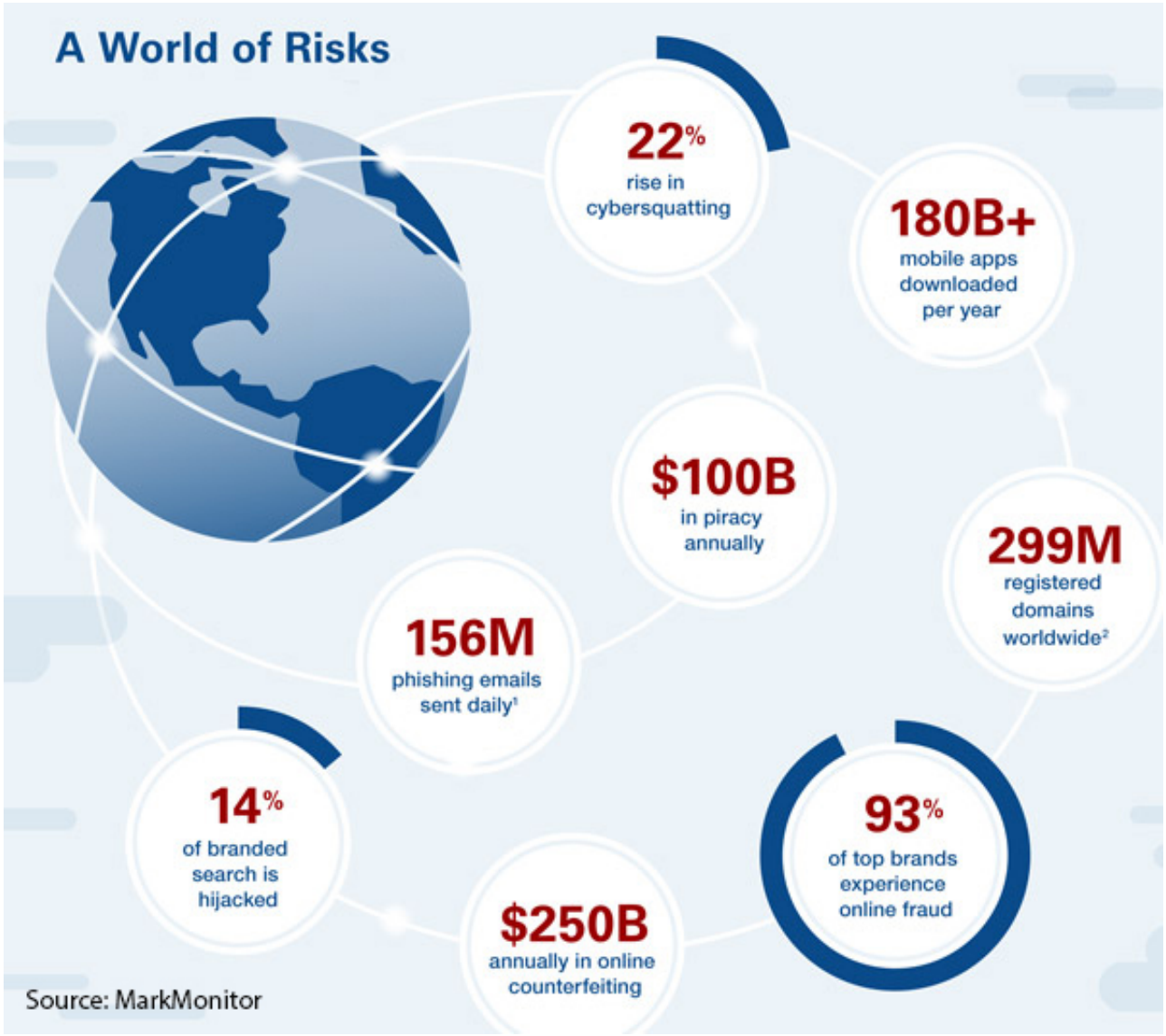
Online Brand Protection: 5 Questions with MarkMonitor's Simon Whitehouse

Author : Jerome McDonnell

Date : May 19, 2016



Brand abuse is big business. It's estimated that **brands** lost over $350 billion last year to online

attacks—and the risks are constantly evolving. While any **brand** can be vulnerable to attack, the more recognizable and powerful the **brand**, the more attractive a target it is.

Following last month's summit in New York on the future of intellectual property and **digital brand** protection strategies, **brand channel** discussed **brand** protection with **Simon Whitehouse**, **Senior Director** at MarkMonitor, a leader in **brand** security.

brandchannel: Do you think enough brands know if or how they're being targeted or abused?

