EUIPO
EUROPEAN UNION
INTELLECTUAL PROPERTY OFFICE

www.euipo.europa.eu

FOCUS ON CYBERSQUATTING: MONITORING AND ANALYSIS

May 2021

1 Executive Summary

1.1 Background

Cybersquatting involves bad faith registration and/or use of another company's trade mark (or another sign that has become a distinctive identifier for that company) in a domain name, without having any legal rights or legitimate interests in that domain name([1]). Rights owners have often expressed their concern over cybersquatting, particularly since the expansion of the generic top-level domains (gTLDs) begun in 2012.

The purpose of this study was to quantify the phenomenon of cybersquatting and to describe the methods and the business models employed by cybersquatters, thus providing a basis for fighting the phenomenon more effectively.

The study benefited from cooperation with EUIPO Observatory stakeholders and relied on data and knowledge shared by brand protection experts from the selected brands.

1.2 Methodology

The detection of cybersquatted domain names requires the identification of domain names containing a trade mark or a confusingly similar variation of it. For the quantitative analysis, the detection and analysis of domain names was conducted across 560 gTLDs and 250 country code top-level domains (ccTLDs), covering approximately 239 million registered domain names. The analysis was carried out in the first quarter of 2020.

The quantitative analysis focused on a selection of 20 brands protected by trade marks, owned by small, medium and large entities across different categories of goods and services. For confidentiality reasons, the selected trade marks as well as their owners

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

are anonymised in this report([2]). The study identified suspicious uses of the selected trade marks in registered domain names and analysed the techniques used by cybersquatters to take advantage of the brands built by the trade mark owners.

In the first step, a search was conducted across the universe of registered domain names to identify those associated with the selected brands. For this exercise, additional keywords were added to some brand names, or certain letters were excluded after the brand name, in order to avoid the formation of common words or proper names similar to the brand in question that would 'pollute' the search results.

Cybersquatters do not always register domain names containing the full trade mark or brand name, but rather a deliberately confusing variant, for example a slight misspelling or replacement of a letter by a digit. Therefore, searches were also conducted for certain permutations of the brand names. Finally, specific keyword searches were added to the brand name to find the most accurate domain names related to each brand.

The search produced a total of 55 181 domain names. In subsequent steps, a random sample of 100 of these domains for each of the 20 brands was analysed manually. For some brands, the number of domains identified was less than 100, hence the total number of domains analysed was 1 864. Of those domains, 993 were found to be related to the brands and were the subject of the quantitative analysis below.

In the final step of the study, 40 'suspicious' domains related to the 20 brands covered by the quantitative analysis were selected for a qualitative analysis. The objective of this analysis was to provide an overview of the different types of infringing business models, based on the top level domains (TLDs) used, the types of intellectual property rights (IPRs) involved, and the characteristics of the internet traffic. The study analysed the business models used by those domains to generate revenue by inducing visitors to make a purchase, as well as the products and services they covered. A taxonomic matrix of the business model framework was used to systematically identify and demonstrate the main features of each business model. This part of the analysis was partly based on the methodology developed by the Office in the Research on Online Business Models Infringing Intellectual Property Rights report.

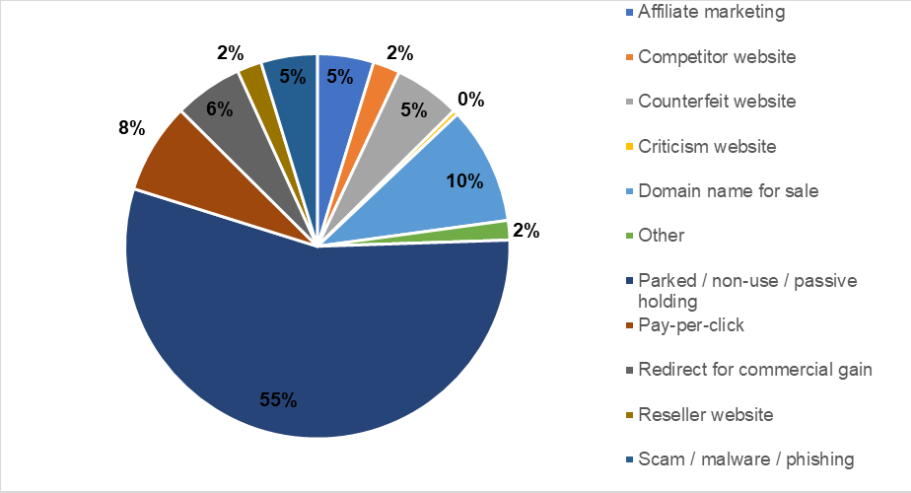
([2]) The 20 trade marks were identified in alphabetical order, brands A to T.

1.3 Results

1.3.1 Quantitative analysis

Just under half of the 993 analysed domain names, 486 (49 %), were considered 'suspicious'; the rest were either legitimately owned by the brand owners, or were not related to the brands in question.

The majority (55 %) of the 486 suspicious domains turned out to be parked or otherwise not actively used. Ten percent of the domains were for sale, while the remainder were used for a variety of activities, of which most concerning were websites selling counterfeits and websites engaged in scams, phishing, or distribution of malware.

