

Anti-counterfeiting 2025



Understanding the Deep and Dark Web: mitigating risk and
protecting your brand

MarkScout

A Global Guide



Make the Dark Web part of your defence strategy

Providing advanced technology and expertise that protects the revenues and reputations of the world's leading brands in the digital world as well as the anonymous, hidden area of the Internet where cybercriminals reign with impunity.

MarkScout Dark Web & Cyber Intelligence™ is a powerful solution to prevent or limit the damage of cyberattacks. It provides near real-time monitoring of these attacks across multiple cybercrime zones — protecting your brand, profits and customer relationships.

Industry insight

Understanding the Deep and Dark Web: mitigating risk and protecting your brand

Counterfeiting is an issue that brands in all industries are contending with – from pharmaceuticals, electronics and beauty products to luxury fashion and apparel and toys. The consequences of fake goods flooding the market can have an impact on many areas of the business, including the bottom line, reputation and customer satisfaction. In some instances (eg, counterfeit pharmaceuticals), the impact extends well beyond economics and affects the health and wellbeing of consumers.

While it is almost impossible to place a monetary value on the counterfeiting market, the scale of the problem becomes apparent thanks to figures from the Organisation for Economic Cooperation and Development and an EU Intellectual Property Office study, which suggest that counterfeit goods account for 2.5% of international trade, equating to around £270 billion.

It is not enough to curb sales or take down sites in the fight against counterfeiters and fake goods. Organisations need to have a multi-layered online brand protection strategy that addresses all channels and avenues that make it possible for counterfeiters to do business, including social media, mobile applications and online marketplaces.

However, there is a more insidious method that counterfeiters (and other cybercriminals) are also using to take advantage of consumers: the Deep Web.

When it comes to the availability of fake goods, everything from counterfeit train tickets to drugs and passports can be found. While some consumers purposely seek out places to purchase items on the Deep Web, many internet users find these sites inadvertently or are purposely directed there through suspect links on social media platforms or websites.

Most of the content on the Deep Web contains information for legitimate uses – including corporate intranets or academic resources residing behind a firewall, social media sites hidden behind a log-in page, online forms, pop-up ads and pages that are unlinked to other sites. However, some sites on the Deep Web also represent potentially unauthorised or suspicious content, such as phishing sites that collect user credentials, sites that disseminate malware, websites and marketplaces that sell counterfeit goods and peer-to-peer sites where piracy often takes place. Consumers may unknowingly stumble upon these unauthorised sites through spam

emails, advertisements or cybersquatted domains, and are at risk of unwittingly releasing personal information or credentials to fraudulent entities.

Illuminating the Dark Web

Deeper beneath the surface layer of the Internet lies the Dark Web, a smaller but potentially more dangerous subset of the Deep Web. The Dark Web is the collection of websites and content that exists on dark nets – overlay networks whose Internet Protocol addresses are completely hidden. Both publishers and visitors to Dark Web sites are entirely anonymous. Dark Web content can be accessed only by using special software such as Tor, Freenet, Invisible Internet Project and Tails. Tor is free to download and use, and enables anonymous access and communication within the Dark Net. Around 2.5 million people access Dark Web content through Tor daily. It is often used by strong privacy advocates, such as journalists and law enforcement agencies, that may be searching for dangerous or sensitive information and do not want their online activity tracked. The very anonymity of the Dark Web makes it an ideal foundation for illicit and criminal activity.

Vast quantities of private information, such as log-in credentials and banking and credit card details, are peddled with impunity on crypto-marketplaces. Cybercriminals also offer their services for hire and even provide tutorials on codebreaking and how to infiltrate corporate networks. Cybercrime itself has become a service that is offered pervasively on the Dark Web. With Bitcoin used as the preferred currency, every transaction between buyer and seller can be conducted anonymously on the Dark Web.

Protecting your brand on the Deep Web

Not only are consumers in danger from counterfeiters and cybercriminals using the Deep Web; brands are at risk, too. The Deep Web and Dark Web are not new, but in recent years fraudsters and cybercriminals have been honing their tactics in these hidden digital channels to strike at their prey more effectively and minimise their own risk of being caught. Moreover, as a higher volume of users learn the intricacies of Tor to access

and navigate the Dark Web, it becomes more difficult to identify a single user and track down cybercriminals. Most organisations have implemented stringent security protocols to safeguard their IT infrastructure, but conventional security measures are designed to protect data and assets inside the firewall, not outside.

Targeted attacks such as business email spoofing (BES) – whereby an internal employee receives an email purportedly

from a corporate executive or the IT team requesting log-in or password information – are difficult to detect with traditional email security. Much like a consumer phishing or malware scam, BES attacks use sophisticated social engineering tactics to compromise login information, which can then be distributed through the Dark Web and eventually precipitate a full-scale cyberattack and data breach. In the end, the most vulnerable points of access to any network are individuals, such as consumers and employees.

Even knowledgeable users may be duped by a BES or phishing attack – and the more people who have access to the network, the more chance that potential lapses may occur. Companies that have many partners, distributors or affiliate organisations have a larger problem, as they allow access to a greater number of individuals. The sharing of confidential data on paste sites can also become a target for theft or misuse. No amount of IT security will prevent a back-door attack on the infrastructure where an individual unwittingly surrenders the key.

