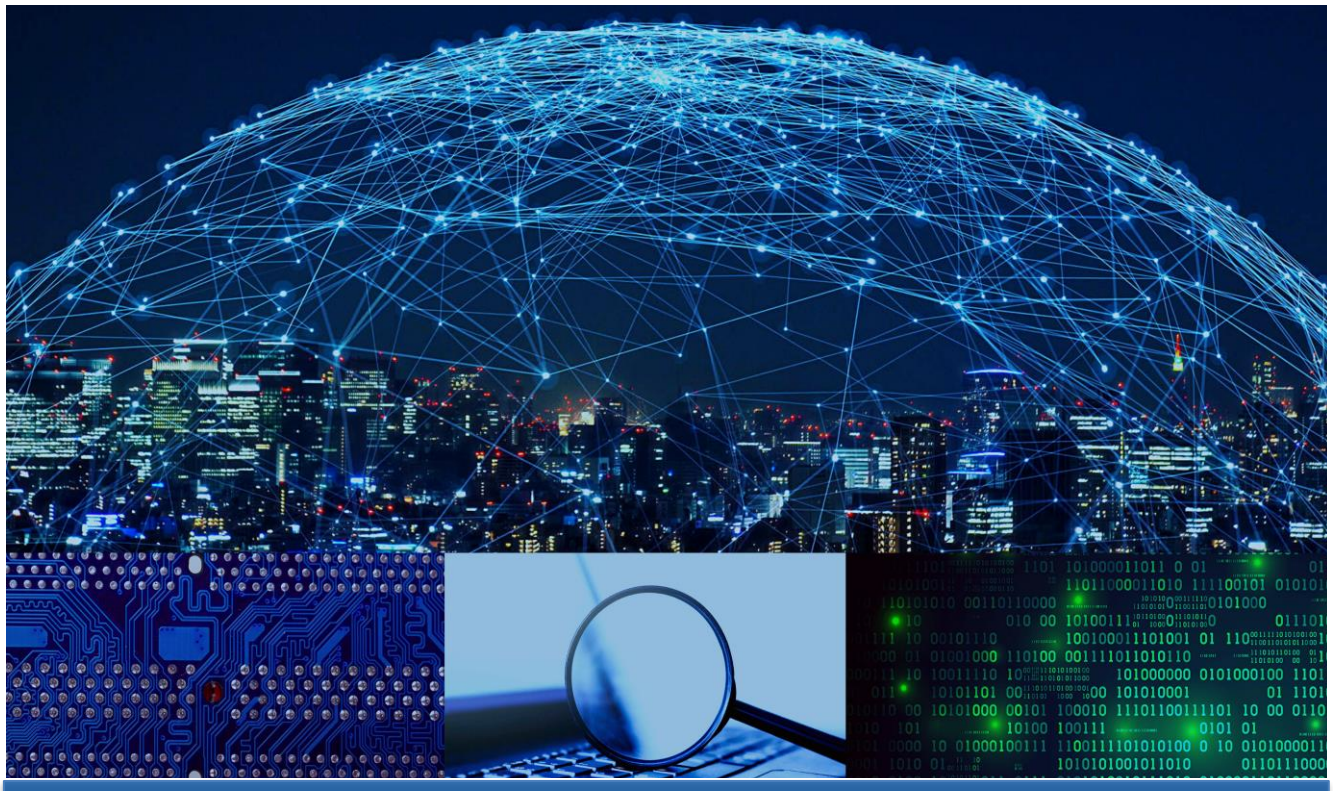
EUIPO
UFFICIO DELL'UNIONE EUROPEA
PER LA PROPRIETÀ INTELLETTUALE

www.euipo.europa.eu

OBIETTIVO CYBERSQUATTING:

VIGILANZA E ANALISI



Maggio 2021

1 Sintesi

1.1 Contesto

Il cybersquatting consiste nella registrazione e/o nell'uso in malafede del marchio di un'altra impresa (o di un altro segno distintivo che serve a identificare tale impresa) in un nome di dominio, senza che sia detenuto alcun diritto legale o interesse legittimo in esso ([1]). Spesso i titolari dei diritti hanno espresso preoccupazione in merito al cybersquatting, in particolare da quando è iniziata l'espansione dei domini di primo livello generici (gTLD) nel 2012.

