EUIPO
EUROPEAN UNION
INTELLECTUAL PROPERTY OFFICE

www.euipo.europa.eu

GROS PLAN SUR LE CYBERSQUATTAGE: SUIVI ET ANALYSE

Mai 2021

1 Synthèse

1.1 Contexte

Le cybersquattage implique l'enregistrement et/ou l'utilisation de mauvaise foi de la marque d'une entreprise tierce (ou de tout autre signe devenu un identifiant distinctif de cette entreprise) dans un nom de domaine, sans avoir de droits légaux ou d'intérêts légitimes sur ce nom de domaine ([1]). Les titulaires de droits ont souvent fait part de leurs préoccupations concernant le cybersquattage, notamment depuis le début de l'extension des domaines de premier niveau génériques (gTLD) en 2012.

L'objectif de cette étude était de quantifier le phénomène du cybersquattage et de décrire les méthodes et les modèles commerciaux utilisés par les cybersquatteurs, et donc de fournir ainsi une base pour lutter plus efficacement contre ce phénomène.

L'étude a bénéficié d'une coopération avec les parties prenantes de l'Observatoire de l'EUIPO et s'est fondée sur les données et les connaissances partagées par les experts de la protection des marques des marques sélectionnées.

1.2 Méthodologie

La détection de noms de domaine cybersquattés nécessite d'identifier des noms de domaine contenant une marque déposée ou une variation d'une marque déposée similaire au point de prêter à confusion. Aux fins de l'analyse quantitative, l'identification et l'analyse des noms de domaine ont été réalisées sur 560 gTLD et 250 domaines de premier niveau nationaux (ccTLD), couvrant environ 239 millions de noms de domaine enregistrés. Cette analyse a été réalisée au cours du premier trimestre 2020.

[1] https://www.icann.org/resources/pages/cybersquatting-2013-05-03-fr

L'analyse quantitative s'est concentrée sur une sélection de 20 marques protégées, détenues par des petites, moyennes et grandes entreprises dans différentes catégories de produits et de services. Pour des raisons de confidentialité, les marques sélectionnées ainsi que leurs titulaires sont anonymisés dans le présent rapport ([2]). L'étude a identifié des utilisations suspectes des marques sélectionnées dans des noms de domaine enregistrés et a analysé les techniques utilisées par les cybersquatteurs pour tirer profit des marques développées par leurs titulaires.

Dans un premier temps, une recherche a été menée dans l'univers des noms de domaine enregistrés afin d'identifier ceux associés aux marques sélectionnées. Pour cet exercice, des mots-clés supplémentaires ont été ajoutés à certains noms de marques, ou certaines lettres ont été exclues après le nom de la marque, afin d'éviter la formation de mots courants ou de noms propres similaires à la marque en question qui «pollueraient» les résultats de la recherche.

Les cybersquatteurs n'enregistrent pas toujours des noms de domaine contenant la marque ou le nom de marque complets, mais plutôt une variante délibérément déroutante, par exemple une légère faute d'orthographe ou le remplacement d'une lettre par un chiffre. Par conséquent, des recherches ont également été menées pour certaines permutations dans les noms des marques. Enfin, des recherches spécifiques par mot-clé ont été ajoutées au nom de la marque afin de trouver les noms de domaine les plus précis liés à chaque marque.

La recherche a abouti à un total de 55 181 noms de domaine. Par la suite, un échantillon aléatoire de 100 de ces domaines pour chacune des 20 marques a été analysé manuellement. Pour certaines marques, le nombre de domaines recensés était inférieur à 100, de sorte que le nombre total de domaines analysés s'élevait à 1 864. Parmi ces domaines, 993 se sont révélés liés aux marques et ont fait l'objet de l'analyse quantitative ci-dessous.

Lors de la dernière étape de l'étude, 40 domaines «suspects» liés aux 20 marques couvertes par l'analyse quantitative ont été sélectionnés pour une analyse qualitative. L'objectif de cette deuxième analyse était de fournir une vue d'ensemble des différents

[2] Les 20 marques ont été identifiées par ordre alphabétique, soit de A à T.

