BUSINESSCLASS
KNOWLEDGE ▪ SEMINARS ▪ INSIGHTS

Blakes

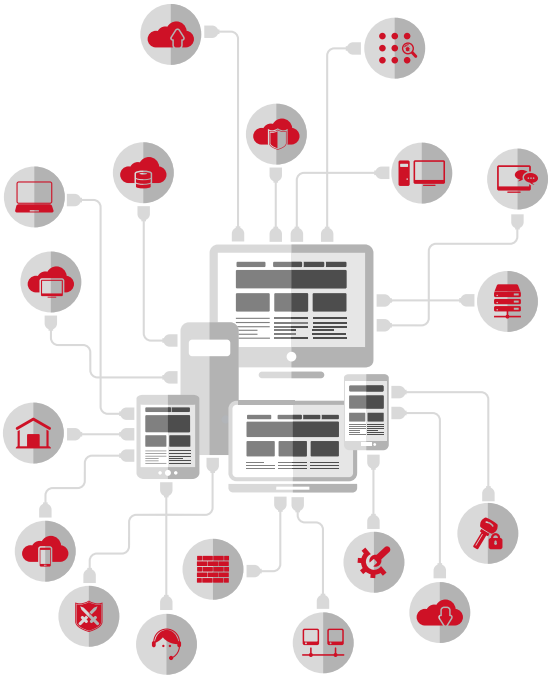
Shining a Light on the Darknet:
What Every Business Should Know

By Sheldon Burshtein

The portion of the Internet that most people generally use is only one of three layers. The commonly used layer that is accessible by search engines is referred to as the clearnet or the surface web and represents only about four per cent of Internet content. In addition to the surface web, the Internet comprises the deep web and the Darknet. The Darknet is where hacked data goes to live and it is likely to become increasingly relevant for communication, commercial activity, terrorism and cybercrimes.

WHAT IS THE DEEP WEB?

The deep web, or the bergie web, was developed by the United States military and differs from the Darknet. The deep web was originally designed in the 1970s to isolate networks from the Advanced Research Projects Agency Network (ARPANET) and hide the locations and IP addresses of U.S. military operations for security purposes. Military, government and law enforcement organizations are still among the main users of the deep web.



The deep web comprises unindexable content, dynamic content pages and otherwise gated content that is not accessible by regular browsers or search engines. The deep web includes large databases, libraries and members-only websites that are unavailable to the general public but rather are gated or hidden so only the intended audience has access. Most of the content on the deep web comprises academic resources maintained by universities and other institutions. It is now commonly used for information saved in the cloud.

WHAT IS THE DARKNET?

Generically, a darknet is a collection of networks employing technologies that permit users to communicate and transact in an anonymous manner. The term "darknet" has been used to differentiate private, anonymous distributed networks from public networks. The term further evolved to refer to a decentralized distributed network that lacks a central index and incorporates privacy encryption security and user anonymity features with the primary purpose of sharing information only with trusted members.

The goal of a darknet is to create a closed network to communicate securely in a manner that avoids detection or penetration so that websites can be accessed anonymously. The Freenet Project is one of the earliest examples of a darknet. The Freenet is a peer-to-peer platform used to anonymously share files, chat and browse and publish "freesites"— websites accessible only through Freenet — without fear of censorship. It allows for the creation of private networks so that content on a particular website can only be accessed by those who have been manually identified. A more modern private network is I2P, which also provides integrated file storage, secure email, chat and blogging.

The Darknet has also come to mean the "hidden" third layer of the Internet. As a result of the anonymity afforded to users, the Darknet has become a home for a variety of clandestine Internet activities and transactions, including intellectual property infringement, cybercrime and terrorism.

HOW DOES THE DARKNET WORK?

The Darknet uses onion routing, a technique for allowing anonymous communication over a computer network.

The onion router (TOR) is free software that allows encryption and is required for access to the Darknet. The term "onion" was selected because it refers to numerous layers. TOR was developed in the mid-1990s by the United States Naval Research Laboratory (NRL).

