THE QUICK START GUIDE TO DARK WEB SECURITY

BITbyBIT™
tech savvy. business smart.

Most Internet users probably think that popular search engines like Google, Bing, and Yahoo give users access to the entire Internet. They do not. In fact, sites accessible through traditional search engines barely scratch the surface of the web. Underlying mainstream Internet are hidden layers of information that most people never access. In reality, there are **three layers to the worldwide web.**

1. **Surface layer**
2. **Deep web**
3. **Dark web**

The surface layer includes public sites that a typical users can access via search engines or by typing a URL into a browser. Estimated to be 500 times larger than the surface web, **the deep web** (also known as the "invisible web") consists of content that is not indexed by standard search engines. These include email clients, online banking sites, and pages inaccessible to "crawlers," software that enables indexing for search engines.

Users can access some sites on the deep web if they have the URL, but others require login credentials. In contrast, **the dark web** (also known as the "darknet") is a small fraction of the World Wide Web that users can access, but only with special software like the **Tor** browser.

Tor is an acronym for "The Onion Router" and like an onion there are many layers of encryption in the Tor bundle. Originally designed by the U.S. Naval Research Laboratory, Tor anonymizes a user's location and identity by sending data across the Internet in a circuitous route, "hopping" along "volunteer" PCs and servers as connection points. Encryption at each point along the route makes it extremely difficult to connect a user to any particular activity.

The Legitimacy of the Dark Web

The anonymous browsing feature of the dark web certainly does attract legitimate, and even life-saving purposes. It offers “crawler-free” web sites and protection for user’s personal identities. There are numerous resources and educational information available without restriction, offering many discussion forums where people can share anonymously. According to Bruce Schneier, a computer security expert, “Internet anonymity is vital for people living in countries where you can be arrested, tortured, and killed for the things you do online. This is why the U.S. government was instrumental in developing the technology, and why the U.S. State Department continued to fund Tor over the years.”

Moreover, patients can seek medical advice through Tor if they do not feel comfortable asking their family doctor, as in the case of the effects of drug use. For example, Spanish doctor, Fernando Caudevilla, who goes by “Dr. X” began offering advice on the dark web in 2013. In his first three months, Dr. X responded to 600 questions and had 50,000 visits to his site. The dark web also provides journalists with a secure place to communicate with informants.

The Nefarious Side of the Dark Web

It is not difficult to imagine that the anonymity of the dark web draws nefarious users as well. These include people who want to purchase illegal narcotics, weapons and other such items, as well those wanting access to extremist group websites. One of the most infamous dark web storefronts was **Silk Road** where users were buying and selling illegal drugs and other goods purchased with bitcoin, a virtual currency hidden within the darknet. According to several sources, over one billion dollars of goods were sold on Silk Road alone before law enforcement took it offline. The shutdown resulted from a partnership between Europol and the FBI that investigated Silk Road and 400 other sites believed to be selling illegal drugs and weapons.

Many experts regard the shutdowns and arrests as a major breakthrough in fighting cybercrime. Yet, the arrest of only 17 people from the 400-plus operations, and the fact that it took law enforcement over two years years to investigate and act, reminds us that technology is dynamic and ever-evolving. Government policy needs to adapt accordingly to develop nimble and effective policies for protecting the public without stifling innovation and economic growth.

Despite shuting down these sites, nefarious users continue to conduct illegal activity. While it certainly makes sense to go after the marketplace/platform, the reality is that criminals will continue to engage in the same illegal acts as before because of the potential profit.

For more information and discussions on the unintended consequences of the Silk Road shut-down, read this TechDirt website.

The Dark Web is a Criminal Marketplace

The dark web is a hidden alleyway where cyber criminals also congregate to sell business information. In the past, large businesses were the main targets. Today, however, small and medium-sized organizations experience an increasing frequency of attacks. Sooner or later, hackers will attack all businesses.

Hackers can spend weeks or even months gaining access to a network by piecing information together. They seek bank account information, then attempt to redirect wire transfers by impersonating the email protocols of key staff such as the CFO or CEO. They can even create counterfeit vendors in a company's system and deliver money to checking accounts through automated clearing house (ACH) transfers or to actual P.O. boxes.

