



Online Brand Enforcement 2025

Protecting Your Trademarks in
the Electronic Environment

The science behind brand protection
in the Deep and Dark Webs

MarkScout

This article first appeared in Online Brand Enforcement: Protecting Your Trademarks in the Electronic Environment 2025, 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.

**World
Trademark
Review**



The world's strongest defense against phishing, malware & fraudulent attacks

Providing advanced technology and expertise that protects the revenues and reputations of the world's leading brands in the digital world and beyond.

MarkScout AntiFraud™ enables enterprises to prevent, quickly detect, and mitigate malware and phishing attacks across a range of digital channels — protecting your brand, profits and customer relationships.

The science behind brand protection in the Deep and Dark Webs

The challenges for brand owners seeking to protect their IP rights online have been on the rise as cybercriminals continue to find innovative ways to penetrate corporate infrastructures. The latest media headlines show a surge in cyberattacks and the devastating consequences these have on the organisations targeted.

One recent case involved the 2015 security breach against TalkTalk (<http://uk.reuters.com/article/uk-talktalk-tlcm-gp-results-idUKKCN0VB0I7>), which allegedly cost the company £80 million and lost it 100,000 customers. Further evidence was revealed in a May 2016 UK government research report (www.bbc.co.uk/news/uk-36239805) which showed that up to two-thirds of big UK businesses have been hit by a cyberattack in the past year alone.

Whether a company has a large customer base that accesses and exchanges financial or personal information online or is a small, niche brand with IP assets to protect, no one is exempt. Fraudsters will stop at nothing to profit from a corporate entity's security vulnerabilities, and the data they steal can fetch a hefty price in underground online marketplaces.

While banking and finance organisations are the most obvious targets, an increasing number of attacks focus on companies in other industries, from healthcare and retail to technology, manufacturing and insurance companies ([www.scmagazine.com/cyberattacks-increase-against-](http://www.scmagazine.com/cyberattacks-increase-against-manufacturing-healthcare-industries/article/491480/)

[manufacturing-healthcare-industries/article/491480/](http://www.scmagazine.com/cyberattacks-increase-against-manufacturing-healthcare-industries/article/491480/)). Data breaches can have a damaging effect on a company's internal IT infrastructure, financial assets, business partners and customers, not to mention on the brand equity and customer trust that companies spend years trying to build.

Battlegrounds deep and dark

Cyberattacks are flourishing, in no small part because the perpetrators have become adept at navigating the waters of the Deep Web and the Dark Web, far below the commonly traversed segments of the Surface Web. These expansive but hidden segments are changing the rules of the game for cybercrime and hacktivism.





Some perspective is in order. A common analogy for the full internet landscape is that of an iceberg. The section of the iceberg above water level is the Surface Web, comprised of visible websites which are indexed by standard search engines. This is what most people use every day to find information, shop and interact online, but it accounts for only about 4% of the Internet.

The remaining 96% of sites are found in the Deep Web, which includes pages that are unindexed by search engines. Most of the content in the Deep Web is legitimate, including corporate intranets and academic resources residing behind a firewall.

However, some sites in the Deep Web also contain a sizeable amount of potentially illegitimate or suspicious content – for example:

- phishing sites that collect user credentials;
- sites that disseminate malware that deliberately try to hide their existence;
- websites and marketplaces that sell counterfeit goods; and
- peer-to-peer sites where piracy often takes place.

Consumers may unknowingly stumble on these illegitimate sites through spam emails, advertisements or cybersquatted domains, and are at risk of unwittingly

releasing personal information or credentials to fraudulent entities. In addition, consumers may be deliberately lured to these sites by fraudsters.

Deeper still is the Dark Web, a collection of websites and content that exists on overlay networks whose IP addresses are completely hidden and must be accessed using anonymiser software (eg, Tor). While there are a number of legitimate users of Tor – such as privacy advocates, journalists and law enforcement agencies, its anonymity also makes it an ideal foundation for illicit activity. Vast quantities of private information (eg, log-in credentials and banking and credit card information) are peddled with impunity on underground marketplaces in the Dark Web. Infiltrating these criminal networks has proven elusive for security analysts because one must first be invited to join the conversation and interact with the group.

Waking up to threats

The Deep and Dark Webs have been in the public eye for some time, but in recent years fraudsters and cybercriminals have honed their tactics in these hidden digital channels to strike at their prey more effectively and minimise the risk of being caught.

While Deep Web sites are not indexed, consumers may still stumble on them, unaware that they have been redirected to an

“

Cyberattacks are flourishing, in no small part because the perpetrators have become adept at navigating the waters of the Deep Web and the Dark Web, far below the commonly traversed segments of the Surface Web

illegitimate Deep Web site. The paths to Deep Web sites are many:

- typosquatted webpages with names that closely match legitimate brands;
- search engine ads for particular keywords that resolve to Deep Web sites;
- email messages with phishing links; and
- mobile apps that redirect to unindexed websites.

The Dark Web presents an even more vexing challenge for cybersecurity professionals. The anonymity that hides identities in the Dark Web allows this medium to thrive as a haven for cybercriminals, where corporate network log-in credentials (eg, phished from employees) can be bought and sold to the highest bidder, opening the door to a cyberattack that most companies are unable to detect or prevent.

