

PONIENDO EL FOCO EN LA CIBEROCUPACIÓN: SEGUIMIENTO Y ANÁLISIS



Mayo de 2021

1 Resumen ejecutivo

1.1 Contexto

La ciberocupación implica el registro de mala fe o el uso, en un nombre de dominio, de la marca de otra empresa (o de otro signo que se haya convertido en un identificador distintivo para dicha empresa), sin tener derechos legales ni intereses legítimos sobre dicho nombre de dominio ⁽¹⁾. Los titulares de derechos han expresado a menudo su preocupación por la ciberocupación, especialmente desde la expansión de los dominios genéricos de nivel superior (gTLD) iniciada en 2012.

El objetivo de este estudio era cuantificar el fenómeno de la ciberocupación y describir los métodos y los modelos de negocio empleados por los «ciberocupas», y proporcionar así una base para luchar más eficazmente contra dicho fenómeno.

El estudio se benefició de la cooperación con las partes interesadas del Observatorio de la EUIPO y se basó en datos y conocimientos compartidos por los expertos en protección de marcas de una selección de marcas.

1.2 Metodología

La detección de nombres de dominio ciberocupados requiere identificar nombres de dominio que contengan una marca o una variación similar a la misma que induzca a confusión. Para el análisis cuantitativo, la detección y el análisis de los nombres de dominio se llevaron a cabo con respecto a 560 gTLD y 250 dominios de nivel superior correspondiente a código de país (ccTLD), que abarcan aproximadamente 239 millones de nombres de dominio registrados. El análisis se llevó a cabo en el primer trimestre de 2020.

<https://www.icann.org/resources/pages/cybersquatting-2013-05-03-es>

El análisis cuantitativo se centró en una selección de veinte marcas protegidas, propiedad de pequeñas, medianas y grandes empresas para diferentes categorías de productos y servicios. Por motivos de confidencialidad, las marcas seleccionadas, así como sus titulares, han sido anonimizados en este informe ⁽²⁾. El estudio identificó usos sospechosos de las marcas seleccionadas en nombres de dominio registrados y analizó las técnicas utilizadas por los «ciberocupas» para aprovechar las marcas creadas por los titulares de dichas marcas.

En el primer paso, se llevó a cabo una búsqueda en todo el universo de nombres de dominio registrados para identificar aquellos asociados a las marcas seleccionadas. Para este ejercicio, se añadieron palabras clave adicionales a algunas marcas, o se excluyeron algunas letras después del nombre de la marca, con el fin de evitar la formación de palabras comunes o nombres propios similares a la marca en cuestión que pudieran «contaminar» los resultados de la búsqueda.

Los «ciberocupas» no siempre registran nombres de dominio que contienen la marca o el nombre comercial completos, sino una variante deliberadamente confusa, como un pequeño error ortográfico o la sustitución de una letra por una cifra. Por lo tanto, también se realizaron búsquedas con determinadas permutaciones en las denominaciones de las marcas. Por último, se añadieron a las marcas búsquedas con palabras clave específicas para encontrar los nombres de dominio más precisos relacionados con cada marca.

La búsqueda arrojó un total de 55 181 nombres de dominio. En etapas posteriores, se analizó manualmente una muestra aleatoria de cien de estos dominios para cada una de las veinte marcas. Para algunas marcas, el número de dominios identificados fue inferior a 100, por lo que el número total de dominios analizados fue de 1 864. De dichos dominios, 993 se consideraron que estaban relacionados con las marcas y fueron objeto del análisis cuantitativo que se indica a continuación.

En la fase final del estudio, se seleccionaron cuarenta dominios «sospechosos» que estaban relacionados con las veinte marcas objeto del análisis cuantitativo a fin de realizar un análisis cualitativo. El objetivo de este análisis era ofrecer una visión general

⁽²⁾ Las veinte marcas se identificaron por orden alfabético, de la A a la T.

de los diferentes tipos de modelos de negocio que vulneran derechos de propiedad intelectual, sobre la base de los dominios de nivel superior (TLD) utilizados, los tipos de derechos de propiedad intelectual (DPI) implicados y las características del tráfico de internet. El estudio analizó los modelos de negocio utilizados por estos dominios para generar ingresos al inducir a los visitantes a realizar una compra, así como los productos y servicios que abarcaban. Se utilizó una matriz taxonómica del marco de los modelos de negocio para identificar y demostrar sistemáticamente las principales características de cada modelo de negocio. Esta parte del análisis se basó parcialmente en la metodología desarrollada por la Oficina en el informe [«Research on Online Business Models Infringing Intellectual Property Rights»](#) (Investigación sobre modelos de negocio en línea que vulneran derechos de propiedad intelectual).

