nombre astronomique de résultats retournés par recherche sur un mot clé.

Arriver dans les premières positions demanderait d'une part beaucoup de temps, et d'autre part, parfois, beaucoup d'argent pour une efficacité directe.

Voilà pourquoi certains sites (entreprises), une fois le coup du risque bien analysé, se lancent dans des techniques déontologiquement peu correctes pour augmenter leur nombre de visites et donc leur chiffre d'affaire? Ces techniques sont appelées « black marketing » ou encore « marketing alternatif ».

III - Le black marketing, une technique offensive !

Le black marketing, en opposition au marketing classique (white marketing), consiste à améliorer la visibilité, l'image, les ventes d'une entreprise à long ou à court terme de manière illégale. Mais ce n'est pas tout, si le black marketing permet d'améliorer les ventes, le chiffre d'affaire, l'image de marque d'une entreprise, il peut en faire de même pour ses concurrents mais avec l'effet inverse ! Ainsi, il sera possible de nuire à l'image de marque du concurrent, à sa crédibilité, sa visibilité sur le web, à voler ses clients ou carrément détruire son entreprise?

Nous allons d'ailleurs voir quelques-unes des différentes techniques plus ou moins nocives permettant soit d'apporter un plus à son site, soit de nuire au site du concurrent.

IV - Quelques techniques du black marketing

IV-A - La désinformation

La désinformation consiste à faire courir une rumeur ou un bruit négatif sur une entreprise ou l'un de ses produits ou services afin de nuire à son image, ses activités ou encore sa visibilité. Cette technique est souvent utilisée par une entreprise concurrente ou par un client mécontent.

IV-A-1 - Comment procéder ?

En utilisant les blogs et les forums comme moyen de communication. Les personnes pratiquant la désinformation utilisent généralement différents comptes fictifs créés à des dates différentes. Ils participent de manière active sur les blogs et forums afin de leurrer les autres utilisateurs.

IV-A-2 - Exemple

Je suis une entreprise (A), je veux commercialiser un produit ou un service mais j'ai un concurrent (B) qui me gêne?

Moi, entreprise A, j'ai 3 comptes sur developpez.com, Toto63 inscrit en septembre 2008 (151 Messages à son actif), Biloutte_du_16ème juin 2009 (89 Messages), LeBelge décembre 2009 (11 Messages).

Après quelques temps, A souhaite lancer un bruit négatif sur un produit ou service de B via le forum developpez.com. A choisi donc de poster un message(??) sur le forum pour expliquer sa mésaventure avec le produit de B. A va répondre (d'une autre IP et machine bien sûr) avec son 2e compte pour affirmer les dires du premier compte. Et le 3e compte va faire de même etc?

Maintenant d'autres internautes ne sont pas dupes, et exigeront peut être plus de détails?

C'est simple, montrer leur des exemples d'autres plaintes en leurs envoyant vos URLs d'autres forums, blogs privés anonymes, etc que vous aurez précédemment mitonnés et fait de même avec peut être 10 autres comptes sur d'autres forums, sur des sujets de blogs, etc? (voir également darksites)

Peu importe si c'est une rumeur ou un fait vérifié, tant que les internautes trouvent des sujets qui traitent de ce post dans Google, ils croiront certainement que tout ceci est vrai !

Ceci n'est bien sûr qu'un petit exemple fictif de ce qu'il est possible de faire?

IV-B - Les darksites

Les darksites sont des sites créés par une entreprise elle-même mais qui masque sa véritable identité ainsi que ses objectifs. Ceux-ci serviront à diffuser des informations soit, pour venter un produit (celui de l'entreprise elle-même) ou pour dénigrer le produit d'une société concurrente. Ainsi les règles ne sont plus respectées.