Il presente studio si prefiggeva lo scopo di quantificare il fenomeno del cybersquatting e descrivere metodi e modelli di business utilizzati dai cybersquatter, fornendo così un punto di partenza per consentire una lotta più efficace a tale fenomeno.

Lo studio ha beneficiato della cooperazione con le parti interessate dell'Osservatorio dell'EUIPO e si è fondato su dati e conoscenze condivisi da parte di esperti in materia di protezione di marchi per le marche selezionate.

1.2 Metodologia

L'individuazione di nomi di dominio interessati dal fenomeno del cybersquatting richiede l'identificazione di nomi di dominio contenenti un marchio o una variazione dello stesso che sia abbastanza simile da ingenerare confusione. Ai fini dell'analisi quantitativa, l'individuazione e l'analisi dei nomi di dominio si sono svolte su un campione di 560 gTLD e 250 domini di primo livello geografici (ccTLD), comprendenti circa 239 milioni di nomi di dominio registrati. L'analisi è stata condotta nel primo trimestre del 2020.

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

L'analisi quantitativa si è concentrata su una selezione di marche, composta da 20 marche tutelate da marchi di proprietà di piccole, medie e grandi imprese e rientranti in diverse categorie di prodotti e servizi. Per motivi di riservatezza, si è proceduto a indicare anonimamente i marchi selezionati e i rispettivi titolari all'interno della presente relazione ([2]). Nello studio si sono individuati usi sospetti dei marchi selezionati in nomi di dominio registrati e si sono analizzate le tecniche a cui ricorrono i cybersquatter per trarre vantaggio dalle marche ideate dai titolari dei marchi.

Nella prima fase, è stata condotta una ricerca all'interno dell'universo dei nomi di dominio registrati allo scopo di identificare i nomi associati alle marche selezionate. A tal fine, si è proceduto all'aggiunta di ulteriori parole chiave ad alcuni nomi di marche ovvero all'esclusione di alcune lettere dopo il nome della marca, al fine di evitare la formazione di parole comuni o di nomi propri che fossero simili alla marca in questione e che avrebbero «inquinato» i risultati della ricerca.

I cybersquatter non sempre registrano nomi di dominio contenenti il marchio completo o il nome intero di una marca, bensì una variante che genera deliberatamente confusione, per esempio adottando una grafia leggermente scorretta o sostituendo una lettera con una cifra. Pertanto, sono state condotte ricerche che riguardavano altresì alcune variazioni dei nomi delle marche. Infine, si è proceduto all'aggiunta di ricerche specifiche per parola chiave al nome della marca, al fine di individuare i nomi di dominio più accurati che si riferiscono a ciascuna marca.

La ricerca ha prodotto un totale di 55 181 nomi di dominio. Nelle fasi successive è stata effettuata un'analisi manuale di un campione aleatorio composto da 100 domini per ciascuna delle 20 marche, per alcune delle quali è stato identificato un numero di domini inferiore a 100. Ne consegue che il numero totale di domini analizzati è stato pari a 1 864, dei quali 993 sono risultati essere collegati alle marche e sono stati oggetto dell'analisi quantitativa sotto descritta.

