THE CORPORATE COUNSELOR

NOVEMBER 2017

The Dark Web

By Elizabeth Vandesteeg and Jeffrey Goldberg

Nearly all of us access the Web on a daily basis. Yet for many of us, there is a fundamental lack of knowledge about the basic structure of the Internet and the way its different levels interact. It is only when stories or criminal cases regarding hidden online markets for illicit and illegal goods, such as Silk Road, hit mainstream news outlets that the general public starts to gain awareness of the deeper pool of sites and information that exist beneath the surface. Such stories are, for many, the sole source of information regarding the so-called "Dark Web."

The goals of this article are: 1) to provide a basic outline of the structure of the Web and to provide some insight into the purpose for and content housed on each level; and 2) to give some practical tips on preventing your company's data from ending up on the Dark Web.

The Surface Web

The overall structure of the Web is often compared to an iceberg. The top level of the Internet, known as the "Surface Web," can be thought of as the tip of the iceberg. The Surface Web is the visible part of the Internet accessed daily by average users and consumers.

The Surface Web is made up of static, indexed webpages and websites that can be accessed through your web browser by directing the browser to a specific web address, *e.g.*, www.sfgh.com (our firm's webpage). Surface websites and pages can be accessed through standard web browsers, such as Internet Explorer, FireFox and Google Chrome.

While the Surface Web may seem immense, it is estimated to make up only approximately 4.5% of the entire Web.

The Deep Web

Underneath the Surface Web is the "Deep Web." Not to be confused with the Dark Web, the Deep Web simply consists of parts of the Internet that are not accessible to the web-crawling search engines mentioned above. That's because the Deep Web is made up primarily of millions of databases (public, subscription or internal) that house information requiring a specific search query made through a webpage. And it includes all web pages behind membership logins.

Users access Deep Web content by typing a direct search query into a website's search form, resulting in access to a database that is not linked or accessible through Surface Web search engines. Common examples of Deep Web content the average person may access routinely are newspaper, legal, financial markets and academic databases.

The Surface Web and the Deep Web often work in conjunction. Users can make queries on search engines and are directed to websites that have non-indexed Deep Web content. As an example, one could use Google to search for the New York Public Library (NYPL) homepage. This Google search and the resulting landing page of www.nypl.org are part of the Surface Web. As the user logs on to the New York Public Library's homepage, he or she can access the Deep Web through the site's built-in search tool. As a way of experiment, if a person were to type

"Ziggy Stardust" into the NYPL's built-in search form, the results of the query would be Deep Web content concerning materials that New York Public Library houses related to David Bowie and artist's seminal 1972 album, "The Rise and Fall of Ziggy Stardust and the Spiders from Mars." The NYPL's search results are non-indexed content that require a user to perform a specific search to access.

The Dark Web

The deepest level of the Internet, one that appears invisible to most, is the "Dark Web." Frequently, the Dark Web and the Deep Web are conflated, but they are not the same thing. The Dark Web refers to any website that is housed on a server that is not accessible by a standard search engine, requiring specific software to access. In comparison to the Deep Web and Surface Web, the total content housed on the Dark Web is minuscule — estimated to be approximately 0.03% of the total Web.

While it is unclear how many people access the Dark Web daily, it appears to be a very small number of individuals. It is estimated that only two million people per day use the required software to access the Dark Web, and only 3% of overall Dark Web software traffic accesses hidden websites.

Accessing the Dark Web

To access the Dark Web, users must have specific software that encrypts and anonymizes the user's IP address. The Onion Router, colloquially known as the TOR browser, is the most popular and well-known tool to access the Dark Web. TOR users may use the browser to hide their true location and appear to be located in a different country.

Who Uses the Dark Web and Why?

The Dark Web has a bad reputation, as people are likely peripherally aware of the illicit activities that occur there. But it is important to note that much of the traffic on the Dark Web is for legitimate purposes.

Legitimate Uses for the Dark Web

First and foremost, browsing the Internet through an anonymizing web browser offers users personal freedom and privacy. TOR users can post content anonymously.

Additionally, a significant number of TOR's users live in closed, totalitarian countries where the Internet is heavily censored. Users in countries such as China and Saudi Arabia use the TOR browser or similar tools to access websites that most of the world can freely visit through a simple Surface Web search. According to Roger Dingledine, one of three founders of the TOR Project, as of July 2017, Facebook is the biggest hidden service accessed using the TOR browser. And Facebook announced that one million people used the Dark Web to access the site last year.

Another legitimate use of the TOR browser and the Dark Web is for journalism purposes. Journalists have admitted to using the Dark Web to contact sources anonymously and to store sensitive documents securely. *The New York Times*, for example, maintains a secure lockbox on the Dark Web to which whistleblowers and sources can send files without fear of having their identities leaked.

Illegal Activities

Despite the legitimate uses for the Dark Web, its reputation for illegal activity is well deserved. The unfortunate truth is that nothing is off limits on the Dark Web. In these hidden and anonymous segments of the Internet, users have the ability buy weapons, child pornography, credit card numbers and other sensitive leaked information. The most well-known Dark Web black market was the Silk Road, an online market where users could anonymously purchase illegal drugs. The Silk Road was launched in 2011 and was shut down by the FBI in 2013. According to the FBI, in less than two years of operation, the Silk Road made an estimated $1.2 billion in revenue.

The Dark Web recently gained mainstream media attention again, this time involving a ransom regarding the data stolen from the March 2017 hacking of the consumer credit reporting agency Equifax, Inc. While information regarding the data breach is still coming to light, the alleged hackers have demanded 600 Bitcoins (approximately $2.5 million at the time of writing) in exchange for the sensitive information of the 143 million people who fell victim to the cyberattack. Currently, it remains unclear how hackers will use the stolen personal information and if that data will be posted to the Dark Web.

If that data is posted, it would not be the first time sensitive information would be disclosed on the Dark Web. In 2015, for example, hackers stole and released account information for some 32 million users of the AshleyMadison.com website. Included in the 9.7 gigabyte data dump were the names, passwords, addresses and phone numbers submitted by the users of the site.

Practical Business Solutions

So, what can a business do prevent against its data being compromised, and to discover whether its data is available for viewing or purchase on the Dark Web? There are companies and professionals dedicated to providing this type of cybersecurity service.

On the prevention side, consultants create preventative measures, such as creating a special encrypted hash of data that may prevent other parties from using it, and to allow the company to identify and recognize its stolen data if discovered. And other companies may apply digital watermarks requiring users to go through an authentication process prior to accessing the files, and potentially even preventing hackers from copying and pasting the data in a separate file.

On the monitoring and detection side, there are security companies that will customize a plan to search the Dark Web using terms and keywords critical to a particular company, and then analyze all collected data to determine whether the company's information appears to have been compromised. These companies may also be able to provide information as to threats that may affect an entire industry.

Conclusion

As a part of an overall information security assessment, smart, forward-looking businesses would be well-served to consider whether a Dark Web scan would be a reasonable and appropriate weapon to add to the security arsenal.

***** **Elizabeth (Lisa) Vandesteeg** is a partner and J**effrey Goldberg** is an associate at Sugar Felsenthal Grais & Hammer. Ms. Vandesteeg focuses her practice on bankruptcy, business divorce, partner and shareholder disputes, and privacy and data security issues. The authors can be reached at evandesteeg@sugarfgh.com and jgoldberg@sfgh.com, respectively.