

THE DARKNET

Introduction

The adjective “dark” is used extensively in information security, and can sometimes be confusing. In this SAVANTURE brief we will shed some light on the Darknet and the Dark Web that resides there, parts of the Internet that few people ever see.

To begin, let's describe the Internet. The Internet is a network of networks that theoretically allows connectivity between any pair of nodes connected to it.

- Metcalfe’s Law states that the value of a network is directly proportional to the square of the number on users connected to it.
- As such the Internet is the most valuable information resource ever created by man.

However the part of the Internet that most people see and use only begins to scratch the surface...literally.

The Internet is Like a Vast Ocean

Think of the Internet like a vast ocean filled with digital content.

- Every day nearly 3 billion World Wide Web users try to reach an estimated 14 trillion web pages of digital content distributed across almost a billion websites.
- Amazingly, only about 1 percent of that digital content lies above the surface and is exposed to, indexed by and publicly accessible via search engines like Google.
- The remaining 99 percent lies below the surface of the water and is hidden from public view with restricted access.

The Surface Web

The 1% of the Internet that everyone is most familiar with is known as the Surface Web or the Visible Web. It is the content that lies above the surface of the water.

If one does a search with a tool like Google, the search results that you see come from in this part of the Internet. The digital content is generally public, it is accessible with any web browser, access does not require user identification or authentication, and can be easily discovered and indexed by search engines like Google that crawl the Internet looking for content.

To the novice this is the part of the Internet that is “free”. It is most definitely not . Giving up your privacy is how you pay to play.

This is the part of the Internet that generates revenue by tracking your usage and selling that usage data to advertisers for revenue. You, the user, are not the customer. You are the product. The customer is the advertiser purchasing data about your usage patterns.

The Deep Web

The 99% of the Internet that lies below the surface of the water is known as the Deep Web, the Hidden Web or the Invisible Web. This digital content is hidden from public view and cannot be discovered by the myriad of search engines crawling the Internet looking for public information.

The Deep Web is estimated to contain 500 times more digital content than the Surface Web. Major commercial databases, academic research, protected intellectual property, commercial applications, etc. reside in the Deep Web. Access to such digital content usually requires per-registration, a digital identity, authentication, authorization, access control, etc.

This is the part of the Internet that generates income from licenses, actual usage, fees and subscriptions rather than from tracking usage and selling that information about usage to advertisers for revenue.

Virtual Private Networks and The Deep Web

The TCP/IP protocol used for Internet traffic makes use of public routers to move packets of data over public network links. Such network traffic can be potentially intercepted and compromised when transmitted in the clear. Email is particularly vulnerable to such compromise since an email message is like a postcard that can be read by each intermediary that touches the message during its routing.

For this reason it is common to encrypt network traffic between the sender and recipient using standard encryption protocols such as SSL, TLS, IPsec, etc. Such a connection is known as a Virtual Private Network or VPN and traverses the public Internet in encrypted form.

Some people classify a VPN as a Darknet, but it really is not. A VPN is simply an encrypted tunnel that provides secure and exclusive connectivity between trusted peers over the Internet using standard protocols. The endpoints in the VPN are identified, authenticated, known and trusted by the other endpoints.

The Deeper You Go, The Darker It Gets

We will now attempt to shed some “light” on the subject of the Darknet and the Dark Web.

If you think of the Internet as a vast ocean, light can penetrate below the surface, but only so far. Light in this case represents transparency, identity and accountability. The deeper you go, the darker it gets, and the more opaque and anonymous you can become. Once you go deep enough you enter the netherworld of the Internet. This is the Darknet and the Dark Web.

- The Surface Web is public access but it also possesses accountability via cookies, website logs, network logs, browser histories, etc. Your IP address can tell others a lot about you, and most websites readily pick up artifacts about you that can be combined to make you far less anonymous that you think you are.
- The Deep Web is restricted, requires registration, an identity, some type of authentication, usually some form of payment, and logs just about everything you do as activity against your identity.

Where do you go when you don't want anyone else to know who you are, or where you are, or see what you are doing?

Darknets and the Dark Web

Some private networks employ non-standard ports, protocols, proxies and multiple, often nested layers of encryption and obfuscation of not just traffic but also the location where the message originated.

The intended purpose of such networks is to provide anonymity to the users connected to the network in addition to preventing disclosure of the information that is being shared. This is the netherworld of the Internet known as the Darknet, and the Dark Web.

Why Operate in the Dark?

Internet usage continues to grow exponentially on a daily basis. There are many instances where licit impenetrable security and anonymity is essential such as human rights activists, victims of domestic abuse, political dissidents repressed by hostile governments, journalists, etc. The Darknet provides such capabilities.