Nella fase finale dello studio sono stati selezionati 40 domini «sospetti» relativi alle 20 marche oggetto dell'analisi quantitativa e per i quali si è proceduto a un'analisi

([2]) I 20 marchi in questione sono stati identificati in ordine alfabetico, con l'indicazione delle marche dalla A alla T.

qualitativa. L'obiettivo della suddetta analisi era fornire una panoramica dei diversi tipi di modelli aziendali che costituiscono una violazione dei diritti, sulla base dei domini di primo livello (TLD) utilizzati, dei tipi di diritti di proprietà intellettuale (DPI) interessati e delle caratteristiche del traffico su internet. Nello studio si sono analizzati sia i modelli aziendali impiegati da tali domini allo scopo di generare ricavi inducendo i visitatori all'acquisto sia i prodotti e i servizi coinvolti. È stata impiegata una matrice tassonomica del quadro del modello aziendale allo scopo di individuare e dimostrare in modo sistematico le caratteristiche principali di ciascun modello. Questa parte dell'analisi si è basata in parte sulla metodologia sviluppata dall'Ufficio nella relazione Ricerca sui modelli aziendali online che violano i diritti di proprietà intellettuale.

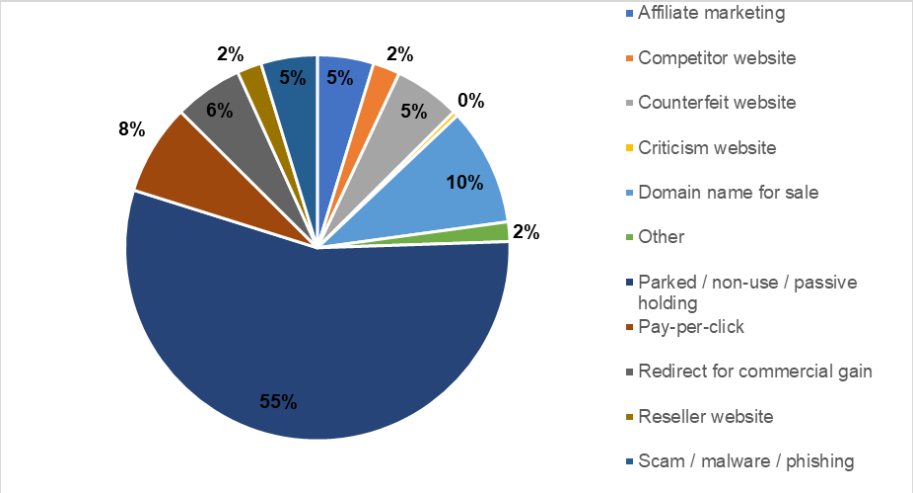
1.3 Risultati

1.3.1 Analisi quantitativa

Poco meno della metà dei 993 nomi di dominio analizzati (486, ossia il 49 %) è risultata «sospetta», mentre i restanti erano di proprietà legittima dei titolari dei marchi o non erano collegati alle marche in questione.

La maggior parte dei 486 domini sospetti (ossia il 55 %) risultano creati ma non sfruttati commercialmente, o comunque non utilizzati in maniera attiva. Il 10 % dei domini figuravano in vendita, mentre il restante risultava impiegato per una serie di attività, la

maggior parte delle quali erano relazionate con siti web che vendono prodotti contraffatti e siti web nei quali si svolgono attività di truffa, phishing o distribuzione di malware.