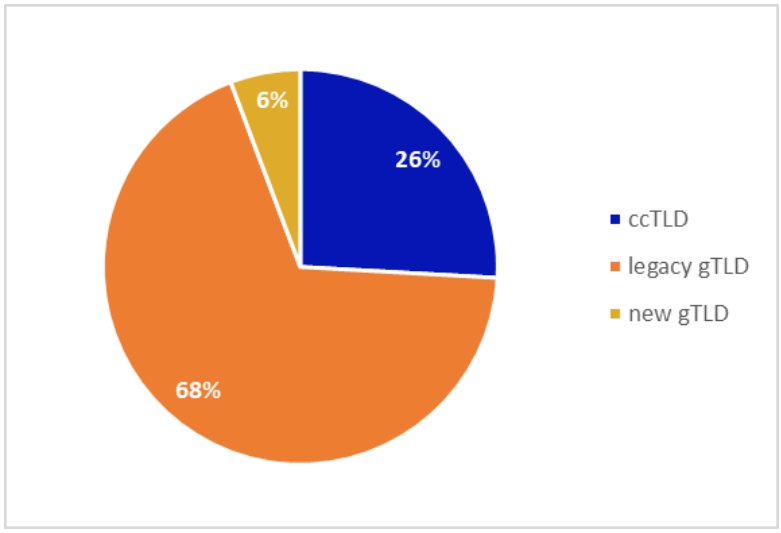


Breaking down the suspicious domains by type of name, 414 (85 %) were 'regular expressions' and 72 (15 %) were 'permutations'. Therefore, a regular expression (i.e. a domain name containing the trade mark within it) was the most common type of cybersquatting.

The average level of cybersquatting was found to be 49 %. Certain sectors, including fashion (66 %), household appliances (64 %), and cars, spare parts and fuels (60 %) suffered from significantly above-average levels, while brands for regular consumer

goods and services (32 %) and professional goods and services (24 %) were less affected.

The distribution of TLDs among the 993 domains studied is shown below.



Legacy gTLDs accounted for 679 (68 %) of the domain names, 257 (26 %) were ccTLDs and 57 (6 %) were new gTLDs. Out of those, 338 legacy gTLDs (50 %), 116 ccTLDs (45 %) and 32 new gTLDs (56 %) were considered suspicious. The fact that the new gTLDs accounted for only a small share of suspicious TLDs could simply reflect the low number of such TLDs compared to the legacy TLDs. At that point in time, the new gTLDs were not a significant source of cybersquatting, although the proportion of suspicious domains among new gTLDs was higher than for either ccTLDs or legacy gTLDs.

A regular expression (i.e. a domain name containing the trade mark within it) was the most common type of cybersquatting, accounting for 85 % of the analysed domains.

Many suspicious domain names were recently registered, with 2019 being the most common registration year for 4 out of the 5 categories and 14 out of the 20 brands with a total of 145, followed by 2018 with 57 and 2017 with 35. Since many domains were registered for 1-year periods, that may simply reflect that cybersquatters let many domains expire (presumably because they did not generate sufficient traffic and revenue).

1.3.2 Qualitative analysis

40 suspicious domain names were selected for qualitative analysis from the domains that were in active use, thus not parked or otherwise passively held.

The key findings were as follows:

- every domain redirected traffic from the legitimate brand as part of internet traffic features;
- 24 domain names (60 %) related to physical or virtual products marketing, while 16 (40 %) related to domain name digital misuse;
- 24 (60 %) domain names offered infringing products or services, 11 (28 %) offered only information and 5 (12 %) offered genuine products;
- 22 (55 %) domain names attracted visitors by projecting legitimacy and 18 (45 %) through both discounts and legitimacy;
- 24 (60 %) domain names generated income through customer payments, 13 (33 %) through pay-per-click and 3 (7 %) through domain name purchase;
- 32 (80 %) domain names were unsecured and 8 (20 %) were secured.

Information about the cybersquatter was not available for 26 of the 40 suspicious domains, having been marked as ‘redacted for privacy’, potentially hindering enforcement actions against the registrant. Information concerning the registrant on WHOIS records is the starting point for dealing with suspicious activity. However, since the General Data Protection Regulation (GDPR) came into force, there is a legal requirement not to publish private data without express consent from individual registrants ([3]).

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

1.4 Conclusions and perspectives

Cybersquatting is a genuine problem for legitimate brands. While not all the domains classified as 'suspicious' represented IPR infringement (e.g. fan sites or sites devoted to criticism), a proportion of cybersquatted sites were used to market counterfeit goods or engage in other illicit activity using the legitimate brand to attract visitors and thereby harming the brand in ways that go beyond counterfeiting.

That could be a particularly serious issue for small and medium-sized enterprises (SMEs), which often lack the resources to actively monitor their web presence to detect cybersquatting and to protect the reputations of their brands.

Further studies of malware and its use online would be needed to further shape the risk/return landscape when cybersquatting is active rather than passive. As technology evolves (e.g. voice to text), new threat pathways will appear, and cybersquatting strategies may evolve to exploit these. Such threats will need to be countered with insight, updated strategies, capabilities by brand owners and supportive service providers.

The findings of this study are of interest to the IPRs experts and internet intermediaries, as well as brand owners and consumers, to highlight the scale of the threat posed by cybersquatters and to provide a basis for fighting the phenomenon more effectively. The study includes a knowledge package to facilitate actions to counter the risk.