IV-B-1 - Exemple

Une entreprise (A) souhaite promouvoir un de ses produits (Un soin du corps par exemple) mais de manière la plus naturelle possible. L'idéal serait que d'autres utilisateurs ventent les produits de A. A va décider de créer un darksite qui aura pour but de tester plein de produits similaires mais de marques différentes. Ainsi, la ou les personnes appartenant à l'entreprise A effectueront des tests et des comparatifs sur chaque produit qui seront diffusés sur le darksite. Tous les produits seront passés en revue mais au bout du compte ils en viendront à la conclusion que le meilleur produit est celui de la société A.

IV-C - Espionnage

Une stratégie de base pour pouvoir faire mieux que ses concurrents, obtenir une meilleure visibilité ou bien encore innover, consiste à espionner le voisin. Savoir ce que le concurrent prépare pour réagir avant qu'il n'agisse !

IV-C-1 - Comment procéder ?

En analysant par exemple l'arborescence de son site. Le fichier robot.txt d'un site web vous en apprendra peut être beaucoup sur une entreprise, ses intentions, ses stratégies, etc.

Il est possible ainsi par exemple, de tomber sur un répertoire non protégé de son concurrent, préparant une campagne publicitaire, une nouvelle version graphique de son site, etc.

IV-D - L'attaque DoS (Deny Of Service)

Cette technique consiste à surcharger un serveur dans le but de le ralentir, voir carrément le rendre inutilisable. Par exemple, si un serveur d'hébergement web est mal configuré, il est possible d'utiliser certains programmes pour faire de l'envoi automatique de mails depuis le site cible hébergé sur le serveur. Cela pourrait provoquer une augmentation considérable des fichiers de logs, et en venir à un espace disque insuffisant.

Il est évident qu'un site d'e-commerce hors service ne serait-ce que quelques minutes pourrait perdre pas mal de vente ainsi que sa crédibilité.

IV-D-1 - Comment s'en prévenir ?

Augmenter la taille des logs, sécuriser les formulaires (!!!), ne jamais mettre son serveur mail en open relay (exiger une authentification), mettre un système d'alertes sur le serveur qui prévient lorsque l'espace disque atteint un certain seuil critique, ne jamais mettre un temps d'exécution de page illimité, etc.

Il est donc possible d'éviter ces attaques de déni de service en respectant certaines règles de prévention de base.

IV-E - Spam bombing/Mail bombing

Autre technique similaire au principe des attaques DoS (Deny Of Service). Elle consiste à envoyer des centaines de milliers d'emails vers `patron@nomdelentreprise.com` ou encore `sales@nomdelentreprise.com` afin d'empêcher la lecture des emails?

L'utilisation d'une telle technique provoquera à court terme la perte d'emails de clients, une qualité des services ralentis, et une perte plus ou moins importante des ventes qui ne pourront aboutir. Les clients insatisfaits et mécontents, eux, iront voir la concurrence?

IV-E-1 - Une variante possible

L'utilisation des formulaires du site cible pour envoyer des milliers de spams à partir du serveur mail sur lequel le site est hébergé. Les emails seront envoyés de `quelquechose@nomdelentreprise.com`.

L'avantage de cette technique est que les emails ne seront pas reçus comme courrier suspect par exemple, sur les messageries telles que hotmail.com. Remonter à la source nous amènerait tout droit vers « `nomdelentreprise.com` » et risquerait de lui attirer, en plus de ça, quelques ennuis?

IV-E-2 - Comment éviter le spam ?

En installant un filtre anti-spam puissant sur le serveur (et non du côté client), en essayant d'enregistrer une copie en base de données (forcer le client à utiliser un formulaire de contact par exemple pour tout ce qui traite des commandes), etc.

IV-F - Spam sur les forums et les blogs

Spammer sur les forums et les blogs en se faisant passer pour un concurrent peut nuire à son image et à son positionnement sur Google. Cette technique peut même conduire jusqu'au black listing par Google !

Je n'entrerai pas plus en détails dans le spam. J'aurais pourtant pas mal d'exemples à proposer...

