WHAT IS

THE DARK WEB?

TABLE OF CONTENTS

UNDERSTANDING THE DARK WEB AND HOW IT CAN AID YOUR INVESTIGATION

What is the dark web and how does it vary from the internet most of us use everyday? Which darknet should I use for my investigation? And how can I access it safely?

The dark web is an area of the internet only available via software clients. Perhaps best known for its association with criminal activity, the dark web has become infamous for its role in the illegal drug trade. But there are less nefarious reasons to access the encrypted dark web. In many countries, it allows demonstrators to subvert authoritarian regimes and provides a free and open internet model that can evade censorship and provide privacy.

For investigators, the dark web can hold crucial information that would be otherwise inaccessible. To acquire these datasets, it is important to understand each area of the darknet, the different clients available to use them and what precautions should be taken before diving in.

The dark web allows users to have encrypted, private access to information, websites and marketplaces. It cannot be found by search engines and requires specific software installation to access. The peer-to-peer sharing model allows for decentralization and anonymity amongst users and generators.

Is the dark web illegal?

The dark web is infamous for illicit underground dark web marketplaces selling contraband across international borders. The Silk Road rose to notoriety in 2011 after a longform article was featured on the then popular site, Gawker. The Silk Road was eventually shuttered by law enforcement agents in 2013. But since the bust, several more dark web markets have appeared in its wake, each seeming more competent then the last. Well-known dark web marketplaces for illegal drug sales and other items include Alpha Bay, Agora and countless others.

The digitized version of the black market means the contraband being offered can go further in larger quantities than any physical predecessor. It also sells more than the illicit substances it's often known for, contraband can include stolen data, illegal firearms and exploitation material. These dark web commerce sites are often powered by cryptocurrency, so the users can shroud their purchases in purported anonymity.

So with all this illegal activity taking place on to the dark web — is it really okay to log on to it? Believe it or not, it's not illegal to access the dark web. While the nature of the dark web has led to abuses and exploitations by bad actors, this underside of the internet is not illicit by nature. The dark web can be a beacon of free speech in authoritarian countries.

Free speech on the dark web

The dark web's role as an anonymous and reliable source of information to dissidents in foreign countries, alongside privacy enthusiasts, is important and legitimate. Many reputable websites have mirrored dark web versions of their website, including news organizations like the BBC, The New York Times and ProPublica. Just because you can't get there by popular search engine, doesn't automatically make it nefarious. But it's important to know the legal, security and privacy implications that come with before attempting to logon to the dark web for research or any other reason.

It may not be illegal to access the dark web, but doing so comes with considerable risks. The dark web is a place where stumbling into the wrong place (including illegal places) is easy to do. Be sure to read the risks and implications section to learn more.

Surface Web vs. Deep Web vs. Dark Web

If there is a dark web, is there a light web? Isn't the internet just the internet? There are many more layers to the world wide web than we realize. Many people, including researchers, are surprised to learn that what they consider the internet is actually just the tip of the iceberg and only accounts for a percentage of all the data online. Many also conflate the deep and dark web, which are entirely different in structure. The internet's searchable and unsearchable areas can be divided into three main buckets; surface web, deep web and dark web.

What is the surface web?

The internet most of us use daily — and probably assumed until now is the entirety of the internet — is actually what's known as the open web or surface web. It is the format of the web we're all used to, composed of open pages easily accessed by traditional search engines on any browser. Despite being where so many users default to, the surface web only accounts for a small portion of the entire internet.

What is the deep web?

The deep web is the next layer of internet information. These are sites that require login or subscription services, such as academic journals, court record databases or even services like Netflix. The deep web has some barriers to accessibility while being adjacent to the surface web and is typically accessed via the same browsers.