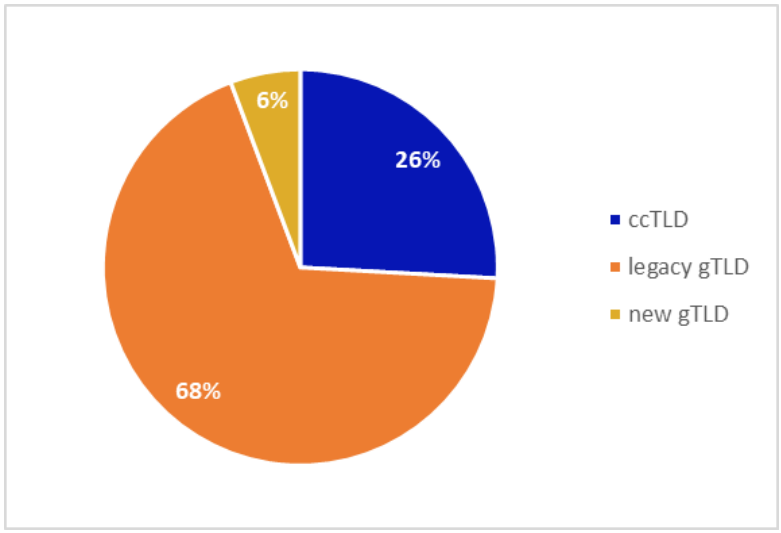


Affiliate marketing	Marketing di affiliazione
Competitor website	Sito web di concorrenti
Counterfeit website	Sito web contraffatto
Criticism website	Sito web dedicato alle recensioni critiche
Domain name for sale	Nome di dominio in vendita
Other	Altro
Parked / non-use / passive holding	Creato ma non sfruttato commercialmente / non in uso / detenzione passiva
Pay-per-click	Pay-per-click
Redirect for commercial gain	Reindirizzamento a fini commerciali
Reseller websit	Sito web del rivenditore
Scam / malware / phishing	Truffa / malware / phishing

Operando una scomposizione dei domini sospetti in base al tipo di nome, è risultato che nel caso di 414 (85 %) nomi si trattava di «espressioni regolari», mentre 72 (15 %) erano «variazioni». Pertanto, le espressioni regolari (ossia i nomi di dominio contenenti il marchio al loro interno) si sono rivelate il tipo di cybersquatting più comune.

Il livello medio di cybersquatting si è attestato al 49 %. Alcuni settori, tra cui la moda (66 %), gli elettrodomestici (64 %), le automobili, i pezzi di ricambio e i combustibili (60 %), hanno visto un livello di cybersquatting significativamente superiore alla media, mentre le marche di prodotti e servizi di consumo corrente (32 %) e di prodotti e servizi professionali (24 %) ne hanno risentito in misura minore.

Di seguito è riportata la distribuzione dei TLD tra i 993 domini che sono stati oggetto di studio.



ccTLD	ccTLD
legacy gTLD	gTLD preesistenti
new gTLD	gTLD nuovi

I gTLD preesistenti corrispondevano a 679 (68 %) nomi di dominio, 257 (26 %) erano ccTLD e 57 (6 %) costituivano nuovi gTLD. Di questi, 338 rappresentavano gTLD preesistenti (50 %), 116 erano ccTLD (45 %) e 32 nuovi gTLD (56 %) erano considerati sospetti. Il fatto che i nuovi gTLD rappresentassero solo una parte marginale dei TLD sospetti potrebbe semplicemente riflettere il numero esiguo di TLD rispetto ai TLD preesistenti. In quel particolare momento, i nuovi gTLD non rappresentavano una fonte importante di cybersquatting, sebbene la percentuale di domini sospetti tra i nuovi gTLD fosse più elevata rispetto ai ccTLD o ai gTLD preesistenti.

Le espressioni regolari (ossia i nomi di dominio contenenti il marchio al loro interno) hanno costituito la tipologia più comune di cybersquatting, rappresentando l'85 % dei domini analizzati.

Di recente sono stati registrati numerosi nomi di dominio sospetti: il 2019 ha rappresentato l'anno in cui si è registrato il maggior numero di nomi di dominio per quattro delle cinque categorie indicate e per 14 delle 20 marche analizzate, con un totale

di 145 nomi di dominio registrati, seguito dal 2018 con 57 nomi di dominio registrati e dal 2017 con 35 registrazioni. Poiché diversi domini sono stati registrati per periodi di un anno, ciò potrebbe semplicemente significare che i cybersquatter ne lascino scadere la validità (presumibilmente perché non hanno generato traffico ed entrate sufficienti).