IV-G - Farmlinks (Fermes de liens)

Ils existent des sites, annuaires ou autres, qui proposent de promouvoir votre site web. Sachez que beaucoup des ces annuaires sont mal vus par Google et pourraient dans un cas extrême vous faire blacklister. Enregistrez vos concurrents sur ce genre d'annuaires (douteux) risquerait de leur nuire?

Cependant, si vous parvenez à enregistrer votre concurrent sur dmoz.org (quand ils veulent bien le faire mais ça c'est une autre histoire?) vous avez toutes vos chances de perdre des clients :-)

IV-H - Génération de faux trafic

Il est possible de faire générer du faux trafic et donc des visiteurs uniques sur votre site web. Cette technique fausserait vos statistiques mais vous permettrait, par exemple, de squatter la pole position sur les sites de services de positionnement. (top hits, etc)

Généralement, ce genre de sites vous propose d'ajouter une image ou une portion de code dans le pied de page de votre site et affichera sur le sien un classement (ordonné par ordre décroissant des visites) des sites les plus populaires pour un thème bien spécifique.

Par exemple un top hits pour les sites de « css showcase ».

Ainsi les visiteurs consultant l'annuaire regroupant tous les sites de css showcase, verraient en première position votre site avec 30 000 visites par jour et cliqueraient sans hésitation sur le votre?

IV-H-1 - Comment s'en prévenir ?

En dénonçant aux administrateurs les sites qui vous semblent suspects tout simplement. Eux feront leur travail pour savoir si le site triche ou non.

IV-I - Les splogs

On appelle « splogs » des sites ou blogs appartenant à une personne ou une entreprise dont le but est d'obtenir du page rank. Ces sites proposent donc du contenu susceptible d'intéresser les visiteurs. Le but est d'obtenir un maximum de splogs, une fois que les splogs disposent d'un PR conséquent, il suffit d'effectuer une redirection 301 de tous les splogs vers le site cible afin d'hériter du page rank entier de chacun.

Maintenant, il existe même des splogs qui auto génère du contenu en allant rechercher des articles via les flux RSS de divers sites web? Ainsi, plus besoin d'administrer les splogs, leur conception et leur paramétrage suffisent !

IV-J - Les pages satellites

Une page satellite est une page web qui ne possède aucun lien direct depuis le site mais qui a été référencée sur google d'une manière ou d'une autre. Ces pages sont conçues pour augmenter le nombre d'entrées des visiteurs et des robots.

IV-J-1 - Exemple

Je suis une entreprise, j'ai un produit à vendre, je crée une page officielle de ce produit que j'ajoute à la navigation de mon site. Cependant, pour maximiser le nombre d'entrées possible et pour augmenter en visibilité, je vais créer plusieurs versions de cette page (en évitant l'effet de duplicate content), afin de référencer ces pages sur google?

Ainsi, sur ma première page, je vais exploiter en profondeur le « terme 1 ». Sur la deuxième page je vais par contre exploiter le « terme 2 ». Sur la troisième page le « terme 3 » et ainsi de suite?

Ne pas oublier que chacun des termes concerne un même produit ou service.

Au lieu de focaliser tous les termes sur une page, je les sépare sur des pages bien distinctes? Ainsi, la visibilité sur les moteurs de recherches est meilleure en fonction de chacun des termes si la densité des mots clés est bien respectée.

Lorsqu'un visiteur tapera le « terme 1 » sur google, il tombera sur la page travaillée pour le terme 1, lorsqu'il tapera le « terme 2 », il tombera sur la page travaillée pour le terme 2 etc. Et toutes ces pages seront utilisées pour la promotion d'un SEUL produit !

PLUSIEURS PAGES = PLUSIEURS ENTREES => UN SEUL OBJECTIF !

IV-K - Le cloaking

Le cloaking consiste à afficher une page différente aux moteurs de recherches que celle vue par les visiteurs. Le principe consiste à détecter les robots afin de leur afficher un contenu différent des humains.