Cybercriminals also seek other key information:

Personally Identifiable Information (PII)

Names and addresses can be used to apply for credit cards, loans, file fraudulent tax returns, transfer money illegally, extort, blackmail and/or engage in hacktivism, the act of hacking a website or computer network to communicate a social or political message.

Phone Numbers

With pilfered phone numbers, criminals engage in phone scams, nuisance marketing and “vishing.” Vishing is the fraudulent practice of making phone calls or leaving voice messages where the caller purports to be from a reputable company to induce someone to reveal personal information, such as bank details and credit card numbers.

Email Addresses

An email address can enable access to online accounts, send unwanted spam or marketing information, and facilitate phishing.

Dealing With Phishing and Deception

To understand these concepts in the context of cybercrime, it is helpful to start with an analogy from history. Medieval castles typically had high, strong walls to defend against attacks from marauders and invading armies. The weakest points of their defenses were gates and sewage tunnels beneath the walls. These structures had to be carefully guarded against incursions. Yet, the biggest threats to a well-built castle were from traitors within the gates. They could bypass the defenders and open the gates or lead invaders through the maze of tunnels.

Likewise, cybersecurity depends on strong firewalls and passwords (gates) to keep out the enemy. It is very difficult for attackers to breach the perimeter defenses of a company with well-managed IT systems. So, they do everything they can to bypass the defenses and trick someone behind the walls to let them in through a gate. Absent a security flaw in the company's cyber-defense, criminals focus on more sophisticated ways to steal passwords to computers, email, and even the network itself. The main types of attacks are "phishing" and deception attacks where the attacker attempts to deceive a defender into giving up some useful information.

Don't Get Hooked by Phishing

Phishing can involve a hacker attempting to fool an unsuspecting user into accessing a malicious link or downloading an infected file through the practice of social engineering. Essentially, social engineering consists of manipulating, influencing, or deceiving in order to gain control over a computer system. The hacker might use the phone, email, "snail mail" or direct contact to gain illegal access. During a phishing attack, cybercriminals make contact that appears to be from a trusted source. They try to lure the defender into entering or providing login and password information, or to click a link that allows them to install software on a company's system. The unsuspecting employee provides the information, clicks the link or downloads the attachment, which then installs or activates malware or ransomware. So prevalent and dangerous is social engineering that Gartner, a leading IT consulting and research firm, calls it the single greatest security risk in the coming years.

These threats are so sophisticated that experts now categorize and define variants of phishing:

Pretexting

Using legitimate known information such as date of birth to gain further information.

Baiting

Baiting mostly occurs through a peer-to-peer or social networking site in the form of a download or a USB drive. A criminal might leave a USB drive with a “compelling” label in a public or conspicuous office location for someone to find. Once the “victim” downloads the malicious file, their computer is infected, thus allowing the criminal to take over the network.

Spear Phishing

After researching and identifying a special target in an organization, the “spear phisher” typically attacks by email appearing to be from a trusted source in an attempt to steal confidential information.

Diversion Theft

Usually a “con” where professional thieves targeting transportation or courier companies set up a diversion, tricking a company into making the delivery somewhere other than an intended location.

Water-Holing

This technique takes advantage of websites people regularly visit and trust. The attacker gathers information about a targeted group to find out which websites they regularly visit and then tests them for vulnerabilities. Over time, one or more members of the targeted group will get infected and the attacker can gain access to the secure system.

Quid Pro Quo

Latin for “something for something,” quid pro quo occurs when hackers pretend to be IT support. They call as many people as they can at a company to say they have a quick fix for a computer issue and instruct an employee to disable their antivirus software. If the employee does this, the hackers install malware and ransomware on the machine.

Rogue

Rogue security software is a form of computer malware that deceives users into paying for the false or simulated removal of malware. In recent years, rogue security software has become an increasingly serious security threat in desktop computing. It is a very popular method, and there are literally dozens of these programs.

So, how does a company defend itself against threats from the dark web?

