World
Trademark
Review™

The Deep Web, darknets, Bitcoin and brand protection

MarkMonitor Inc
Akino Chikada

Online Brand Enforcement 2016

Protecting Your Trademarks in the Electronic Environment

This article first appeared in *Online Brand Enforcement: Protecting Your Trademarks in the Electronic Environment 2016*, a supplement to *World Trademark Review*, published by Globe Business Media Group – IP Division. To view the guide in full, please go to www.WorldTrademarkReview.com

Contributing firm
MarkMonitor Inc

The Deep Web, darknets, Bitcoin and brand protection

Author
Akino Chikada

Brand owners seeking to protect their intellectual property online face a new front in the digital world: the Deep Web and the darknets contained within it.

Abuse in the Deep Web can be broad and hidden, with cybersquatters and fraudsters trying to ply their trade. However, once detected, there are means to identify the perpetrators and to enforce IP rights. The anonymity and hidden nature of a darknet allow under-the-radar trade in mass quantities of counterfeit goods alongside illicit drugs and weapons, and present special challenges to law enforcement agencies and brand owners.

Understanding the internet landscape

The Internet is divided into two sections. The 'Surface Web' is composed of regular websites that are indexed and searched with standard search engines. However, this represents only 4% of the Internet. The remaining 96% is a vast, uncharted ocean known as the 'Deep Web'. This is comprised of websites that are not indexed by any search engines. In other words, a standard search engine will not access the content of 96% of the Internet – as with an iceberg, most of the content is hidden below the surface, on un-indexed websites. When you browse the Internet, you are really just floating on the surface. Underneath the surface, trillions of pages exist that the search engines never see.

Darknets, unlike the Deep Web, are networks that overlay the public Internet and can be accessed only via specific software. There are two types of darknet: friend-to-friend or peer-to-peer networks (which are used for file sharing) and large, popular anonymous networks such as Tor, Freenet and I2P.

What is in the Deep Web?

The Deep Web is estimated to be 500 times the size of the Surface Web, containing more than 7,500 terabytes of content. So, why is this content hidden from search engines? Much content remains un-indexed for legitimate reasons, such as a corporate internet behind a firewall. Most of the content on social media sites such as Facebook and Twitter is hidden behind a log-in page. There are also vast databases of information in places such as the US Patent and Trademark Office that are not indexed.

There is also a lot of suspicious content on the Deep Web, which includes websites that deliberately hide below the surface since they are selling counterfeit or grey-market goods. Additionally, there are phishing sites that collect user credentials and sites disseminating malware that deliberately try to obfuscate their existence. The Deep Web includes peer-to-peer sites where piracy takes place and marketplaces for counterfeits and unauthorised goods. Further, fraudulent social media posts use brand impersonation to trap unwary consumers into disclosing personal information. Responsible marketplaces and social media sites try to keep their sites clean and safe, but the fraudsters are always trying to find ways to insert themselves.

Defeating fraudsters in the digital world requires disrupting both their means of distribution and their ability to promote themselves. They promote themselves to consumers by directing people to the Deep Web via social media, websites, mobile apps, page searches, page search ads and phishing or spam emails.

What is a darknet?

A darknet is, by definition, part of the Deep Web. Within a darknet, both visitors and publishers are entirely anonymous. Anonymity is achieved by using tools such as Tor, I2P and Tails.

Tor is free software which enables anonymous communication. It was originally developed in the mid-1990s by the US Naval Research Laboratory and today 2.5 million people access Tor on a daily basis. It is used by privacy advocates who do not want their online actions tracked. People searching for dangerous and sensitive information take advantage of Tor's anonymity. They include journalists, law enforcement agencies and criminals.

Downloading Tor takes just a couple of minutes on www.torproject.org (see Figure 1).

Accessing underground marketplaces

Tor enables anonymous search for specific goods, both legitimate and illegitimate. Websites such as deepdotweb.com provide links to some of the more popular marketplaces.

