What is the Dark Web?

News outlets portray the dark web as a vast, seedy underworld. They picture hoodie-clad men behind desktops. Their faces shrouded in darkness. Here, you can trade anything: drugs, weapons, murder. Cue the ominous music.

The truth is a bit less exciting. In reality, the dark web is a pretty small place. And the activities that happen there are less sensational than widely believed.

Still, the dark web can serve as a valuable source of intelligence. And if you're not watching it, you could miss serious threats to your organization.

So in this article, we'll review exactly what is the dark web. We'll also look into what types of threats you can find there. And finally, we'll discuss how to navigate this world safely.

WHAT IS IT?

The dark web refers to encrypted online content not indexed by normal search engines.

Hatched by the U.S. Navy in 2002, it first served as a way for agents to navigate the internet without detection. Today, the dark web allows anyone to move online with more anonymity.

To access the dark web, you need to download a special browser — for example, you can download one called 'Tor'.

Tor resembles standard software like Chrome or Firefox. But unlike normal web browsers, Tor won't register your IP address when you visit a website.

Instead, the program bounces your request through several servers around the world. At each stage, Tor packages your personal information with layers of encryption — hence its nickname as the "onion" browser.

This process does a lot to hide your presence online.

Snoopers won't see your location, communications, or other activities. Additionally, Tor allows you to access hidden sites you can't find on standard web browsers.

WHAT CAN YOU FIND?

Contrary to media reports, the dark web is a small place. Researchers estimate it represents less than 0.001% of online content. And most of this material consists of dead or inactive sites.

Much of the more nefarious activities said to take place here also turn out to be exaggerated.

News outlets report sellers offering hitman services. Though in reality, most documented cases turn out to be scams.

Similarly, guns represent a smaller portion of dark web deals than often reported. Weapons, after all, are difficult to hide in the mail. And criminals would rather buy firearms from trusted sources over a faceless vendor.

Furthermore, Tor's anonymity actually serves a good purpose for ethical users.

The dark web represents an important tool for journalists and whistleblowers. Activists can publish information or discuss ideas with less risk of detection by authorities.

For this reason, news outlets, such as the BBC and The New York Times, publish mirrors of their websites on the dark web. This allows people in tyrannical countries to sidestep government censors.

Still, Tor's anonymity attracts a cast of shady characters.

Dark web forums serve as hubs for criminal activities. Popular products include drugs, stolen goods, pirated content, hacked passwords, and illegal pornography. In other words, niche products which can be easily sent online or through the mail.

Dark web advertisement for COVID-19 vaccine discovered by Europol.

The top selling product right now? COVID-19 vaccines.

Worldwide, demand for COVID-19 vaccines continues to outstrip limited supplies. This has created an opportunity for criminals, catering to those looking to skip long lines for treatments.

In one report, researchers at Check Point Software Technologies discovered "hundreds of advertisements" on the dark web for COVID-19 vaccines.

Criminal vendors pitched their treatments with headlines like **"Buy fast. CORONA-VIRUS VACCINE IS OUT NOW"** to **"Say bye bye to COVID19=CHLOROQUINE PHOSPHATE."** Prices range from between **$500.00** to **$1,000** for an unspecified dose.

Dark web advertisement for COVID-19 vaccine discovered by Europol.

Additionally, you'll find extremists lurking on the dark web.

Forums provide a haven for bad actors kicked off mainstream websites. Groups can exploit the Tor browser to fund operations, recruit new members, and plan upcoming attacks. All of which can occur with little fear of detection from authorities.

Estimates on the number of illegal websites hosted here vary. But a recent study by Johns Hopkins University found more than half of dark web content caters to criminal and extremist groups.

People sometimes use the phrases "dark web" and "deep web" interchangeably. These two concepts are related, but not exactly the same. You can find a quick rundown on the difference between the deep and dark web by clicking here.

WHAT THREATS & INTEL CAN YOU FIND?

Despite sensational claims, the dark web still serves as a great source of intelligence. And a failure to keep tabs on it could mean overlooking serious risks to your organization.

Credit Card Information

Stolen credit card details represent another bestseller. Going rates depend on the credit limit, country of origin, and freshness of the theft. And researchers have found a wide range for prices, from $0.11 to $986.00 per card.

Stolen Goods

Criminals use dark web forms to move stolen goods. Security teams often search for phrases like ‘new’, ‘unused’, or ‘still in the box’ alongside their brand names.

Insider Threats

Insiders often market illegal services, such as espionage, embezzlement, or malware deployment, on dark web forums. And because few firms watch for such threats, employees can engage in these activities for years.

Personal Records

Criminals can exploit leaked personal information, such as medical and financial records, to blackmail employees. Bad actors can also use this data for money laundering, spearfishing campaigns, and identity theft.