1.3.2 Analisi qualitativa

Ai fini dell'analisi qualitativa sono stati selezionati 40 nomi di dominio sospetti relativi a domini in uso attivo, che quindi non risultassero creati ma non sfruttati commercialmente o altrimenti detenuti passivamente.

Di seguito sono riportati i principali risultati:

- ogni dominio reindirizzava il traffico dalla marca legittima in quanto parte delle funzionalità del traffico su internet;
- 24 nomi di dominio (60 %) si riferivano alla commercializzazione di prodotti fisici o virtuali, mentre 16 nomi di dominio (40 %) erano relazionati all'uso improprio digitale degli stessi;
- 24 (60 %) nomi di dominio offrivano prodotti o servizi che costituivano una violazione di diritti, 11 (28 %) erano di semplice natura informativa e 5 (12 %) offrivano prodotti autentici;
- 22 nomi di dominio (55 %) richiamavano visitatori perché percepiti come legittimi; 18 nomi di dominio (45%) erano percepiti come legittimi e convenienti a fronte degli sconti offerti;
- 24 nomi di dominio (60 %) generavano entrate attraverso pagamenti da parte dei clienti, 13 nomi di dominio (33 %) attraverso la modalità «pay-per-click» e 3 nomi di dominio (7 %) producevano entrate mediante l'acquisto di nomi di dominio;
- 32 nomi di dominio (80 %) non erano protetti, mentre 8 nomi di dominio (20 %) godevano di protezione.

Le informazioni relative al cybersquatter non sono risultate disponibili per 26 dei 40 domini sospetti, essendo state contrassegnate come «omesse per questioni connesse alla tutela della vita privata», impedendo potenziali misure di contrasto nei confronti del dichiarante. Le informazioni riguardanti il dichiarante sui registri WHOIS

costituiscono il punto di partenza per la gestione delle attività sospette. Tuttavia, dall'entrata in vigore del regolamento generale sulla protezione dei dati (RGPD),sussiste l'obbligo giuridico di non pubblicare dati privati senza l'esplicito consenso da parte dei singoli dichiaranti ([3]).

1.4 Conclusioni e prospettive

Il cybersquatting costituisce un problema reale per le marche legittime. Sebbene non tutti i domini classificati come «sospetti» costituissero una violazione dei DPI (per esempio siti dedicati ai sostenitori o siti dedicati alle recensioni critiche), una percentuale dei siti interessati dal fenomeno del cybersquatting veniva utilizzata per commercializzare merci contraffatte o intraprendere altre attività illecite ricorrendo alla marca legittima per richiamare visitatori e quindi danneggiare la marca mediante attività che vanno oltre la contraffazione.

Si potrebbe trattare di una questione particolarmente grave per le piccole e medie imprese (PMI), le quali spesso non dispongono delle risorse per monitorare attivamente la propria presenza sul web al fine di rilevare attività di cybersquatting e proteggere la reputazione delle proprie marche.

Emerge la necessità di ulteriori studi concernenti i malware e il relativo utilizzo online, al fine di definire ulteriormente lo scenario concernente il rapporto tra i rischi e il rendimento quando si è in presenza di cybersquatting attivo anziché passivo. Con l'evoluzione della tecnologia (per esempio, i servizi che consentono la conversione da voce a testo), emergeranno nuove minacce e le strategie di cybersquatting potrebbero evolversi allo scopo di sfruttare tali possibilità. Queste minacce dovranno essere affrontate con perspicacia, ricorrendo a strategie aggiornate, alle capacità dei titolari delle marche e al sostegno da parte dei fornitori di servizi.

I risultati che emergono dal presente studio costituiscono un elemento di interesse per gli esperti di DPI e gli intermediari di internet, nonché per i proprietari e i consumatori di marche, al fine di evidenziare la portata della minaccia costituita dai cybersquatter e

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

fornire un punto di partenza per garantire una lotta più efficace contro questo fenomeno. Lo studio comprende un pacchetto di conoscenze volte a facilitare le azioni destinate a contrastare tale rischio.