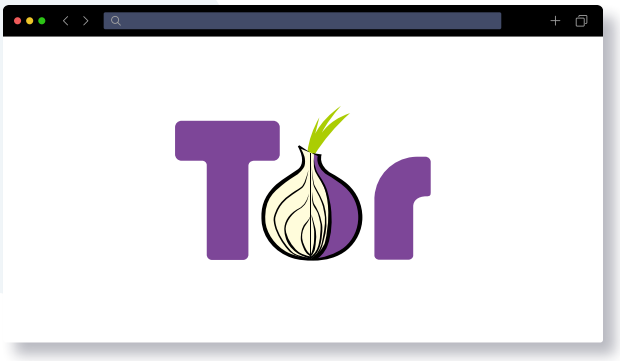
What is the dark web?

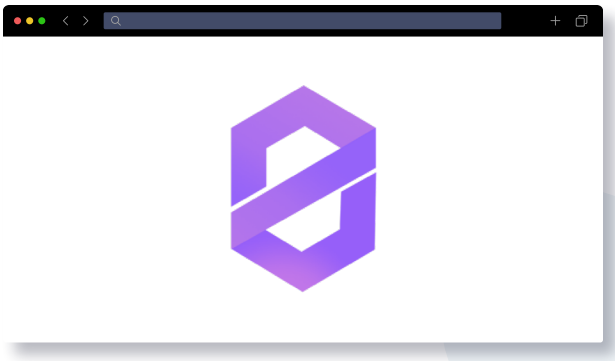
The dark web is the area of the internet that can only be accessed by using a specific software. There are different versions available, from the most well-known, such as The Onion Router (most commonly known as Tor), to the lesser used, such as Freenet. Each dark web requires it's own browser or software to access it. Many users of the dark web access it to remain anonymous, but there may be some fallacy in that assumption of anonymity.

Of all internet traffic, the dark web only composes a very small amount. But limiting your search to the surface web and leaving everything below untouched could be a mistake in your research. Information on the dark web's hidden sites could prove to be essential evidence.

The Dark Web Networks and Possible Risks

To access the dark web, a special software or client is needed. Each version of the dark web provides its own dataset, encryption services and risks from attempting to access it.





The Tor browser

The most commonly used darknet service is **Tor** browser. It stands for The Onion Router, developed by the U.S. Naval Research Laboratory in 2002. It was created to provide layers of encryption (hence the reference to onions) in order to anonymize communication between intelligence professionals. Tor operates almost like a traditional web browser, you can download it to your machine and use it to access different sites.

By diverting traffic through multiple nodes on its way to the client, the originator of files and sites can be hidden, making them more difficult to trace. The multi-layered encryption gives anonymity to its users and service providers alike. Many sites are given a random URL which ends in .onion. Anyone can download the Tor browser onto their machine, but like any other browser, there are still ways to track activity and hacking risks.

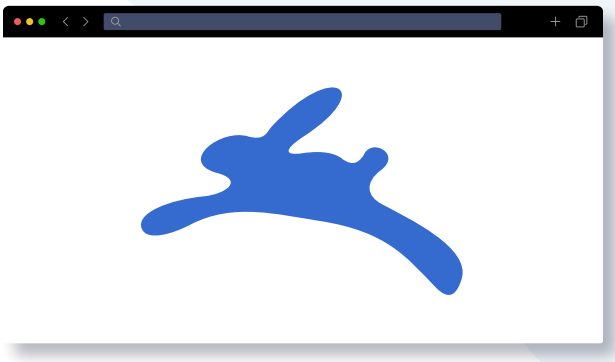
In the Tor browser, the biggest weakness is the point information travels between the exit node and the destination site. This unencrypted area presents a vulnerability to users.

ZeroNet

Lesser known darknets include **ZeroNet**, a peer-to-peer-based web hosting model developed in 2015 that doesn't use IP addresses or domains for websites. Sites are not hosted via a typical service and can only be accessed by public key. It makes sites free to create and share and almost impossible to shut down.

To access ZeroNet, you can use a regular browser with the application running in the background. Information from it can also be downloaded and made available offline. The content is made available via BitTorrent, which shares bits of information across many peers, each one hosting a piece of the information needed. By distributing the information through many hosts, it makes it nearly impossible to track down or scrub all of the pieces of content from the web. Each peer can then reshare and distribute themselves once they have downloaded it.