IV-K-1 - Comment détecter une page cloakée ?

En analysant une page en « cache » via le moteur de recherche de google. En utilisant des services de détection de pages cloackées?

Essayez le **détecteur de cloaking**

Le cloaking permet également d'améliorer le page rank d'un site en proposant un lien référent sur un site sans que celui-ci ne soit visible par son propriétaire.

IV-L - Le referer cloaking

Le « referer cloaking » est une variante du cloaking. Cette technique permet d'afficher un contenu ou une publicité cible en fonction des mots clés encodés dans les moteurs de recherches.

Ainsi si un utilisateur tombe sur une page exploitant le referer cloaking avec l'expression « Namur Belgique », la page pourra lui afficher par exemple toutes des offres d'hôtels ou de restaurants de la ville de Namur.

IV-M - Keyword stuffing

Consiste à insérer une liste de mots clés ou des paragraphes de textes entiers dans le but d'améliorer le référencement sur les moteurs de recherches.

Le texte est généralement masqué pour les visiteurs, ainsi seul les moteurs de recherches voient le contenu ajouté.

IV-M-1 - Comment ces listes de mots clés ou portions de textes sont-ils cachés ?

Simplement en mettant du texte blanc sur fond blanc, noir sur fond noir etc.

Les moteurs de recherches peuvent détecter ces techniques en analysant les feuilles de styles (CSS) et peuvent aller jusqu'à blacklister les sites utilisant de telles techniques.

Pour contourner ce risque, certains webmasters utilisent du texte blanc en insérant en fond une image blanche? Ainsi google ne parvient pas à cerner l'arnaque (du moins pour l'instant).

IV-N - Phishing

Cette technique consiste à récolter des informations confidentielles de l'entreprise, d'un utilisateur ou consommateur de manière frauduleuse.

Par exemple, un concurrent de msn pourrait envoyer facilement un email à chaque client msn en se faisant passer pour msn afin de récolter des informations confidentielles.

IV-N-1 - Comment s'en prévenir ?

Ne jamais répondre à un mail demandant des informations de type « nom d'utilisateur » et « mot de passe », ne pas communiquer de numéro de téléphone ou d'adresse si vous n'êtes pas certain de la source, etc.

IV-O - Exploitation des failles XSS (Cross Site Scripting)

Il faut savoir qu'il est possible de faire beaucoup de dégât si un site n'est pas protégé contre les failles XSS.

IV-O-1 - Qu'est-ce qu'une faille XSS ?

C'est le fait de pouvoir injecter du langage de script tel que du code javascript, ou encore du code HTML dans un site, via tout ce qui est formulaire, via les paramètres passé en URL, etc.

Une faille XSS vous permettra par exemple, d'afficher des publicités sur le site cible de votre concurrent, ou encore rediriger les visiteurs de votre concurrent vers votre propre site. Plus futile encore, récupérer les informations confidentielles des clients de votre concurrent, telles que mots de passes, nom d'utilisateur, adresse email, etc. Ou encore de faire planter la page tout simplement?

Il existe 2 types de failles XSS, la faille persistante, et non persistante.

IV-O-2 - La faille XSS persistante

Cela signifie que le résultat sera enregistré sur la page (un forum, les commentaires d'un blog, etc.) L'effet sera immédiat.

IV-O-3 - La faille XSS non persistante

Le résultat n'est pas enregistré (un moteur de recherches qui affiche le résultat de la recherche, une erreur SQL générée, etc.)

Il faudra pour une faille non persistante, envoyer l'URL affichant le résultat à la cible (généralement un administrateur de site web, un client). Une fois la personne ayant cliqué sur l'URL, l'attaque prendra effect ! Généralement, pour

récupérer le login et mot de passe d'un administrateur, il faut que celui-ci soit connecté sur son site avant de cliquer sur l'URL.