The most popular items sold on these underground marketplaces are drugs – both illicit drugs (eg, heroin, methamphetamines and cocaine) and prescription pharmaceuticals. Personal account and financial information is traded. Pirated content is distributed. Counterfeit goods are sold openly, often in massive quantities. Think of something illegal and it is most likely available on darknet marketplaces. The threats to intellectual property are wide and varied.

Some underground marketplaces are very sophisticated and have many of the features found in well-known marketplaces on the Surface Web. They provide seller ratings, seller profiles, order history and online discussion groups to share information about the products (see Figure 2).

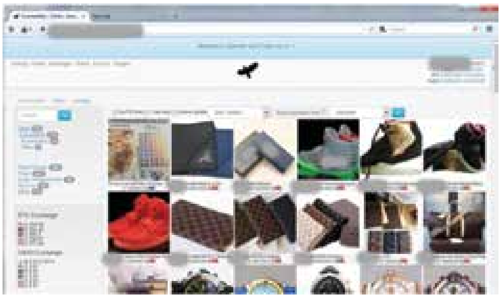
A typical Tor marketplace includes thumbnails of counterfeit or grey-market goods, as well as the exchange rate for Bitcoin or Dash – the popular cryptocurrencies used for transactions. Marketplaces exist that are dedicated to (among other items) pirated software, child pornography, luxury goods, pharmaceuticals and counterfeits.

Chat forums and darknet discussion

A darknet typically includes a range of channels where criminals and hacktivists exchange tips. Depending on their industry, brand owners should consider taking proactive steps to monitor these discussions in order to determine the threats that they pose. This requires the creation of cover stories and fake

FIGURE 1: Downloading Tor

FIGURE 2: A typical Tor marketplace



personas, so partnering with an experienced professional organisation is strongly advised.

Perhaps one of the more troubling aspects of darknets is the sale of personal information, including bank account credentials, credit card information and other kinds of personal financial information that hackers and phishers have acquired.

What role does Bitcoin play and how does it work?

Many darknet sites use Bitcoin or Dash as private digital currencies to facilitate their transactions. A number of different cryptocurrencies are in circulation, but Bitcoin is the one that seems to be most popular with these sites.

Bitcoin is truly fascinating in the way that it works. It is an anonymous currency that uses peer-to-peer technology and has no central banking authority. This means that users can transact directly without needing an intermediary. It is an instrument of alternative finance which has emerged outside of the traditional financial system.

As of August 2015, over 14 million bitcoin were in circulation. The value of 1 bitcoin fluctuated between $223 and $309 over the course of 2015.

There are a number of advantages to consumers using Bitcoin for transactions, and these same features make it more challenging to enforce against brand infringement. Since Bitcoin is not controlled by any central authority, it lives outside the established financial system and is decentralised and anonymous. Transactions are not associated with names, addresses or any identifying information.

There are obvious benefits for people using this form of payment for illegal underground transactions. With no means to trace purchases through credit card records or fiscal reporting regulations, both buyers and sellers are free of government regulation and oversight. Law enforcement agencies cannot follow a money trail to the source of the activity.

Brand owners cannot ignore the fact that an increasing amount of commerce, both legitimate and otherwise, is being facilitated by the anonymous nature of Bitcoin. A growing list of businesses – from coffee shops to florists – now accept payment in Bitcoin.

Sources of IP abuse in the Deep Web

Brands are at risk in the Deep Web. Even though sites are not indexed, they can be reached in a number of ways. Many consumers are not even aware that they have been redirected to a Deep Web site. This can occur in a number of ways, including via:

- typosquatted, un-indexed web pages with names that are close matches to legitimate brand sites;
- search engine ads for particular keywords that resolve to Deep Web sites;
- mobile apps that redirect to un-indexed websites; and
- email messages with links that redirect to Deep Web sites.