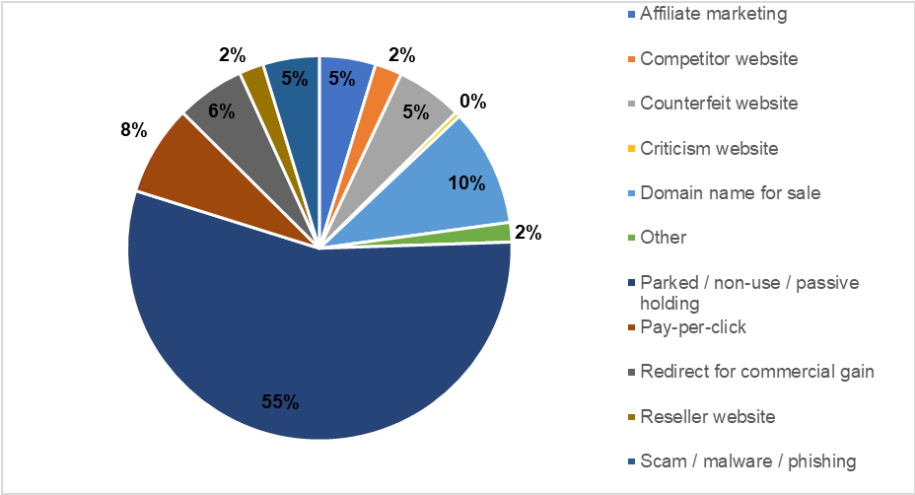
types de modèles commerciaux portant atteinte aux DPI, sur la base des domaines de premier niveau (DPN) utilisés, des types de droits de propriété intellectuelle (DPI) concernés et des caractéristiques du trafic internet. L'étude a analysé les modèles d'entreprises utilisés par ces domaines pour générer des revenus en incitant les visiteurs à effectuer un achat, ainsi que les produits et services couverts. Une matrice taxonomique du cadre des modèles d'entreprise a été utilisée pour identifier et démontrer systématiquement les principales caractéristiques de chaque modèle d'entreprise. Cette partie de l'analyse s'appuyait notamment sur la méthodologie élaborée par l'Office dans le rapport intitulé «Recherche sur les modèles d'entreprises en ligne portant atteinte aux droits de propriété intellectuelle».

1.3 Résultats

1.3.1 Analyse quantitative

Un peu moins de la moitié des 993 noms de domaine analysés, soit 486 (49 %), ont été considérés comme «suspects»; les autres étaient soit légitimement détenus par les titulaires de marques, soit sans lien avec les marques en question.

La majorité (55 %) des 486 domaines suspects se sont avérés être soit parqués, soit pas activement utilisés. Dix pour cent des domaines étaient à vendre, tandis que les autres étaient utilisés pour diverses activités, parmi lesquels les plus préoccupants étaient les sites web vendant des contrefaçons et les sites web pratiquant l'escroquerie, l'hameçonnage ou la diffusion de logiciels malveillants.

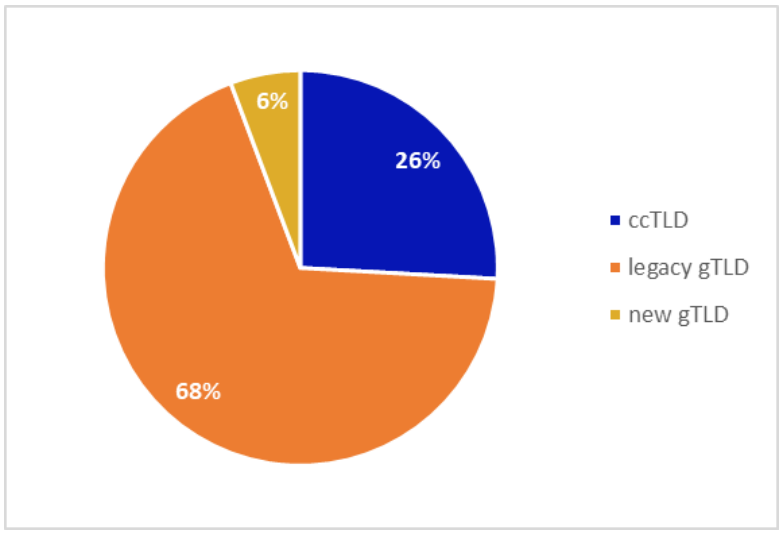


Affiliate marketing	Marketing d'affiliation
Competitor website	Site web concurrent
Counterfeit website	Site web de contrefaçon
Criticism website	Site web consacré à la critique
Domain name for sale	Nom de domaine à vendre
Other	Autre
Parked / non-use / passive holding	Parqué/non-utilisé/détention passive
Pay-per-click	Paiement par clic
Redirect for commercial gain	Réorientation en vue d'un gain commercial
Reseller websit	Site web de distributeurs
Scam / malware / phishing	Escroquerie/logiciel malveillant/hameçonnage

En décomposant les domaines suspects par type de nom, 414 (85 %) étaient des «expressions régulières» et 72 (15 %) des «permutations». Par conséquent, une expression régulière (c.-à-d. un nom de domaine contenant la marque en son sein) était le type de cybersquattage le plus courant.

Le niveau moyen de cybersquattage a été estimé à 49 %. Certains secteurs, dont la mode (66 %), l'électroménager (64 %) et l'automobile, les pièces détachées et les carburants (60 %), ont subi des niveaux de cybersquattage nettement supérieurs à la moyenne, tandis que les marques de produits et services de consommation courante (32 %) et de produits et services professionnels (24 %) sont moins touchées.

