ISACA
TECH BRIEF

The Darknet

The Darknet: What is it?

While most people think of the Internet as a single, homogeneous entity, that perception is incorrect. It actually consists of different types of content, with different access methods and degrees of risk and legality. Some of the content is, at best, unsettling and, at worst, criminal.

The most commonly known Internet is the publicly available web that is familiar to most users and is generally accessed by browsers and search engines. It is also known as the surface web, the visible web or the clearnet and is used to communicate with others, gather news and information, buy and sell goods, and promote products and services. Perhaps not as well known is the deep web, which is accessible only to users who know how to get there, perhaps via a direct link, IP address or Internet relay chat (IRC) room.[1]

Within the deep web lies the darknet, a world of content that exists on overlay networks (such as Tor) whose URL addresses are hidden. The darknet uses a .onion domain and its URLs are random and hard to remember/find because they feature nonsensical numbers/letters and can change every few hours. Accessing the darknet requires special software that uses a randomized path to its destination. This indirect path helps obscure users' location and identity and protects their (and the publishers') anonymity—an important feature, given the nature of some of the activity that takes place there.

"Companies have to be consistent about monitoring the darknet for company information before they think they have been compromised. When a hacker breaks into a company, he will gather as much data as possible, sift through it, cherry-pick what he wants and make money off it for a while. Only after that will he post it, possibly weeks or months after the hack."

TIM SINGLETARY, BUSINESS AREA MANAGER FOR CYBER RISK SERVICES, PERATON

1 Pagliery, Jose; "The Deep Web you don't know about," CNN tech, 10 March 2014, *http://money.cnn.com/2014/03/10/technology/deep-web/index.html*

How is the darknet being used?

The darknet is most commonly associated with illegal activity. News stories typically refer to the darknet as a place where drugs (e.g., from the online black market, Silk Road), guns, counterfeit money, hacking software, hackers' services and child pornography are bought and sold. In some cases, nonexistent items lure shadowy buyers into sham purchases: Scammers set up dark websites to collect funds, then shut down suddenly and leverage the privacy and anonymity of the darknet to evade their irate (would-be) customers.

Often gathered via data breaches, personally identifiable information (PII) can surface on the darknet, where individuals' names, addresses, birthdates, account numbers, government-issued identification numbers, credit card numbers, medical information, etc., appear at bargain rates.

Selling PII on the darknet is especially attractive because it can be offered more than once. After the information is exposed, it can be exchanged repeatedly over time—each time at a price. In fact, the practice is so lucrative and pervasive that it has taken on some aspects of conventional surface-web transactions: sites review PII providers to indicate which are preferred sources—much as a satisfied diner might favorably review a restaurant.

Not all activity on the darknet is criminal. Individuals or organizations may need or want the privacy protection of the darknet for legitimate reasons. For example, people living in closely scrutinized, totalitarian societies may communicate with each other and the outside world via the darknet; law enforcement agencies may collect dangerous or sensitive information by searching it, knowing their activities are less likely to be tracked; military agencies may surveil enemy activity; and whistleblowers may leak information to the media while remaining anonymous (e.g., *The New Yorker* has a site called Strongbox™ for this purpose).

In addition to these purposes, legitimate users exploring the darknet may find links to the texts of rare books, collections of news from mainstream sites and forums to discuss current events anonymously. Information security professionals may track activity on the darknet to keep a finger on the pulse of hackers and learn what content is typically monetized; in this way, practitioners learn which enterprise assets require extra protection. Companies may use the darknet to gather business intelligence, including information on competitors, employees and leaked confidential or proprietary corporate information.

How do the numbers stack up?

Percentage of **2,723 live dark websites** hosting illicit material, as monitored over a five-week period[2]

Number of people **who access the darknet** through Tor daily[3]

Percentage of companies on the 2017 *Fortune* 500 **exposed on the darknet**[4]

2 Guccione, D.; "What is the dark web? Why (and how) to visit this invisible part of the internet," CSO, 19 January 2018, *https://www.csoonline.com/article/3249765/data-breach/what-is-the-dark-web-is-it-illegal-and-should-you-ever-visit-the-dark-web.html*

3 Jamieson, C.; "Understanding the Deep and Dark Web: mitigating risk and protecting your brand," World Trademark Review, 18 May 2017, *www.worldtrademarkreview.com/Intelligence/Anti-counterfeiting/2017/Industry-insight/Understanding-the-Deep-and-Dark-Web-mitigating-risk-and-protecting-your-brand*

4 DarkOwl™, "Every company in the 2017 Fortune 500 is exposed on the darknet," *https://www.darkowl.com/darknet-index-fortune-500/*

"A lot of companies believe that putting a fence around the building secures the company. A firewall does not secure the company. You have to secure the assets and everything else. A company is like a tomato: tough on the outside but once you are past that, you have access to everything inside."