Direct Threats

Dark web forums often serve as a place for extremists to plan coordinated attacks. Bad actors, furthermore, could use such channels to make direct threats against company executives, employees, or properties.

Account Credentials

Stolen passwords represent a valuable commodity on the dark web. Forums provide a thriving marketplace for criminals to buy and sell leaked data. Though you can find many hacked account details posted for free on public paste sites. In total, researchers estimate more than 15 billion stolen credentials circulate on the dark web.

“How-To” Guides

Like in the business world, criminals love to share "best practices." Users post step-by-step instructions on how to conduct fraud against an organization. Articles can include supporting documentation, such as templates, scripts, images, and official seals.

Building Blueprints

Blueprints represent useful information for bad actors. For example, knowledge of a building's layout and security checkpoints can be invaluable for planning a robbery. If such documents have circulated on the dark web, it could leave your organization vulnerable.

Intellectual Property

Classified data, such as formulas, trade secrets, and product blueprints, are hot commodities. Medical research around new drugs and therapies also represent especially popular products.

Software Vulnerabilities

Software exploits often show up first on dark web forums. In fact, more than three-quarters of all disclosed vulnerabilities appear online before getting listed in the National Vulnerability Database. But by watching out for exploits on the dark web, cybersecurity teams can patch vulnerabilities quicker. That reduces the odds of unauthorized users gaining entry to your network systems.

In the above cases, dark web monitoring can pay dividends for your organization. And by reacting to threats quickly, you can mitigate the potential fallout.

For instance, you can change leaked credit card numbers with a phone call to the bank. A hacked password could be updated. Organizations can notify at-risk employees or customers.

Additionally, a heads up on an upcoming attack can allow teams to beef up their security measures and redirect defenses as needed.


Crawled from:
(President and CEO of)
▪ Current Address:
**** Confirmation ****
** Last Sale:
-- Sold for
[https://www.realtor.com/realestateandhomes-detail
- Address:
- Sellers:
- Buyer:
- Sold:
- Filed:
- Price:
[https:
Associated Phones:

Leaked personal information of a senior executive on the darknet, including wi-fi passwords, home address, and family member details, discovered by Navigator.

Spotting threats on the dark web presents a challenge. But it's worth the effort, given the value of intelligence available.

As mentioned above, accessing the dark web first requires downloading Tor. Once installed, the browser allows you to access both normal and dark web sites.

You can tell normal and dark web sites apart by their URLs. Dark web addresses contain the top-level domain '.onion' instead of '.com' or '.org'. URLs also use a scrambled naming structure that makes them difficult to find and remember.

For example, you can find the BBC's dark web mirror site at the address **bbcnewsv2vjtpsuy.onion**. Similarly, you can find The New York Times at **nytimes3xbfgragh.onion**.

Finally, specialized search engines like Torch, NotEvil, and Candle allow you to find relevant content. Additionally, directories like dark.fail or Reddit forums like **/r/darknet** also provide useful resources.

Hackers have many tactics to ensnare new users. Worse, it's easy to stumble upon disturbing or illegal content. So exercise extreme caution when online.

Careless surfing comes with serious legal and cybersecurity risks. It would be smart, therefore to employ a skilled technology analyst before building any type of dark web monitoring.

Alternatively, many companies find it safer and cheaper to buy services from third-party vendors. Dozens of businesses have built tools to collect and index dark web content.

These services can allow you to effectively watch the dark web for threat intelligence. And this data collection can be conducted without the risk of downloading malware, overlooking valuable information, or stumbling upon illegal content.

Be warned: the dark web has no shoratage of scams, malware, and phishing sites. Admittedly, media reports exaggerate the size and scope of the dark web.

Still, keeping an eye on this criminal underground provides valuable threat intelligence. If you know what types of assets are being monetized online, you can respond appropriately.

Just be sure to watch your tracks if you visit.

Best Practices for browsing the Dark Web

Use a VPN. Tor server nodes are public and well mapped. That means internet providers can detect when users have employed the browser. To be clear, using Tor and exploring the dark web is perfectly legal. But it will raise suspicion from authorities. So if you want to use Tor without drawing attention, it makes sense to route your traffic through a VPN.

Exercise caution when clicking on URLs. Always get a recommendation from a trusted friend before visiting any dark web sites. Or if this isn't possible, verify a URL from multiple sources.

Double-check URLs. A simple typo could lead you to dangerous or illicit websites. And it's easy to happen upon imagery you'd rather not see. That's why it's critical to verify the .onion URL you have entered is correct. It also makes sense to save correct URLs in an encrypted note for easy access later.

Don't download anything. Dark websites make very little use of HTTPS. And the anonymity of the technology makes it impossible to know who you're dealing with. For those reasons, it makes sense to avoid downloading any files while browsing.