What is the deep web? A quick guide for beginners

There's a huge portion of the web that you can't access through a traditional search engine. In fact, analysts estimate sites like Google and Bing have indexed less than one percent of the total internet.

What's the other 99% out there? That's what is known as the deep web — a vast repository of information hidden from the causal web searcher. Security teams should take note. Most of the deep web is benign. But thanks to its sheer size and inaccessibility, the deep web provides a perfect hiding spot for bad actors like criminals and extremist groups. If you're not monitoring it regularly, your security team could overlook valuable sources of threat intelligence. The deep web can also provide a treasure trove of information for everything from emergency response and cybersecurity to identity resolution on a person of interest.

WHAT IS IT?

Simply put, the deep web refers to online content not indexed by traditional search engines. Analysts estimate the deep web consists of as much as 99% of the total internet — between 1,000 and 2,000 times larger than the "surface web" accessible to ordinary users. And the amount of content hosted on the deep web continues to grow each year.

In other words, most of what we often think of as the internet — Wikipedia, news sites, YouTube, and blog posts — is just the surface. Beneath that is a vast, mostly uncharted ocean of information.

So, what exactly can you find down there? Much of it is harmless.

The vast majority of the deep web consists of database-driven websites. For example, government pages like the Federal Reserve's FRED data service or the Securities and Exchange Commission's EDGAR search system fall into this category. This also includes academic journals, online marketplaces, and internet forums.

Beyond that, the deep web also consists of gated content behind a log-in page. This includes paid services like Netflix or The New York Times. Analysts also consider protected content like your personal email, online bank account, and Dropbox dog photo album deep web content, too.

Finally, websites can simply opt to exclude themselves from search engine results. Search engines also have difficulty tracking isolated pages with no inbound links. So these websites get lumped into the deep web bucket as well.

But beware: the deep web also contains a collection of anonymous networks known as the "darknet." The darknet is technically a subsection of the deep web. However, unlike the rest of the deep web, the darknet is encrypted. It is unindexed by search engines and unreachable through conventional web browsers like Chrome or Safari. To access a darknet site, you need specialized encryption software like Tor.

Explaining how this software works gets a bit technical. But essentially, services like Tor make your web browsing activities anonymous and untraceable. Tor almost completely hides information on a user's identity, location, and data transfers.

> A comprehensive study by Johns Hopkins University professor Thomas Rid found over half of the sites on the dark web cater to illegal products and services.

Such anonymity has many uses. In recent years, the darknet has emerged as an important tool for whistleblowers and political dissidents. But it also serves as a hub for black markets to distribute drugs, illegal pornography, pirated content, stolen goods, and much more.

WHY IS IT IMPORTANT FOR SECURITY PROFESSIONALS?

Given its sheer size, the deep web represents a valuable source of risk intelligence. And if you're not monitoring the deep web, you could overlook emerging threats against your organization. Some examples:

Data Leaks
Many corporate security teams focus on internal network logs and darknet feeds for signs of a data breach. But if you focus exclusively on these channels, you're likely to miss quite a lot. Data leaks can occur on more mainstream, deep web sources like chan boards, paste sites, and alternative social networks.

Executive protection
High-level executives represent tempting targets for attackers. Senior personnel may be picked out because of their job title, an unpopular decision, or recent public statements. And threat actors sometimes reveal their intention on deep web forums and communities. Constant monitoring of such channels can allow security personnel to identity, analyze, and mitigate risks to their executive team.

Passwords or accounts
Hackers often sell stolen account credentials, credit card numbers, and other personally identifiable information on dark web forums. Passwords represent especially valuable commodities in the online underworld because criminals know users often reuse them across multiple accounts. Searching for leaked information online allows security teams to spot data branches quickly, mitigating damage for customers and your company's reputation.

Vulnerabilities & exploits
Darknet criminals often share so-called zero-day or zero-hour vulnerabilities — a chink in a software's security with no current patches. Finding information on the zero-day vulnerabilities can allow tech teams to implement fixes before vendors release an update.

