Kaspersky For Business

The Dark Web: Myths, Mysteries and Misconceptions

The dark web. It sounds like some mythical realm where cybercriminals operate anonymously and are shrouded in secrecy. While the dark web does provide a haven for criminals, the truth about how it operates is often much more mundane than that. Many companies who are breached learn that their data is for sale on the dark web, so naturally, they have many questions. By shedding some light on this dark topic, we hope to clear away some of the murkiness and help you to understand how you can protect your company.

What is the dark web?

Dark Web

The dark web consists of anything that is not commonly indexed on the surface web and on search engines like Google. It forms a part of the deep web and can only be accessed using special software, such as the Tor browser.

In a recent analysis of the dark web by Securelist, many of these sites had a short lifespan. Most dark web sites were active for at least 200 days, but usually not more than 300 days. Some were online for less than two months.[1]

The dark web does take some level of technical sophistication to access. It's not just a matter of downloading the Tor browser and typing in a URL, so people need to put in some effort in order to gain entry.

Deep Web

The deep web is also known as the hidden web or invisible web, and it is comprised of any content not accessible to search engines. Estimated to be 500 times larger than the surface web, the deep web includes such content as proprietary corporate data, confidential public data protected by government regulation, and commercial information accessible only to select groups of people such as subscribers, private email, and private social media content. Examples of deep web content include that contained on university library sites, NASA or LexisNexis.

Surface Web

The surface web is the indexed web that all of us know, including search engines like Google. Estimates vary about how large the surface web is, some saying it is only 1 percent of the total content that is actually on the web. Others say that figure is wildly exaggerated. Current estimates that the surface web contains over 4.6 billion pages seem to be accurate. All can agree that it is growing exponentially every year.[2]

[1] Law enforcement agencies in Tor: impact over the Dark Web

[2] World Wide Web Size

What is Tor?

Tor stands for "the onion router" and is a method for anonymizing data. It actually refers to two things—the network and the browser. The network constitutes a large number of volunteer computers that run a specialized server application. The browser enables users to both hide their identity behind anonymizing software and access special services only available through the Tor browser.

Run by activists who are dedicated to privacy and anonymity, the Tor Project is a non-profit organization that supports the network and develops the software. The technology upon which Tor is based (.onion) was developed back in the 1990s by the U.S. Navy in order to protect intelligence communications. Today, the U.S. government, specifically the U.S. Department of State Bureau of Democracy, Human Rights and Labor, remains a major funder of the Tor Project.

How does it work?

The technology behind Tor is open source, which means that programmers and experts can see into the source code. Unlike some virtual private networks (VPN), Tor does not have a commercial stake in collecting user data and they are committed to remaining non-profit. **More than 17.5 million downloads of Tor have been recorded to date.**[3]

Despite its anonymizing mechanics, Tor is certainly not completely untraceable. For example, if you access sites on the surface web from the Tor browser, you can still be identified. And due to its layered, anonymizing technology, the Tor browser is a little slower than your normal connection.

Who uses Tor?

The Tor Project claims that more than 2 million people use Tor daily. But despite the reputation of the dark web as being a haven for criminal activity, a recent survey concluded that only 45% of .onion sites appear to host illegal activity.[4] And it's not as vast as some people have made it out to be. While the surface web hosts billions of different sites, it is estimated that Tor hidden sites number only in the thousands, perhaps tens of thousands but no more. Therefore, we can conclude that its reputation for being a place where criminals go to hang out is not entirely accurate—or at the very least, not a complete picture of the situation.

In fact, many use Tor for perfectly legitimate purposes. Activists from countries that suppress freedoms, journalists looking to protect their sources and even law enforcement and the military use Tor to establish secure communications, avoid surveillance and get around censorship. In countries where Facebook is banned, Tor has even launched a hidden version of the site where more than 1 million users can access the social networking platform.

Many also think that merely downloading the Tor browser is a sign of criminal activity. While law enforcement and intelligence authorities may monitor Tor downloads, it is not illegal to do so, although some countries do view it as a signal of possible nefarious activity.

[3,4] *15 Things You Need to Know About Tor*

Myths and Misconceptions

Like anything that seems shrouded in mystery, there are rumors about the dark web that are inaccurate or simply untrue. Since criminals do operate on the dark web, often selling stolen company data, it is important for businesses to understand what they are dealing with. To that end, we'd like to clear up a few things.