IV-O-4 - Comment s'en prévenir ?

En sécurisant votre code notamment en empêchant aux visiteurs d'injecter du code en l'échappant. En PHP on utilisera par exemple, strip_tags, htmlentities ou encore html_specialchars, etc.

IV-P - Page HiJacking

Le page hijacking consiste à voler la position d'un concurrent sur les moteurs de recherches en fonction du contenu de la page.

IV-P-1 - Comment procéder ?

En faisant un « copier/coller » d'une page de vos concurrents qui n'est pas encore référencée par google ! En effet, lorsque google rencontre 2 pages à contenus similaires, il va choisir en fonction de la date d'ancienneté (date de passage de googlebot) celle qu'il va conserver. Lorsqu'il rencontre 2 pages à contenus similaires, il va conserver celle où le bot Google,googlebot, est passé en premier !

Attention donc à ce qu'un de vos concurrents ne parvienne à faire référencer la copie de votre page avant vous ! Ainsi, vous ne pourrez apparaître dans Google, vous perdrez en visibilité et votre concurrent sera gagnant?

IV-P-2 - Comment s'en prévenir ?

Le processus de référencement d'une page peut être excessivement lent pour un site à faible page rank ou Trustrank, un site comme developpez.com se voit référencer ses pages parfois quelques minutes après leur conception. Cela est dû à la popularité du site, à son page rank élevé, à son nombre de trafic et à sa fréquence de mise à jour. Un site dynamique fréquemment mis à jour se verra référencé plus rapidement qu'un site peu mis à jour. Une petite astuce pour augmenter le temps de référencement de votre page, serait par exemple de mettre en fin de votre post sur developpez.net, un lien vers la page que vous souhaiteriez référencer. Ainsi, vu le passage fréquent de googlebot, il y a de forte chance que celui-ci suive votre lien et analyse en premier votre page. Cela vous permettra d'éviter de vous faire voler votre page par votre concurrent?

Vous pouvez faire la même manipulation sur d'autres sites fréquemment référencés par Google. Forums, sites d'actualité, etc.

V - Que risque-t-on à employer de telles techniques ?

En fonction de l'infraction vous pouvez risquer une peine de prison plus ou moins importante ainsi que parfois plusieurs milliers d'euro d'amende?

Il est difficile de déterminer ce que vous risquer précisément en fonction de telle ou telle infraction, sachez cependant que les entreprises, web agences, agences de communication ou autre, analysent le coût du risque de manière à savoir si employer l'une ou l'autre techniques précédemment vues en vaut la chandelle ou non.

Si un procès de quelques milliers d'euro à lieu, mais qu'au bout du compte cela à permis à l'entreprise de se procurer une augmentation de son chiffre d'affaire de plusieurs millions, celle-ci n'hésitera pas à utiliser quelques techniques du black marketing pour arriver à ses fins.

Sachez cependant que ce sont parfois les agences de communication et web agences qui prennent les risques bien souvent sans que les sociétés pour qui elles travaillent n'en soit forcément au courant.

VI - Conclusion

Après un court tour d'horizon de « quelques-unes » des techniques possible du marketing alternatif axé web, nous constatons que ces techniques permettent parfois d'apporter un plus à son business, mais aussi de nuire de manière parfois très efficace à son concurrent.

Encore une fois, le contenu que vous venez de lire à pour but de vous avertir de l'existence de telles techniques et du danger potentiel que celles-ci représentent. En aucun cas cet article n'est conçu pour vous inciter à mettre en pratique de telles méthodes de black marketing.

Néanmoins, si vous seriez tenter d'essayer une approche de ce genre, soyez prêts à en assumer les conséquences? Conséquences juridiques ou même représailles de vos concurrents?

VII - Liens utiles

[Ceqoya seotools](#)
[Cours et tutoriels sur le webmarketing](#)
[FAQ Webmarketing](#)
[Livres sur le webmarketing](#)