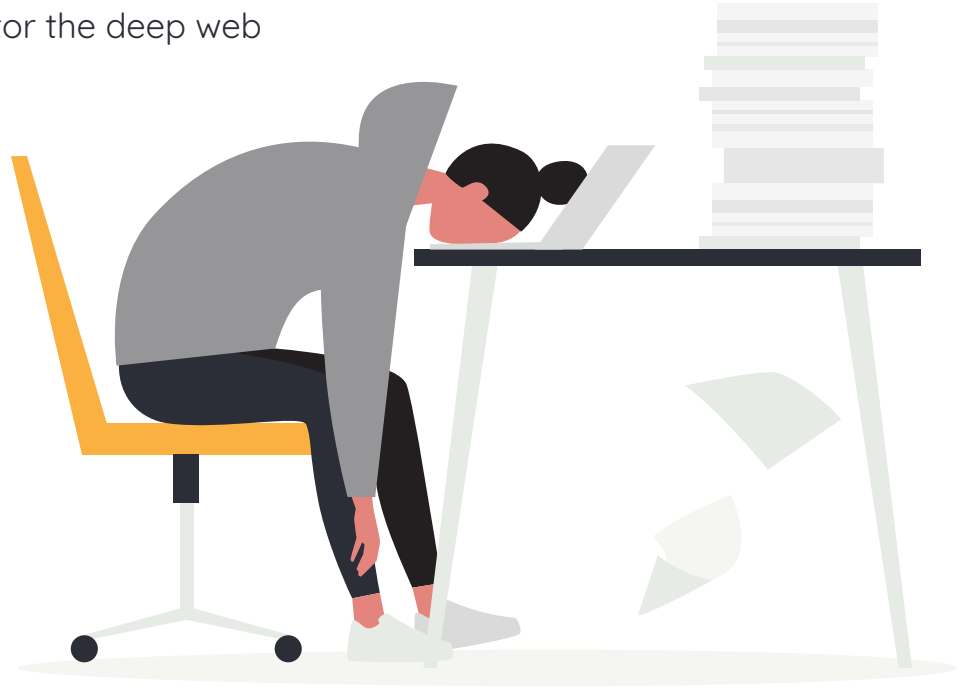
Insider threats
Insider threats often reveal themselves on the deep web. A malicious contractor could use darknet sites to sell credentials, intellectual property, stolen goods, or other corporate assets. Alternatively, a disgruntled employee could use a deep web channel to make threats against your organization. Monitoring whether your company's name appears on deep web sites can allow you to detect insider threats quickly, mitigating potential damage.

Misinformation
Rumors and conspiracy theories can spread quickly across the internet. Deep web monitoring can allow your security team to spot misinformation before it goes viral.

Stolen or counterfeit goods
Criminals will often attempt to sell stolen or counterfeit goods in online marketplaces like eBay, Kijiji, and MercadoLibre. Such listings, however, don't often turn up in Google or Bing search results. Monitoring these websites can protect customers, prevent theft, and safeguard your company's brand image.

You have two options to monitor the deep web for threat intelligence.

Firstly, you can set up your own monitoring system and search for information manually. Or second, you can purchase a Deep Web monitoring service.



Manual monitoring has a few advantages. Obviously, it's free. You can tailor your search to your organization's needs. And you can set-up a simple system with as little as a few links in your browser's bookmark tab.

The disadvantage of this approach comes down to time. Deep web monitoring becomes a labor-intensive task, checking a long and growing list of websites each day. And given the sheer size of the deep web, even a large security team will miss valuable information.

The darknet specifically presents more problems. Few search features make navigation difficult. You can accidentally stumble upon dark, disturbing content. And cybercriminals often attack unsavvy users with viruses, trojans, worms, and other computer malware.

Monitoring services make deep web intelligence gathering far simpler

Monitoring services, by comparison, make deep web intelligence gathering far simpler. A search that would manually take hours or even days, can be completed in seconds. Keyword filters can also find the most relevant content by clearing unrelated posts.

Moreover, some monitoring services allow security teams to set up automated alerts. An analyst can be notified on their phone or dashboard as soon as something of interest pops up on a deep web channel. This can save countless hours of trolling through websites.

But the best part of a deep web monitoring tool comes down to data breadth. Services will track dozens or hundreds of different channels — chan boards, petition sites, classifieds, paste sites, alternative social networks, etc. That reduces the chances of your security team missing any valuable intelligence.

In short, most of what we think of as the internet is only the tip of the proverbial iceberg. The bulk of content hosted online lies buried in the deep web.

Most of this content is harmless. But amid the mountains of information lies nuggets of valuable intel. A savvy security team should, therefore, include deep web monitoring into their threat intelligence program.