Consumers may similarly be duped by brand-associated social engineering attacks, unknowingly revealing personal or financial information that can be sold on criminal Dark Web networks. Cybercriminals move silently and quickly to exploit the valuable data before the user becomes aware. Monitoring potential threats on the Deep Web and Dark Web provides the intelligence to take appropriate action. Cybercriminals often communicate and interact via private cybercriminal social media forums and chat rooms, and in some cases threat actors even boast or congratulate each other after successful attacks, which can be tracked and monitored.

Threat intelligence empowers brand owners to take action by allocating the right security resources before an attack and analysing the data to connect the dots between threat actors in order to prevent future attacks.

In other cases, the damage of a data breach can be mitigated – for example, when credit card numbers are stolen – by working with financial institutions to cancel the cards before they can be used fraudulently. The stakes for companies are high. Cyberattacks that propagate on the Dark Web pose a significant threat to proprietary corporate information, trade secrets, employee network access credentials and consumer financial and personal information. It falls to organisations and their security operations centres to identify the activity in order to limit financial liability to the company and irreparable damage to the brand.

How attacks work on the Dark Web **Financial services**

Visibility into Dark Web activity can yield important benefits for financial institutions. 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 to identify a person sharing insider or proprietary information on the Dark Web and determine the right course of action to minimise the damage.

Healthcare

Data breaches in the healthcare industry can be especially alarming, because they expose not only the healthcare organisation's proprietary data, but also a vast number of patients' medical information and associated



No amount of IT security will prevent a back-door attack on the infrastructure where an individual unwittingly surrenders the key



Internal education for the entire company and the partner channel can go a long way towards mitigating the potential for attack and serious data breach

personal information. A dump of customer information from a medical clinic, for example, included images of authorised signatures, email addresses, billing addresses and account numbers.

Engineers and software code

Data shared on public websites or social media forums can inadvertently lead to cyberattacks and data breaches. For example, an engineer who asks a question of fellow engineers about a coding issue might share proprietary source code within the group. Seeing how internal code is designed could help an attacker to identify potential vulnerabilities and open the door to hacking or a cyberattack. Part of the solution for situations such as this is advanced education about the dangers of sharing code publicly. In addition to *ad hoc* management of individual events, group training can be conducted for an entire engineering group, for example, as a reminder of the importance of protecting proprietary information.

Combating cyberattacks on the Deep and Dark Web

When developing and implementing an online brand protection strategy, it becomes obvious that organisations need to expand plans to include monitoring the Deep and Dark Web.

Organisations should monitor threats across multiple cybercrime zones. IT security teams should ensure that they are monitoring as many digital segments as possible where cybercrime frequently takes place. These include not only Deep Web and Dark Web sites, but also other digital channels where fraudster-to-fraudster interactions occur

(eg, social networks, Internet Relay Chat, chat sites and data paste sites). Companies must also take an effective defensive posture, developing advanced alerts before, during and after an attack occurs, ultimately providing the vital intelligence needed to take the appropriate action.

Some organisations may be tempted to try their hand at infiltrating cyber threats on the Dark Web themselves. However, in order to do so, they must first go through the painstaking process of scouring the Dark Web and trying to access cybercriminal hangouts manually to detect and identify threats. They must then find a way to build trust with hackers and fraudsters over time. Even a large team of security analysts cannot sufficiently achieve the coverage needed for any measurable success. Such attempts are labour intensive, time consuming and by no means scalable as a reliable security strategy. It is better to employ an automated approach that leverages smart technology to achieve network penetration faster and in a more coordinated fashion.

In addition, education and awareness must be a priority within the organisation. Education should focus on two distinct audiences to raise awareness of threats before they can affect the company. Customer outreach is critical – in particular for companies in the financial services, healthcare and other industries where users access and exchange personal or financial information. Online consumers must be regularly reminded of the dangers of phishing scams and social engineering attacks, and that they should never provide personal information unless on the verified banking, healthcare or partner site.

Likewise, internal and business partner employees are increasingly being targeted through BES and other spear phishing attacks. Human resources and payroll professionals are becoming common targets for these corporate-focused attacks, because of their access to employee and other sensitive company information. Employees who commonly receive requests from senior executives may be particularly vulnerable to these types of attack. Internal education for the entire company and the partner channel can go a long way towards mitigating the potential for attack and serious data breach.

Conclusion

The Internet provides businesses with abundant opportunities in terms of expanding their markets, selling more products and widening their reach. However, it is a landscape that also lends itself to furthering the aims of cybercriminals and counterfeiters. In order to fully capitalise on these opportunities and mitigate risk, organisations need to strike a balance when it comes to the online space. A key part of this is understanding the threats,

the risk that they pose to the organisation and how they can be effectively overcome. All of these topics fall under the banner of a comprehensive online brand protection strategy, and can be addressed as part of an evolving plan that will ultimately protect the organisation's reputation, customer trust and bottom line. **WTR**