La répartition des DPN parmi les 993 domaines étudiés est présentée ci-dessous.



ccTLD	ccTLD
legacy gTLD	ancien gTLD
new gTLD	nouveau gTLD

Les anciens gTLD représentaient 679 (68 %) des noms de domaine, 257 (26 %) étaient des ccTLD et 57 (6 %) des gTLD nouveaux. Parmi ceux-ci, 338 anciens gTLD (50 %), 116 ccTLD (45 %) et 32 nouveaux gTLD (56 %) ont été considérés comme suspects. Le fait que les nouveaux gTLD ne représentaient qu'une part réduite des DPN suspects pourrait simplement refléter leur faible nombre par rapport aux anciens DPN. À ce moment-là, les nouveaux gTLD n'étaient pas une source significative de cybersquattage, bien que la proportion de domaines suspects parmi les nouveaux gTLD ait été plus élevée que pour les ccTLD ou les gTLD existants.

L'expression régulière (c.-à-d. un nom de domaine contenant la marque en son sein) était le type de cybersquattage le plus courant, représentant 85 % des domaines analysés.

De nombreux noms de domaine suspects ont été récemment enregistrés, 2019 étant l'année d'enregistrement la plus courante pour quatre des cinq catégories et 14 des 20 marques, avec un total de 145, suivie de l'année 2018 avec 57 et de l'année 2017, avec 35. Étant donné que de nombreux domaines ont été enregistrés pour des périodes d'un an, cela peut simplement refléter le fait que les cybersquatteurs ont laissé de

multiples domaines expirer (vraisemblablement parce qu'ils n'ont pas généré suffisamment de trafic et de revenus).

1.3.2 Analyse qualitative

Quarante noms de domaine suspects ont été sélectionnés pour une analyse qualitative à partir des domaines qui étaient en usage actif, et donc n'étaient ni parqués ni maintenus passivement.

Les principales conclusions ont été les suivantes:

- tous les domaines redirigeaient le trafic depuis la marque légitime dans le cadre des fonctionnalités du trafic sur l'internet;
- 24 noms de domaine (60 %) concernaient la commercialisation de produits physiques ou virtuels, tandis que 16 (40 %) concernaient une utilisation numérique abusive de noms de domaine;
- 24 noms de domaine (60 %) proposaient des produits ou services de contrefaçon, 11 (28 %) ne proposaient que des informations et 5 (12 %) proposaient des produits authentiques;
- 22 noms de domaine (55 %) attiraient les visiteurs en étant perçus comme légitimes et 18 (45 %) à la fois en étant perçus comme légitime et en accordant des remises;
- 24 noms de domaine (60 %) généraient des revenus grâce aux paiements de clients, 13 (33 %) grâce au paiement par clic et 3 (7 %) grâce à l'achat de noms de domaine;
- 32 noms de domaine (60 %) n'étaient pas sécurisés et 8 (20 %) l'étaient.

Les informations relatives au cybersquatteur n'étaient pas disponibles pour 26 des 40 domaines suspects, ayant été marquées comme «expurgées pour des raisons de confidentialité», ce qui était susceptible d'entraver toute mesure coercitive/répressive à l'encontre du titulaire du nom de domaine. Les informations concernant le titulaire d'un nom de domaine dans les dossiers WHOIS constituent le point de départ du traitement d'une activité suspecte. Toutefois, depuis l'entrée en vigueur du règlement général sur

la protection des données (RGPD), il existe une obligation légale de ne pas publier de données privées sans le consentement exprès des titulaires d'un nom de domaine individuels ([3]).

1.4 Conclusions et perspectives

Le cybersquattage est un véritable problème pour les marques légitimes. Si tous les domaines classés comme «suspects» ne présentent pas des atteintes aux DPI (par exemple, les sites de fans ou les sites consacrés à la critique), une partie des sites cybersquattés ont été utilisés pour commercialiser des produits de contrefaçon ou se livrer à d'autres activités illicites en utilisant la marque légitime afin d'attirer des visiteurs et ont, de ce fait, nuit à la marque déposée d'une manière qui va au-delà de la contrefaçon.

Cela pourrait être particulièrement grave pour les petites et moyennes entreprises (PME), qui manquent souvent de ressources pour surveiller activement leur présence sur le web afin de détecter le cybersquattage et de protéger la renommée de leurs marques.

D'autres études sur les logiciels malveillants et leur utilisation en ligne seraient nécessaires pour façonner davantage le paysage risque/rendement lorsque le cybersquattage est actif plutôt que passif. À mesure que la technologie évolue (avec, par exemple, la transcription de données vocales en données texte), de nouvelles possibilités de menace apparaîtront, et les stratégies de cybersquattage seront susceptibles de s'adapter afin de les exploiter. Ces menaces devront être contrebalancées par des données détaillées, des stratégies actualisées, l'amélioration des capacités des titulaires de marques et le soutien des prestataires de services.

Les conclusions de cette étude présentent un intérêt pour les experts en DPI et les intermédiaires de l'internet, ainsi que pour les titulaires de marques et les consommateurs, puisqu'elles soulignent l'ampleur de la menace posée par les

[3] https://www.eurodns.com/blog/WHOIS-database-gdpr-compliance

cybersquatteurs et fournissent une base pour lutter plus efficacement contre ce phénomène. L'étude comprend également un ensemble de connaissances susceptibles de faciliter les actions de lutte contre le risque.