The dark web is not necessarily a vast underground den of thieves. While almost half of the dark web appears to be dedicated to criminal activity (see *What is Tor?* section), a large portion of Tor users are those who are in need of privacy or protection for legitimate reasons. In countries where internet use is suppressed, people who seek out freedom from censorship use the dark web to communicate and share information. For journalists, many value the anonymity of the dark web to protect their sources. In fact, the *New York Time*s even has a secure lockbox on the dark web for whistleblowers or other sources. Political dissidents who need protection from their governments use the dark web to communicate with the rest of the world. It is indeed true that the dark web is used for criminal activity, but that activity can also be found in vast numbers on the surface web.

It's also a popular myth that major crime syndicates operate on the dark web when, in fact, the average criminal participant on the dark web is a small-scale hacker. Malware is widely available on the dark web, and the dark web is full of scams. It should come as no surprise that criminals don't just steal from businesses and individuals but also from each other.

The iceberg analogy is a big exaggeration. It is often said that the dark web is like an iceberg with a vast amount of the content located beneath the surface where only a select few can find it. But the dark web is not nearly as big as people think. In fact, compared to traffic on the surface web, the dark web is tiny. Approximately 2 million people use Tor daily, and only a fraction of those are visitors to the dark web. Compared to the billions of people who use the surface web daily, you can see why the iceberg analogy quickly starts to melt away.

The dark web is not completely anonymous. Using the Tor browser makes you difficult to track but not impossible. Law enforcement monitors Tor downloads and often creates dark web sites to lure criminals, so there are ways for them to use the technology to catch a thief.

The dark web is not illegal. While downloading the Tor browser is not illegal, it may make you a person of interest to law enforcement. Authorities know that people sometimes start out on one path on the dark web but end up someplace entirely different where they may get pulled into criminal activity.

Tales from the Dark Web

Law enforcement has had several notable success stories in bringing down criminal rings on the dark web. Silk Road and Alpha Bay are two such examples of a successful takedown of criminal dark web activity.

Silk Road

The Silk Road marketplace operated on the dark web and was taken down by the FBI in 2013, resulting in the arrest of Ross William Ulbricht who went by the pseudonym Dread Pirate Roberts. He was charged not only with the distribution of narcotics, including heroin and LSD, but also with a number of computer hacking crimes. Having boasted to *Forbes* magazine that he would never be caught, the FBI ultimately arrested Ulbricht inside the San Francisco Public Library.

Silk Road not only offered tens of thousands of listings for controlled substances, but also advertised hundreds of computer hacking services, as well as forged driver's licenses, passports, Social Security cards, credit card statements and other documentation that would enable identity theft. It also offered up some helpful hints, including hosting a community forum that offered guidance on conducting transactions on the site and tips for avoiding law enforcement. Silk Road was accessible only through the Tor network and only accepted payments in Bitcoins.

As for how much money changed hands, the charges against Ulbricht state that between February 2011 and July 2013, there were 1.2 million transactions on the site, involving almost 147,000 unique buyer accounts and 3,877 unique vendor accounts generating $1.2 billion.

The court documents provide information on Ulbricht's activity on the Silk Road platform, including how site administrators were managed and compensated, threats from competitors and details of an alleged murder for hire.

AlphaBay

In July of 2017, U.S. authorities along with law enforcement in Europe and Asia announced the takedown of the dark web's largest illicit market.

AlphaBay was a Tor hidden service whose transactions used Bitcoin, Monero, Ethereum and other cryptocurrencies. It sold everything from malware and hacking tools to drugs, counterfeit goods and even toxic chemicals. The market was also used to launder hundreds of millions of dollars. Sadly, the Department of Justice could attribute overdose deaths in Oregon and Florida to drugs purchased through AlphaBay.

AlphaBay had an estimated 200,000 users and 40,000 vendors on the site. More than 250,000 listings for drugs and toxic chemicals were found for sale, as well as 100,000 for malware, hacking tools, guns and more. To give a sense of scale, Silk Road had 14,000 listings at the time it was seized by authorities.

The takedown came after the July 5th arrest of the creator and administrator of AlphaBay, Alexandre Cazes, a Canadian living in Thailand who committed suicide in custody a week later. Cazes' assets and those of his wife were seized, including homes, luxury cars and a Thai hotel. According to the Department of Justice, Cazes owned millions in cryptocurrency from the AlphaBay operations.

What can you do to protect your company?