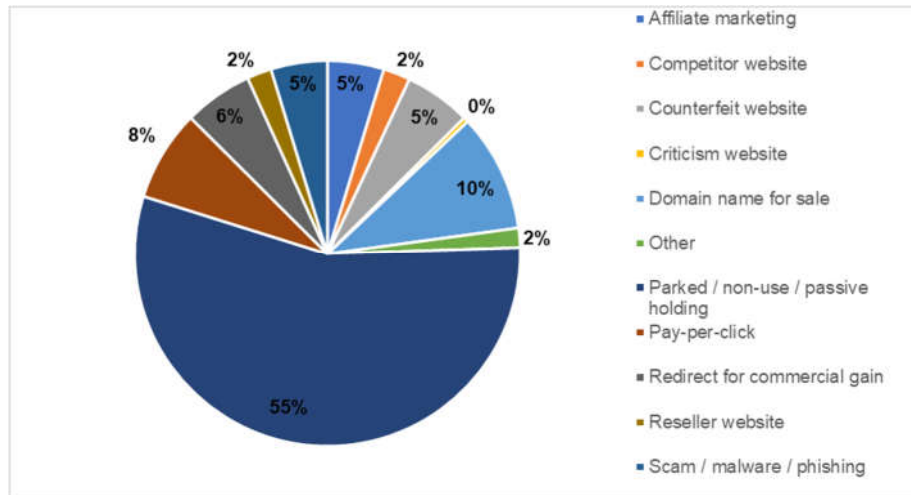
1.3 Resultados

1.3.1 Análisis cuantitativo

De los 993 nombres de dominio analizados, algo menos de la mitad, 486, se consideraron «sospechosos» (un 49 %); el resto era propiedad legítima de los titulares de las marcas o no estaban relacionados con las marcas en cuestión.

La mayoría de los 486 dominios sospechosos (el 55 %) estaban aparcados o, por alguna razón, no se utilizaban activamente. El diez por ciento de los dominios estaba a la venta, mientras que el resto se usaba para diversas actividades, de las cuales la mayoría

consistía en sitios web que vendían falsificaciones y sitios web dedicados a estafas, suplantación de identidades o distribución de programas malignos.

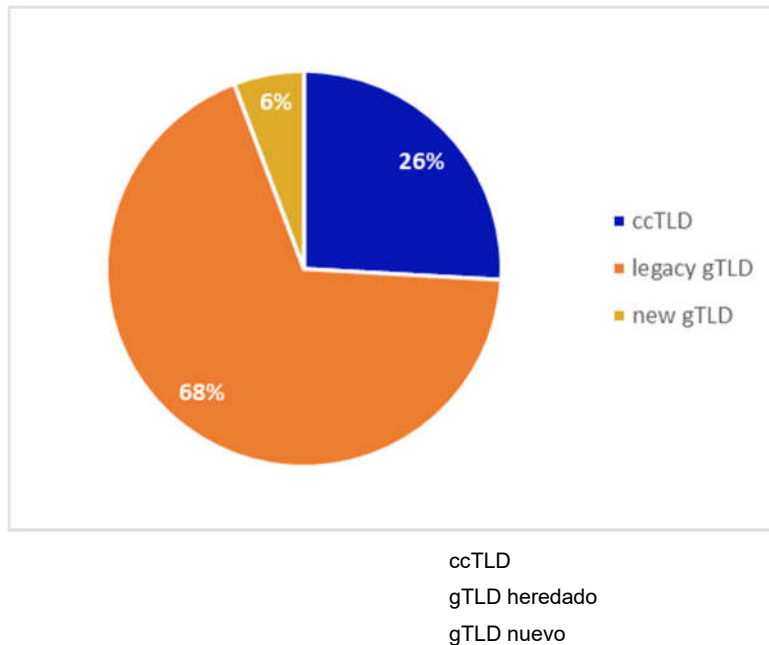


- Comercialización de afiliados
- Sitio web del competidor
- Sitio web falsificado
- Sitio web de críticas
- Nombre de dominio a la venta
- Otros
- Aparcados, no utilizados o tenencia pasiva
- Pago por clic
- Redireccionamiento para obtener beneficios comerciales
- Sitio web del revendedor
- Estafa, programa maligno o suplantación de identidad (*phishing*)

Al desglosar los dominios sospechosos por tipo de nombre, 414 (el 85 %) eran «expresiones regulares» y 72 (el 15 %) eran «permutaciones». Por lo tanto, la expresión regular (es decir, un nombre de dominio que contiene la marca) fue el tipo más común de ciberocupación.

Se observó que el nivel medio de ciberocupación era del 49 %. Algunos sectores, como el de la moda (66 %), los electrodomésticos (64 %) y los automóviles, las piezas de recambio y los combustibles (60 %), experimentaron niveles significativamente superiores a la media, mientras que las marcas de bienes y servicios de consumo habitual (32 %) y de bienes y servicios profesionales (24 %) se vieron menos afectadas.

A continuación, se muestra la distribución de los dominios de primer nivel entre los 993 dominios estudiados.