Further, the more users who learn the intricacies of Tor to access and navigate the Dark Web, the greater the scale of anonymity becomes. The number of points in the Dark Web's distributed network of relays makes it more difficult to identify a single user and track down cybercriminals – it is like trying to find a needle in a haystack when the haystack continues to grow.

Science and strategy behind protection

Brands can potentially mitigate abuse in the Deep Web, depending on the site. If a website attempts to hide its identity from a search engine, there are technological solutions to uncover and address this abuse. Conventional tools commonly used by companies to protect their brands can also tackle fraudulent activity

in the Deep Web, including takedown requests to internet service providers, cease and desist notices and, if required, the Uniform Domain Name Dispute Resolution Policy.

As for the Dark Web, where anonymity reigns and the illicit buying and selling of proprietary and personal information are commonplace, companies can arm themselves with the right technology and threat intelligence to gain visibility into imminent



REAL-WORLD EXAMPLES

Third-party breach

A fraudster began targeting healthcare clinics and stealing large client databases of between 20,000 and 9 million records each. A company – not the direct target, but affected by regulatory and brand reputation risk as a result of the breach – was alerted immediately. Resources were increased and the vulnerabilities used by the fraudster were understood, allowing for cyber intelligence cooperation which reduced the risk of additional breaches.

Physical attacks

A bank was alerted of an upcoming physical attack on its premises. The bank contacted law enforcement agencies, which on the specified day helped the bank to increase security. As a result, the disruption to the bank was minimised.

Hacking tools

In a forum a hacker shared a tutorial on how to hack Company A. Company A was alerted via its monitoring solution and worked with its security and engineers to fix its vulnerabilities. The end result was that future hacks using the same vulnerability were mitigated.

IP theft

An engineer from Company B needed assistance with coding and posted proprietary code to a forum, which could have had disastrous effects. Company B was alerted via its monitoring solution that proprietary code was being shared and took action by hosting an internal education session. It also conducted a thorough review to ensure that the code did not expose vulnerabilities in its systems.

Stolen user credentials

A fraudster stole hundreds of customer credentials from a company, likely through phishing. The fraudster then published a list of these credentials on a forum in the Dark Web to establish credibility. The company in question was alerted via its monitoring solution and its customer service team was able to contact the victims to issue new usernames and passwords in order to protect their accounts. The result was minimised fraud remediation costs.

“

In the event of a data breach where credit card numbers are stolen, threat intelligence can help to limit the financial damage to consumers by revealing stolen numbers before they can be used

threats. Actively monitoring fraudster-to-fraudster social media conversations, for example, enables companies to take necessary security precautions before a cyberattack, or to prevent or lessen the impact of a future attack. In the event of a data breach where credit card numbers are stolen, threat intelligence can help to limit the financial damage to consumers by revealing stolen numbers before they can be used, so that consumers can contact their banks to cancel the cards.

Technology can even help to identify and infiltrate cybercriminal networks in the Dark Web which might otherwise take a considerable amount of manual human effort by a security analyst team. Access to technology can significantly lighten the load for security teams and anchor a more reliable and scalable security strategy.

In light of so many cyber threats, it falls to organisations and their security operations teams to leverage technology to identify criminal activity and to limit financial liability to the company and irreparable damage to the brand.

Key industries at risk

A growing number of industries are now being targeted by cybercriminals but there are tangible steps which companies can take. For financial institutions, awareness of Dark

Web activity yields important benefits. Clues for an impending attack might potentially be uncovered to save millions of pounds in breaches and stop the erosion of customer trust. Improved visibility can also help companies identify a person sharing insider or proprietary information in the Dark Web and determine the right course of action to reduce the damage.

One of the most common attacks against the financial services industry is called a 'credit card dump'. Cybercriminals either hack a retailer's network or use malware to infect a point-of-sale device in order to steal and sell credit card numbers, expiry dates and other

user information on the Dark Web. Other criminals can then use the information to make unauthorised purchases.

In the healthcare industry, data breaches can be especially alarming because they expose not only the healthcare organisation's proprietary data, but also patient's medical information and associated personal credentials. This could include images of authorised signatures, email addresses, billing addresses and account numbers. Cybercriminals who use information like this can exploit it to compromise more data, such as social security numbers and private medical records. Credentials could even potentially lead to false identities being sold.

Comment

Most organisations have implemented stringent security protocols to safeguard their IT infrastructure. However, conventional security measures do not provide the critical intelligence needed to analyse cyberattacks that propagate in the Deep and Dark Webs. It is fundamentally harder to navigate a medium where web pages are unindexed and anonymity can be used to hide criminal activity.

Meanwhile, cyberattacks on organisations across a wider number of sectors continue to surge, putting proprietary corporate information, trade secrets and employee network access credentials at risk. Businesses must be aware of all threats to their intellectual property in all areas of the Internet – and the visible segments are just the tip of the iceberg. Leveraging every available tool to monitor, detect and take action where possible is vital when it comes to addressing the threats that these hidden regions of the Internet pose.