Very often, when cybercriminals steal data from a company, that data is sold to other criminals on the dark web. Finding your company's confidential information—or that of your employees or customers—on the dark web is a scenario that no company wants to encounter. Fortunately, there are key steps you can take to avoid this scenario.

Protect your information from being breached in the first place by using a multi-layered security solution. The best defense against cybercrime is installing the right technology to protect your organization. With a robust, multi-layered security solution in place, you can be sure to catch most attacks that target your workplace.

Educate your employees. Technology can only go so far in protecting your company's information. Your employees need to be educated to understand what to do, what not to do, and how to handle it if they suspect that a cyberincident has taken place. This includes teaching them the following:

- **Stay away from the dark web.** You may wish to prohibit employees from visiting the dark web during the workday or while they are using company hardware. Many people are curious about the dark web, but it is best not to give into that curiosity.

- **Stay away from public wifi.** Many employees are on the road or working remotely. We recommend avoiding using public—and unprotected—wifi, which is how many cybercriminals can infiltrate a network.

- **Teach employees what NOT to do.** Do not open or download attachments from unknown email addresses. Do not click on any links within email messages if you don't know the sender. Even the most savvy and dedicated employees can be tricked into these actions. It is important to educate employees to understand that even these simple actions can have huge consequences.

- **Look for a padlock or HTTPS in your browser window.** If employees must conduct sensitive transactions on work devices, it is important for them to understand how to practice secure browsing habits.

Keep all your software up to date. Software companies discover vulnerabilities all the time and send out patches and updates to their customers. Very often, IT departments have a weekly schedule where they set aside time to update software. It can be done quickly and efficiently, but it is essential that it is done regularly. Cybercriminals exploit these weaknesses to get at sensitive information.

Institute a strong password policy. Believe it or not, many breaches occur because employees are using simplistic passwords or using the same password for everything. By instituting password guidelines and policies, you will have built another layer of defense around your organization.

If you are breached, call in the experts. When it comes to cybercrime, you need to know what you're doing. First, notify your cybersecurity vendor or internal security teams to investigate. You may need to turn to law enforcement who are trained in how to deal with cybercriminals.

Kaspersky® Threat Intelligence

Tracking, analyzing, interpreting and mitigating constantly evolving IT security threats is a massive undertaking. Security Threat Intelligence Services from Kaspersky Lab gives you access to the intelligence you need to mitigate these threats, provided by our world-leading team of researchers and analysts. **Kaspersky Lab Threat Intelligence Services** include threat data feeds, botnet tracking, and APT intelligence reporting.

Kaspersky Lab's knowledge, experience and deep intelligence on every aspect of cybersecurity has made it the trusted partner of the world's premier law enforcement and government agencies, including INTERPOL and leading CERTs. Leverage this intelligence in your organization today.

True Cybersecurity for Business

Kaspersky Lab's True Cybersecurity approach combines multi-layered security with cloud-assisted threat intelligence and machine learning to protect against the threats your business faces. True Cybersecurity not only prevents attacks, but also predicts, detects and responds to them quickly, while also ensuring business continuity for your organization.

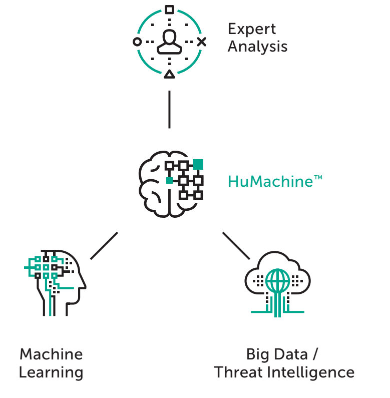
About Kaspersky Lab

Kaspersky Lab is one of the world's fastest-growing cybersecurity companies and the largest that is privately-owned. The company is ranked among the world's top four vendors of security solutions for endpoint users (IDC, 2014). Since 1997, Kaspersky Lab has been an innovator in cybersecurity and provides effective digital security solutions and threat intelligence for large enterprises, SMBs and consumers. Kaspersky Lab is an international company, operating in almost 200 countries and territories across the globe, providing protection for over 400 million users worldwide.

Learn more about cybersecurity: **www.securelist.com**

usa.kaspersky.com
#truecybersecurity

Kaspersky Lab, Inc.
500 Unicorn Park, 3rd Floor Woburn, MA 01801 USA
Tel: 866-563-3099 | Email: corporatesales@kaspersky.com


Expert
Analysis
HuMachine™
Machine
Learning
Big Data /
Threat Intelligence