There are also illicit activities that take place over the Darknet, including copyright violation, criminal activity, child pornography, hackers for hire, etc. It is also the land of alternate digital currencies like

Bitcoin. Law enforcement and government security organizations struggle with the Darknet since it is so secretive and unregulated.

Information security companies like SAVANTURE use information gained from searching the Darknet to anticipate new security vulnerabilities and exploits and to develop plans and practices to defend against them.

There is nothing inherently good or evil about the Darknet. It is, however, a much more dangerous place to operate because of its lack of accountability, and most Internet users do not need to take on the risk and exposure of spending a great deal of their time there unless there is a good reason to do so and they know what they are doing.

How Does a Darknet Work?

The most common and well known Darknet implementation model is The Onion Router or Tor. Tor, like the ARPANET, was created by the US for military use and then released to the general public.

Tor was designed to enable individuals to use the Internet anonymously, so their activities and location cannot be seen by anyone else. Tor directs Internet traffic through a free, worldwide, volunteer network consisting of more than five thousand relays to conceal an individual's location and usage from anyone conducting any type of network monitoring.

The onion routing refers to nested layers of encryption like layers of an onion used to obfuscate communications such that they are only readable by sender and recipient. The nested encryption eliminates any instances where the communication is in the clear any any time during its transmission.

More information about Tor, documentation and the software needed to use Tor is freely available at www.torproject.org. Tor is not directly accessible using a standard web browser. Access to Tor requires installation of software that operates as a proxy between the user and the Tor network.

Conclusion and Summary

Most businesses aren't going to be aware of, nor should they be concerned with the Darknet day-to-day. However, there is a lot of information on the Darknet and your outsourced partner for security, or if your managing security internally, you should subscribe to a service that provides your organization awareness of any mentions of your company on the Darknet. Remember:

- The Internet like a vast ocean filled with digital content.

- Only about 1 percent of that digital content lies above the surface in the Surface Web and is exposed to, indexed by and publicly accessible via search engines like Google. This part of the Internet is “free” and funded by recording and selling your searching and browsing habits.
- The remaining 99% of the Internet is known as the Deep Web and is estimated to contain 500 times more digital content than the Surface Web. This section of the Internet contains commercial digital content and systems that usually require authentication and payment of fees to use.
- Part of the Deep Web is known as the Darknet and associated Dark Web, and is anonymous and inaccessible with a standard web browser. Tor (The Onion Router) network is the best known example of this part of the web.
- The Darknet has some legitimate uses but is also used for illegal and illicit activities and is more dangerous to use due to the lack of accountability and regulation. Most Internet users can do what they need to do in the Surface Web and the Deep Web.
- Companies like SAVANTURE search the Darknet to learn about new vulnerabilities and exploits and build safeguards and protection for our customers with what we learn.

SAVANTURE: We can help Simplify your Security and Compliance

***We are SAVANTURE. We can help.
Simply put, we make security easier!***

This is our mantra, and it drives everything we do. By stating our name boldly we show pride in its meaning and our commitment to work hard each and every day to build the reputation of the company and its people. When you hear SAVANTURE we want you relate the name immediately to commitment, trust, and see us as an extension of your business. We will strive to develop the highest level of trust with you and your organization. That means not only does SAVANTURE stand ready to help, but we are always actively working on your behalf to better protect your business and reduce risks to your Revenues, Reputation, and Regulatory Compliance. We believe this can only be achieved through our Corporate Strategy that provides our customers a seamless integration of intelligent and experienced PEOPLE, proven PROCESSES, and a best-in-class platform with the single motivation of helping our customers. Our success is helping organizations like yours to attain a higher degree of Information Assurance for their business. This allows you to better serve and earn the trust of your customers and business partners.

SAVANTURE’s suite of cloud based security tools can also be purchased individually or in any combination. SAVANTURE provides the same great tools used by our CISOs and staff to you. The Cloud Managed Security Services (MSS) suite includes:

- **Security Information Element Management Service (SIEM)**
- **Log Management Service (LMS)**
- **Vulnerability Management System (VMS)**
- **Authentication Management Service(2FA)**

In addition, as a full service Security Services Provider we provide:



Keeping it Simple Series: **DARKNET**

- **Genesis5** for those that need more than just the tools and desire a full operational solution providing 24x7 monitoring and management of your infrastructure, we deliver a full Managed Security Services Provider (MSSP) solution. We differentiate this solution through a higher level of policy collaboration and strategy bundling within Genesis5 through CISO advisory services.
- **Consulting Services** include packaged solutions for augmenting or providing program overview for your Chief Information Security Officer (CISO), Chief Privacy Officer (CPO), and IT Security Information assurance program



11951 Freedom Drive, 13th Floor, Reston VA 20190

Reach us at sales@savanture.com or +1.703.863.8568 or +1.888.556.1370