Unlike Tor, ZeroNet is not anonymous.



I2P, Invisible Internet Project

Another network is **I2P**, or the "Invisible Internet Project," released in 2003. Unlike the previous two sources for websites and file sharing, I2P focuses mostly heavily on encrypting communication between users. Unlike Tor, it encrypts via a peer-to-peer model instead of a single thread.

Access to I2P uses a browser and an application in the background. It provides untraceable communication by establishing one-way tunnels through peers. Each client becomes a node in the tunnel and tunnels then expire after 10 minutes. The system is referred to as "garlic routing." The one-way messages are encrypted for recipients, as well as their delivery instructions.

Freenet

Freenet is another peer-to-peer network for sharing decentralized data created in 2000. It is used in two forms – the "opennet" allows connection to any user, while the "darknet" connects only to friends. The ability to access only known contacts, provides a higher degree of trust than other softwares.

Access is created through a backend web application and requires a key to access. While it was originally used by dissidents to circumvent censorship laws, it is now popularly used by cyber criminals to offload stolen and malicious content.

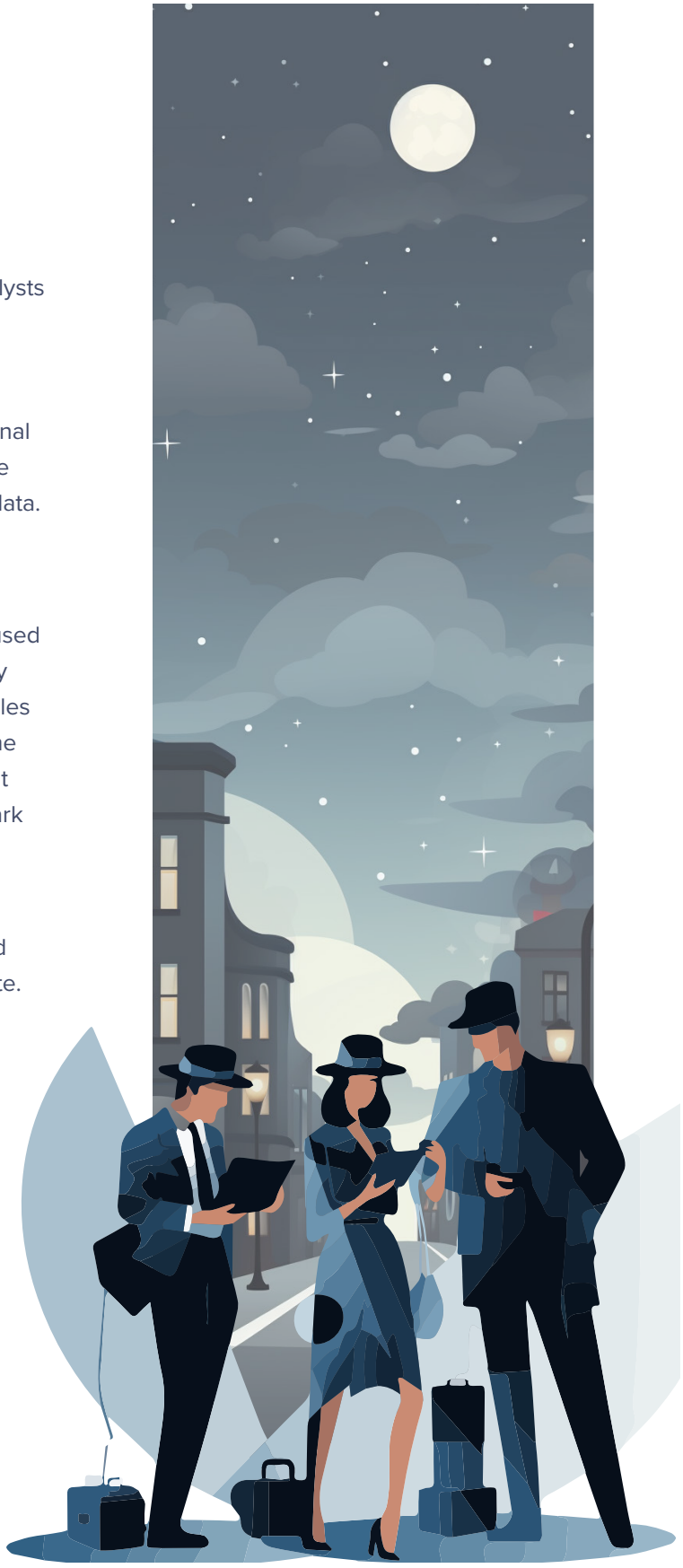
The traffic is routed via the closest nodes in the open net to create efficient routing. In the darknet, routes are set up manually and only trusted parties know your node's IP address. The inconvenience of the darknet infrastructure is outweighed by the security it provides. In this system, information stays available after the publisher has disconnected.