679 de los nombres de dominio (el 68 %) eran gTLD heredados; 257 (el 26 %) eran ccTLD y 57 (el 6 %) eran gTLD nuevos. De ellos, 338 eran gTLD heredados (50 %), 116 eran ccTLD (45 %) y se consideraron sospechosos 32 gTLD nuevos (56 %). El hecho de que los gTLD nuevos solo representaran una pequeña proporción de los TLD sospechosos podría simplemente reflejar el escaso número de dichos TLD en comparación con los TLD heredados. En ese momento, los gTLD nuevos no eran una fuente significativa de ciberocupación, aunque la proporción de dominios sospechosos entre los gTLD nuevos era mayor que para los ccTLD o los gTLD heredados.

Una expresión regular (es decir, un nombre de dominio que contiene una marca) fue el tipo más común de ciberocupación, y representó el 85 % de los dominios analizados.

Recientemente se registraron muchos nombres de dominio sospechosos, siendo 2019 el año de registro más frecuente para 4 de las 5 categorías y 14 de las 20 marcas, con un total de 145, seguido de 2018 con 57 y 2017 con 35. Dado que muchos dominios se registraron por períodos de un año, ello puede simplemente reflejar que los

«ciberocupas» dejaron que muchos dominios expiraran (presumiblemente porque no generaron suficiente tráfico e ingresos).

1.3.2 Análisis cualitativo

Se seleccionaron cuarenta nombres de dominio sospechosos para el análisis cualitativo de los dominios que estaban en uso activo, por lo que no estaban aparcados ni mantenidos de forma pasiva.

Las principales conclusiones fueron las siguientes:

- cada dominio redirigía el tráfico desde la marca legítima como parte de las funciones del tráfico de internet;
- 24 nombres de dominio (el 60 %) estaban relacionados con la comercialización de productos físicos o virtuales, mientras que otros 16 (el 40 %) estaban relacionados con el uso indebido digital de nombres de dominio;
- 24 nombres de dominio (el 60 %) ofrecían productos o servicios infractores; otros 11 (el 28 %) ofrecían únicamente información y 5 (el 12 %) ofrecían productos auténticos;
- 22 nombres de dominio (el 55 %) atraían a los visitantes al proyectar legitimidad y otros 18 (el 45 %) mediante descuentos y legitimidad;
- 24 nombres de dominio (un 60 %) generaron ingresos a través de pagos de clientes, 13 (un 33 %) a través de pagos por clic y 3 (el 7 %) a través de la compra de nombres de dominio;
- 32 nombres de dominio (un 80 %) no estaban protegidos y 8 (un 20 %) sí lo estaban.

La información sobre el «ciberocupa» no estaba disponible en veintiséis de los cuarenta dominios sospechosos, ya que se había seleccionado «proteger la privacidad», lo que podría dificultar la adopción de medidas coercitivas contra el solicitante de registro. La información relativa al solicitante de registro en los registros WHOIS es el punto de partida para abordar las actividades sospechosas. Sin embargo, desde la entrada en vigor del Reglamento General de Protección de Datos (RGPD), existe la disposición

legal de no publicar datos privados sin el consentimiento expreso de los solicitantes de registro individuales ⁽³⁾.

1.4 Conclusiones y perspectivas

La ciberocupación es un verdadero problema para las marcas legítimas. Aunque no todos los dominios clasificados como «sospechosos» representaron una vulneración de los DPI (por ejemplo, sitios de fans o sitios dedicados a la crítica), una parte de los sitios web ciberocupados se utilizaron para comercializar productos falsificados o para participar en otras actividades ilícitas utilizando la marca legítima para atraer visitantes y, de este modo, perjudicar a la marca de formas que van más allá de la falsificación.

Ello podría ser un problema especialmente grave para las pequeñas y medianas empresas (pymes), que a menudo carecen de los recursos necesarios para supervisar activamente su presencia en la web con el fin de detectar la ciberocupación y proteger el renombre de sus marcas.

Se necesitarían más estudios sobre programas malignos y su uso en línea para definir mejor el panorama de riesgos o de beneficios cuando la ciberocupación sea activa y no pasiva. A medida que la tecnología evolucione (por ejemplo, el reconocimiento de voz), aparecerán nuevas vías de amenazas y las estrategias de ciberocupación pueden evolucionar para aprovecharlas. Dichas amenazas tendrán que contrarrestarse con ideas, estrategias actualizadas, capacidades de los titulares de marcas y el apoyo de los proveedores de servicios.

Las conclusiones de este estudio se consideran interesantes para los expertos en DPI y los intermediarios de internet, así como para los titulares de marcas y los consumidores, a fin de poner de relieve la magnitud de la amenaza que plantean los «ciberocupas» y proporcionar una base para luchar más eficazmente contra dicho fenómeno. El estudio incluye un paquete de conocimientos para facilitar las medidas destinadas a contrarrestar el riesgo.

<https://www.euodns.com/blog/WHOIS-database-gdpr-compliance>