How to combat abuse in the Deep Web

Brands can mitigate abuse in the Deep Web. Even though a website might be attempting to hide its identity and not be found by a search engine, experience shows that methods to uncover and address the abuse exist.

Just like on the Surface Web, a suite of standard tools is available to brand owners to combat abuse, once detected. These include takedown requests to internet service providers, cease-and-desist notices and, if required, the Uniform Domain Name Dispute Resolution Policy.

Identifying IP abuse in a darknet

A darknet is a completely different environment in which to identify and address IP abuse. For most companies, the risks and means of mitigating them are still evolving.

Companies first need to understand their level of risk. Certain types of company are at greater risk than others. For example, financial institutions are obviously at risk. Fraudsters leverage a number of social engineering scams to steal log-in credentials and credit card information from financial customers. They then sell stolen credentials and credit card information via social media, chat forums and underground marketplaces. Using anonymiser technology to access a darknet, fraudsters provide buyers with a step-by-step guide to purchase stolen credentials and credit card information with ease. Fraudsters also sell cloned credit cards at a discounted price, guaranteeing 'promised funds'. In one example gathered from a darknet, a fraudster was selling 50 stolen credit cards for $400 and 500 cards for $5,000.

Companies that are faced with counterfeit distribution of their products should determine whether a darknet is being used as a distribution channel for their goods. Massive quantities can be bought and sold without the brand owner's knowledge, if it does not investigate darknets.

Companies should determine whether they need some sort of regular monitoring of darknets. Options include periodically monitoring darknets or taking a snapshot to evaluate the scale of the problem. Third-party experts can assist with this task.

Not every company needs to implement a programme at this point. It varies by vertical, acceptable level of risk and willingness to invest.

How to combat IP abuse in a darknet

Due to anonymity, online enforcement on darknets is difficult.

However, brand owners should not ignore darknets. While anonymity makes enforcement difficult, darknets are open to investigation. A landscape overview will help brand owners to understand the scale and scope of threats.

Typically, these marketplaces require a customer to register and provide standard credential information. Some will not allow a party to join without an invitation – although this can be surprisingly easy to secure.

Depending on the issues faced, a brand owner might consider working with experts who can carry out test buys in order to understand what is being sold and whether such goods are counterfeit, grey market or even stolen.

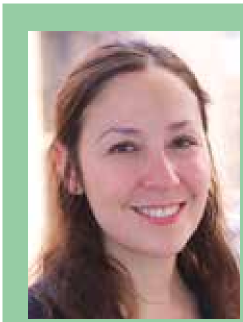
These are the early days of identifying and mitigating IP abuse on darknets and the situation is fluid and evolving. Although it has been occurring for a long time, it is only now starting to gather attention from the mainstream media. Now is a good time for businesses to examine this area and find out what is going on out there.

Summary

Both the Deep Web and darknets pose a clear and present danger for brand owners. It is important to understand the difference between these evolving areas and act accordingly.

Brand owners need to be aware of threats to their intellectual property in all areas of the Internet, both visible and hidden, and identify the perpetrators where possible in order to enforce IP rights effectively.

Engaging with experienced advisers should allow brand owners to understand the internet landscape in full – not just the 4% that one can find via a standard search engine. **WTR**



Akino Chikada
Senior Product Marketing Manager
akino.chikada@thomsonreuters.com

Akino Chikada is a brand protection product marketing manager for MarkMonitor AntiFraud. She started her career in public relations and marketing in London and has worked in Europe, Asia and the United States. She has led and served in interim roles in global marketing strategies, product marketing, events management, public relations, corporate communications and regional marketing. Ms Chikada holds a BA from the University College of London and an MSc from the London School of Economics. She has trilingual fluency in English, Italian and Japanese.

MarkMonitor
Protecting brands in the digital world

Clarivate Analytics

MarkMonitor Inc
50 California Street
Suite 200
San Francisco CA 94111
United States
Tel +1 415 344 6000
Fax +1 415 344 5093
Web www.markmonitor.com