Should you access the dark web for your investigation?

Each of these darknet services can benefit investigators of law enforcement agencies, intelligence practitioners, financial services analysts and other researchers. The dark web can be a resource to help evaluate leads, corroborate or disprove information and track data leaks. The dark web can also provide context of how criminal marketplaces are operating and what tactics are being used to commit hacks or to track stolen data.

Many hackers discuss trade secrets in dark web forums. This information can help mitigate cyberthreats before they are committed or be used to recover leaked data from a breach. They may also post leaked passwords and accounts or sales of hacked devices. Financial crimes are often the subject of posts too. Stolen online bank account access or credit cards may be traced on the dark web.

When tips come in, following them in all places they lead may necessitate dark web access and help gain information on how bad actors operate.



Implications and risks of dark web research

Despite the benefits, many may have reasonable doubts and concerns about accessing the dark web. While accessing it is not illegal per se, it is important to take steps to mitigate any risks or potential legal threats, especially when entering areas of the dark web where illegal activity is being conducted. Dark web research requires careful policies, auditing abilities and security measures before logging on.

First, develop processes and procedures for your company and any employees who may be utilizing the dark web for their research. Be sure to consult your company's legal counsel in this step, as they will have the best guidance for your circumstances and organization.

Since dark web marketplaces or forums are often monitored by law enforcement, it can be difficult to distinguish between criminal actors and good faith investigators. Avoid implications or attributions by having a plan. Be sure to document your plan of operation before gathering information or accessing a criminal forum. Maintain a complete record of activities while on the dark web and have a policy in place for "rules of engagement" when on sites where criminal activity may occur.

For more resources on the legality of dark web access, consult Legal Considerations when Gathering Online Cyber Threat Intelligence and Purchasing Data from Illicit Sources by the United States Department of Justice.

Other risks include security of investigators and their machines. While the dark web's purpose is to provide some anonymity, there are still risks of malicious content or attribution when accessing. The safest way to gain access is by using a secure cyber service product.

How to Access the Dark Web Safely

Each dark web service can be accessed via self-installed software or a dark web browser from the services themselves. However, simply downloading the Tor browser or that of any other darknet could come with malicious content, analyst attribution or risk your company's IT or security policies, not to mention the potential for legal hot water if you were to accidentally stumble into the wrong dark web forum. Even relying on a virtual private network cannot protect you or your research from bad actors.

Analysts need a secure remote browser to access dark web sites. That means the ability to have all activity completely auditable to ensure the safety of the company and analyst alike. It also means the ability to manage attribution so angry site admins don't track a researcher back to their real-life persona, and protection from easy to click malware. A cloud-based isolated browser, such as Silo for Research, is needed to allow you full access with easy-to-use service that works in sync with your company's IT security and compliance. There are security controls in place and built-in auditing.

For more information on how tools like Silo can help you safely utilize the dark web in your investigation, visit our website or request a demo.