Cómo combatir el problema de *whack-a-mole* en los casos de *webs copycat*

Sumario

Las *webs copycat* plantean un problema *whack-a-mole*: cada retirada suele irseguida de la aparición inmediata de nuevas webs fraudulentas similares. Para combatirlo eficazmente es esencial combinar monitorización continua, la preservaciónde la prueba y una actuación rápida. También resulta clave activar de forma coordinada distintas vías de *enforcement* frente a registradores, proveedores de *hosting*, medios de pago, buscadores y plataformas. Las actuaciones aisladas suelen ser insuficientes y poco sostenibles en el tiempo. La respuesta debe integrarse en una estrategia global de protección de marca online.

POR

Patricia Guillén

Baylos IP abion

El título de este artículo exige, en primer lugar, explicar dos conceptos en inglés que son muy habituales en la jerga de protección de marca online y que no tienen una traducción fácil al castellano:

- Las **webs *copycat***, webs "*copiotas*" de réplica o imitación, son sitios web creados en su mayoría con IA para replicar la apariencia, identidad y funcionamiento de la web oficial de una empresa. La réplica puede afectar, tanto al nombre de dominio (normalmente con palabras añadidas o errores ortográficos), como al uso de marcas, diseños, fotografías, etc. Todo ello con el objetivo de, en la mayoría de los casos, captar datos personales, atraer tráfico a publicidad o, en última instancia, estafar a los internautas sin llegar a vender nada.

- Un problema ***whack-a-mole***, traducido literalmente como "*golpea al topo*", describe una situación en la que, cada vez que se resuelve o elimina un problema concreto, aparece otro igual o muy similar en otro lugar, obligando a actuar de forma repetida sin conseguir una solución definitiva.

Aclarado lo anterior, cualquiera que esté familiarizado con la **protección de marca en el entorno online** sabe de lo que estamos hablando: combatir los casos de suplantación se convierte en una carrera de fondo que parece no tener fin. Cada vez que se cierra una web, salen otras, obligando a los titulares a invertir tiempo y recursos para eliminar (o al menos minimizar) una realidad fraudulenta que es compleja.

La monitorización continua es clave para detectar nuevas *webs copycat* de forma temprana.

Entonces, **¿qué podemos hacer para combatir este problema?** A continuación incluimos algunos consejos que ayudan a combatir eficazmente este fenómeno:

1. Monitorización y detección temprana

Conocer el problema y su magnitud es el primer paso para poder solucionarlo o, al menos, gestionarlo apropiadamente. Contar con un **sistema monitorización continua** permite detectar de forma ágil nuevos registros de dominio, resultados en buscadores, marketplaces, redes sociales y campañas publicitarias. A nivel de dominios, existen opciones de vigilancia preventiva (*early warning systems*) que detectan nuevos registroscoincidentes con la palabra o palabras vigiladas, variaciones tipográficas y cambios relevantes en WHOIS/DNS. Por ejemplo, es posible recibir una alerta si un dominio altamente similar al que tú usas activa registros MX para potenciales acciones de phishing. A nivel contenido, es posible rastrear marcas, logos o imágenes dentro del contenido web, así como el favicon, generalmente copiado en las webs *copycat* para aumentar la apariencia de web original.

Preservar la prueba antes del *take down* es determinante para poder ejercitar acciones posteriores.

2. Preservación de la prueba y actuación inmediata

En este tipo de casos, la rapidez es un factor determinante. Una sola web copycat puede causar un **daño significativo en un periodo muy breve**. Sin embargo, actuar con rapidez no debe significar actuar sin preservar previamente la prueba. Por ello, antes de solicitar un *take down* de la web infractora conviene documentar de forma exhaustiva el contenido y funcionamiento del sitio. Esto incluye, entre otros, la obtención decertificados web (*safe stamping*) con el que poder acreditar el contenido web, o la prueba relativa a medios de pago aceptados o redes sociales vinculadas. En otras palabras, aunque muchas veces no lleguemos a saber quién hay detrás de esta web, sídebemos identificar todas las vías posibles para hacer enforcement. Estascomprobaciones, que pueden realizarse en minutos, son determinantes para fundamentar una denuncia penal, una demanda civil o acreditar la mala fe en un procedimiento de recuperación de domino ante la WIPO.

3. Acumulación de vías de *enforcement* y actuación frente a intermediarios

Incluso con una estrategia sólida implementada, conseguir cerrar una web *copycat* no es darle a un botón. Una vez obtenida la prueba, se deben iniciar **procesos de *take down*de forma acumulada** por cada una de las infracciones (marca, diseños, derechos de autor) frente a registradores, proveedores de

hosting, plataformas, medios de pago o buscadores. La eficacia de la respuesta dependerá, en buena medida, del nivel de *compliance* de los intervinientes. Por ejemplo, una acción exitosa ante el registrador puede suspender un dominio; una acción exitosa ante un proveedor de servicios de pago puede impedir la monetización de la actividad fraudulenta; o una acción exitosa ante una red social puede reducir sustancialmente el tráfico a esa web.

La estrategia más eficaz será, por tanto, aquella que **combine distintas vías de *enforcement*** hasta conseguir el resultado.

4. La estrategia global como única forma de protección eficiente

Como decíamos, la aparición de este tipo de webs rara vez es un fenómeno aislado, sino una situación *whack-a-mole,* un patrón recurrente que se repite, normalmente a gran velocidad. Por ello las acciones individuales resultan insuficientes y a menudo también insostenibles a nivel de dedicación y costes. Por ello, es conveniente establecer una estrategia global de protección de marca y contenidos digitales que **dificulte de forma sostenida la continuidad de la actividad infractora**, bloqueando su operatividad y si no es posible, al menos, reduciendo su visibilidad y capacidad de monetización.

Una estrategia global de protección de marca online permite combatir el fenómeno de forma más eficaz y sostenible que las actuaciones aisladas.