Simon Whitehouse: There is a growing awareness from **brands** across industries on the importance of online **brand** protection—particularly in today's omnichannel environment. Organizations recognize that having a comprehensive **digital brand** protection strategy ensures they are able to protect both themselves (for example, their reputation and bottom line) and their customers, who are likely to be affected by the availability of counterfeit goods online.

bc: How should brands go about implementing a strong digital brand-protection strategy?

Whitehouse: Online **brand** impersonators and counterfeiters create **brand** confusion by interfering with a **brand**'s **digital** promotions, intercepting web traffic and threatening e-commerce revenues. One of the first things to do is to be proactive and keep fraudsters from coming between a **brand** and its customers. By addressing their deceptive tactics, marketers can reclaim web traffic and revenues, and improve ROI on **digital marketing** initiatives.

It's also crucial that organizations don't overlook the threats of **brand** impersonation, **brand** fraud and counterfeit goods in the rapidly evolving landscape of **digital** channels. These channels, including **social** media and mobile apps, are becoming an increasingly important part of people's personal and business lives. With **marketing** ROI at risk, **marketing** executives must make **social** and mobile essential components of their **brand** protection strategy.

bc: Are particular industries or brands more vulnerable than others?

Whitehouse: While counterfeiting, **brand** abuse and domain squatting can affect **brands** in most industries, we're finding an increased prevalence in the fashion and luxury goods space. Luxury **brands** have historically been more hesitant in embracing e-commerce as part of their sales strategies, but now as more and more of these **brands** develop their web presence, the prevalence of counterfeiting luxury goods online is growing. In fact, according to the 2015 MarkMonitor Online Barometer, almost 25 percent of consumers bought a product online that turned out to be fake, with fashion, footwear, electronics and **digital** content being the most prevalent product categories.

bc: How are protection and enforcement strategies adapting to new threats?

Whitehouse: We often see a single counterfeiter operating 40 percent to 60 percent of all rogue sites targeting a particular **brand** and selling counterfeit versions of that **brand**'s wares.

Shutting down these networks is an effective way to disrupt, and even potentially cripple, the counterfeiter's business. But fighting these networks manually is time-consuming and ineffective. There's a new strategy that uses technology to focus on the scale of the problem, which is quite effective in the fashion and luxury **brand** industry.

By identifying clusters of sites that display the same characteristics, **brands** can apply one injunction to shut down multiple rogue sites as well as future rogue sites that can be tied back to the original network. This approach maximizes the impact and the ROI of litigation.

This new technology can identify a larger volume of sites, zeroing in on clusters by analyzing data such as nonvisible content, external site associations and visible content (e.g., prices and graphics).

Gathering rogue sites' "fingerprints" cost-effectively speeds the investigative phase of litigation and lays the groundwork to identify additional sites that pop up after the first round of domain names are seized. As a result, **brand** owners can determine the true scope of infringement and maximize the impact of their litigation investments.

In terms of emerging threats, **brands** are developing and bolstering their **brand** protection efforts around **social** media, recognizing that these channels can be used to mislead consumers through fraud or counterfeiting—either through fake pages or unauthorized use of copyrighted materials and trademarks.

To combat instances of **brand** misuse or misappropriation, solid strategies are needed. Typically these include proactively registering a **brand** across **social** media platforms, adopting tools that can automatically monitor **social** media for impersonation and the misuse of **brands** and trademarks, and acting on cases of misuse or abuse once they have been identified.

bc: So what's the story with generic top-level domains (gTLDs)?

Whitehouse: Since the launch of the gTLDs three years ago, over 800 new generic name spaces have been made available in which to register domains, enabling organizations to have sites like your**brand**.clothing, your**brand**.london and your**brand**.cloud. The objective is to give people and organizations the potential to build targeted sites with direct navigation to the sites.

2015 closed with a total of 11.2 million new gTLD registrations with .xyz, .top, .wang, .win and .club being the top five in terms of total registrations.

The sheer number of new gTLDs being launched means it no longer makes business sense to register every key **brand** term in every new extension. This may force a change in approach to online **brand** protection strategies, from one based on traditional defensive domain registrations, to one that monitors this larger internet namespace for **brand** abuse. Ideally this should involve **brand** protection, legal and risk management personnel. This collaboration will assist **brands** in developing policies to detect, police and mitigate domains that infringe on company trademarks and steal their website traffic.

//