JAY FERRON, CHIEF SECURITY OFFICER, INTERACTIVE SECURITY TRAINING

What is the risk for enterprises?

Enterprises that access the darknet for whatever reason must recognize that they are subject to associated risk, both for themselves and for their customers. The most obvious risk is the exposure and/or loss of customer data and its subsequent sale on the darknet (as occurred with recent hacks of Adobe®, Equifax® and Target®). Not only do enterprises face the wrath of customers and the fiscal consequences their defection may entail; enterprises may also incur large expenditures to find and fix breaches and address disruption to business. Failure to handle a data breach quickly and competently can downgrade a business's reputation and the value of its brands. Some organizations, especially smaller ones, may not survive.

Identity theft is not the only risk on the darknet. Gift card fraud is a relatively simple undertaking for hackers, who can compromise the gift card network or steal gift card information directly from users. Once the information is sold through the darknet, it can undermine the value of gift cards and damage the reputation of the issuer. A similar risk is credit card fraud, as credit card information is easily stolen and traded. Businesses that sell services or products to customers using fraudulent credit cards lose money on each transaction.

Hackers target employees or business partners as easy sources of information that can be monetized on the darknet. Through email spoofing and social engineering, employees receive inauthentic email that appears to be from a corporate executive or IT team requesting log-in or password information. The employee thinks it is a legitimate request and provides the information, which becomes a commodity on the darknet.

All of these crimes can jeopardize an enterprise's customers, partners and vendors; require significant investment to repair; and erode its reputation in the marketplace. Sadly, because of the anonymity and privacy of the darknet, most enterprises will not know when attacks are coming, what kinds of attacks they are likely to incur, where the attacks will likely originate nor who will be behind them.

"As long as people want to buy data and information to use against individuals and corporations, the darknet will continue. If anything, it may go more public—in essence, hiding in plain sight."

ROB STROUD, CHIEF PRODUCT OFFICER, XEBIA LABS

How can enterprises protect themselves?

Information security is a 24/7 vocation best undertaken by skilled, knowledgeable professionals. They are an enterprise's best defense against hacking. Enterprises that do not have such professionals on staff should not delay in hiring or contracting the necessary expertise.

Following are a few tips for enterprises to mitigate the risk associated with the darknet:

- **Never use a computer that is important to the business to connect to the darknet.** It can too easily become infected with malware or allow unwanted traffic to enter the enterprise's network. If it is necessary to connect to the darknet, it must be done from a secure environment—a device that is not connected to the rest of the enterprise's network.
- **Be proactive with respect to the enterprise's interests and the darknet.** Consider investing in staff or a third party to monitor the darknet for any company-related content, data, references or mentions. By monitoring hackers' activity and conversations, the enterprise may learn the techniques they use to compromise businesses, enabling a more effective counterdefense. Enterprises should be aware that proactive, comprehensive monitoring is time-consuming, labor-intensive and not particularly scalable. Information may not appear on the darknet for months after it is stolen. Monitoring the darknet should, by no means, be the only security activity the enterprise undertakes.
- **Investigate stronger commercial solutions.** These may require a license and generally have a cost, so enterprises must ensure that expenses are commensurate with the value of the asset by focusing on high-risk, high-value systems.
- **Use basic security tactics like creating backups.** Backups are especially helpful in responding to ransomware, preparing a disaster recovery plan, educating employees (and third parties) on attack vectors and appropriate responses, whitelisting and/or blacklisting selected sites, instituting multi-factor authentication and requiring strong passwords.
- **Consider acquiring insurance** to back up other security practices.

Despite the necessary security controls, the darknet itself cannot be controlled, nor should enterprises attempt to control it. At best, enterprises can monitor the darknet and respond if their information is offered for sale. New darknets are already starting to appear, and the same nefarious characters pursue the same illegal activities throughout the new iterations; however, hackers and criminals increasingly connect workstations rather than servers and allow only certain individuals into their small groups. The new darknet appears to be deeper, darker and harder to trace; to meet the challenge, enterprises and trained professionals alike must be proactive and keep up with innovations in the field.

For more information, go to:
www.isaca.org/darknet

ISACA®