There are measures at a company's disposal. If prepared for a breach, an organization can deploy more effective safeguards to make their data harder to interpret. And, the sooner the organization knows its data is on the dark web, the sooner it can act -- especially if there is a plan in place to mitigate negative consequences.

10 Tips to Develop a Cybersecurity Strategy

1. Companies should focus their efforts and think holistically. Over half of organizations in the U.S. use six or more resources to thwart cyberattacks. The more resources focused on attacks, the fewer an organization can devote to other mission-critical matters.

2. Don't assume one solution can do it all. About 60% of businesses use mitigation tools not built for distributed denial of service (DDoS) defense. Standard tools such as rewalls can create bottlenecks and accelerate outages.

3. Take a layered approach. About one-third of companies with DDoS-specific defenses (especially those that have been hacked) combine a mitigation tool with a mitigation service. The mitigation tool blocks the disruptive application and short-lived attacks, while cloud-based servers scrub the volumes of potentially malicious traffic.

4. Know the limitations in employing network security personnel.

5. Identify users that handle sensitive information and enforce two-factor authentication.

6. Review internal security policies and procedures, specifically those related to financial transactions to prevent CEO fraud.

7. Check firewall configuration and make sure no criminal network traffic is allowed out to command and control servers.

8. Leverage new-school security awareness training including frequent social engineering tests using multiple channels, not just email.

9. Have “weapons-grade backups” in place.

10. Work on the security budget to show it is increasingly based on measurable risk reduction and eliminate overspending on point solutions targeted at one threat or another.

Dark Web Monitoring

Dark web monitoring is one of the best proactive measures a company can take to protect itself.

It is important to understand that a company's ability to measure cybersecurity risk and implement a comprehensive cybersecurity strategy not only can avert a cyberattack, (risk mitigation) but in practical terms, helps to justify a return on the increasing investments in online applications. Risk measures can be related to company financials, performance, or technology, and to the frequency of attacks the organization thwarts. Each measure provides guidance for management teams in evaluating their overall risk.

A report from OWL Cybersecurity revealed that every Fortune 500 company has some level of risk from the dark web. Using an algorithm, OWL ranked companies by their "Darknet Index" score which reflects the extent of the company data that can be misused, and how the availability of breached data impacts its overall cybersecurity profile. You can find more on the Fortune 500 rankings here.

When hacked or stolen, company data often ends up for sale on the dark web in confidential and anonymous transactions. While there has been little indexing of dark web sites, OWL developed and maintains the most comprehensive database of 24,000 domains on Tor and other dark web networks throughout the world. The database updates continuously with 10 to 15 million pages per day and is searchable in 47 languages. This is key to organizations monitoring their data on the dark web.

More Facts about the Dark Web

- Every Fortune 500 company has a presence on the dark web.
- Amazon has the largest dark web footprint due to its enormous Internet presence and large amount of customer data.
- Overall, technology and communication companies have the highest Darknet Index score, which indicates they are the most attractive to hackers.
- Financial firms have lower scores, however, they are frequent targets despite their recent sizeable investments in cybersecurity.
- Companies with the highest scores have valuable intellectual property (IP) exposed on the dark web.
- Industry sectors that are vigilant and have invested in cybersecurity tend to have smaller dark web footprints and lower scores.

Companies should monitor the Darknet Index over time, noting not only their scores, but those of THEIR competitors. In doing so, companies can determine the efficacy of their cybersecurity efforts. They can then act quickly to address security shortcomings and mitigate damage.

There is another benefit to dark web monitoring that reveals the structure of compromised passwords, so then companies can change them. Many people use a password structure based on a keyword such as Maryjoe12!@. Old passwords that show this structure actually aids criminals since many people use the same password for other websites. In fact, according to the Center for Internet Security, between 31% and 55% of people use the same password at multiple sites. Sale of passwords on the dark web can bring cybercriminal as much as $2,800 in bitcoin for each transaction.

The barbarians are at the gate and a cyberattack can commence at any time. By actively patrolling the dark web, companies are able to identify holes in the defenses and shore them up before an attack occurs, or at least limit the damage after it does happen.