In 2002, the NRL released to the public a version of TOR. The open source release meant that anyone could download and use TOR to browse the surface web anonymously and visit anonymous websites on the Darknet. Several million people use TOR daily. As a result, websites started to flourish on the Darknet.

Each Darknet website is allocated a specific .onion IP address containing a 16-unit alpha-numeric combination followed by the .onion designation, like «a1b2c3d4e5f6g7h8.onion». A user must use the .onion address to access the applicable website (.onion is not a top-level domain that is established or supported by the Internet Corporation for Assigned Names and Numbers (ICANN)).

The Darknet is popular among bloggers and journalists living in jurisdictions where censorship and political imprisonment are common. There are numerous chatrooms. Facebook has a Darknet website that is designed for users who visit Facebook by using TOR to evade surveillance and censorship. Over a million users access Facebook via TOR each month.

DARKNET MARKETPLACES

A key aspect of the Darknet is the number of marketplace websites that sell counterfeit, pirated and illegal goods. For example, users may be redirected from a website on the surface web to a Darknet website without knowing. This may occur through unindexed webpages with names closely resembling domain names of legitimate brand websites or by way of search engine results for keywords that resolve to advertisements with links to Darknet websites. It may also result from mobile apps or emails with links that redirect users to unindexed Darknet websites.

The most popular marketplace on the Darknet was Silk Road, until it was shut down by the U.S. government. The individual who operated Silk Road was convicted of a number of crimes, including conspiring to violate various laws, and was ordered to pay over US$180-million in fines and sentenced to life in prison without parole.

As soon as the government shut down Silk Road, another individual set up Silk Road 2.0 and was promptly charged with the same crimes as the operator of the initial website. Many other Darknet marketplaces, including Alpaca, Cloud 9, Hydra and Pandora, have also been taken down by law enforcement as a result of the use of honeypots, which are websites set up to attract and trap people participating in illegal activities.

However, numerous marketplaces continue to thrive on the Darknet, including Abraxas, Agora, AlphaBay, Andromeda (formerly Dark Bay), BlackBank, Blue Sky, Evolution, Free Market, Middle Earth, Nucleus, Outlaw Market, Pirate Market, RAMP and Tochka. Some of these are accessible by invitation only, but function in the same way as surface web marketplaces.

Darknet marketplaces generally comprise full-featured markets with vendor pages, product review pages, product listings, as well as customer support and dispute resolution procedures. Many Darknet marketplaces only effect transactions with virtual currency, which uses cryptography for security, including bitcoin. (See our September 2015 *Blakes Article: Will that be cash, credit or bitcoin? The pros and cons of digital currency*).

For a long time, one of the features contributing to the clandestine aspects of the Darknet was the absence of a meaningful search engine. However, the Grams search engine (a search engine for TOR-based Darknet markets) now indexes a number of the Darknet's leading marketplaces.

OTHER CRIME ON THE DARKNET

Surveys have revealed that among the most prevalent goods sold on Darknet marketplaces are illicit drugs, credit cards, weapons and counterfeit and pirated goods. The most commonly purchased services are virtual currency, fraud, hacking, hoax, phishing and terrorism services.

When records obtained in data breaches are published and offered for sale, it is often on the Darknet. For example, hackers published on the Darknet the member data obtained from the Ashley Madison dating website.

Surveys show that child pornography is in demand on the Darknet. In a U.S. prosecution for child pornography crimes, it was revealed that the Federal Bureau of Investigation took control of Playpen, the largest known Darknet child pornography service, by way of a network investigative technique to capture the IP and media access control (MAC) addresses of users and thereby obtain evidence of the accused's sale of pornography.

The increasing use of the Darknet as a platform for intellectual property infringement as well as commercial and other crime requires businesses to be mindful of the current and potential impact to them of the Darknet.

CONTACT US

Sheldon Burshtein
416-863-2934
sb@blakes.com