THE DARK WEB: A GUIDE FOR BUSINESS PROFESSIONALS

By Dan Patterson

TechRepublic

INTRODUCTION

Hacking is a fact of life for businesses and consumers alike. Often, leaked data surfaces and is sold to miscreants—hackers, shady government organizations, and other bad actors—on the Dark Web.

The Dark Web—or dark net, backweb, onionweb—is frequently misunderstood. The network is used by legitimate actors, like law enforcement organizations, cryptologists, and journalists as often as by malefactors and criminals.

Here's a look at how the Dark Web works, the content that populates the encrypted internet, and the encryption tools needed to safely navigate the network.

EXECUTIVE SUMMARY

- **What is the Dark Web?** Much like the internet—or clearnet—that billions of people access every day from mobile and desktop devices, the Dark Web is a network of websites, forums, and communication tools like email. What differentiates the Dark Web from the clearnet is that users are required to run a suite of security tools that help anonymize web traffic. The Dark Web is used for both nefarious and reputable purposes. Criminals exploit the network's anonymity to sell guns, drugs, and humans, while organizations like the UN and Facebook use encryption to protect dissidents in oppressive countries.
- **Why does the Dark Web matter?** The Dark Web matters for two significant reasons: ideology and practicality. Where encryption exists, there also exists a large market of users who want to remain anonymous.
- **Who does the Dark Web affect?** The Dark Web affects every internet user. If your data was leaked as part of a government or corporate hack, it's for sale on the Dark Web.
- **How is the Dark Web accessed?** The Dark Web is most commonly accessed using the Tor security suite and the Tails flash-bootable operating system.

WHAT IS THE DARK WEB?

The Dark Web is a network of websites and servers that use encryption to obscure traffic. Dark Web sites require the .onion top-level domain, use non-memorable URL strings, and can be accessed only by using the open source, security-focused Tor browser. Because it's portable and disposable, Tails, a Linux-based operating system that boots from a flash drive, adds a layer of security to Deep Web activity.

Because the tools required to access Dark Web sites help protect user—and server—anonymity, in the past decade the Dark Web has become a magnet for criminal activity. The Silk Road, an eBay-like market for drugs and weapons, famously helped establish the market for peer-to-peer anonymous criminal commerce. The site grabbed mainstream headlines in 2013 when it was taken down by the FBI. In its place rose a number of copycat markets. The negative press, coupled with YouTube horror stories, glued the Dark Web's reputation to illicit behavior. Today, the Dark Web markets sell drugs, weapons, malicious software, and piles of consumer and sensitive corporate data.

But the Dark Web is not all bad news. ProPublica, a well-respected investigative news organization, has a Dark Web site to help the company securely communicate with sources. The United Nations law enforcement department, the Office on Drugs and Crime, monitors the Dark Web and shares data with the public and global police organizations. Even Facebook, the world's largest social network, has a Dark Web site relied on by more than one million users per month.

- **What is the clearnet?** Clearnet sites are sites that track user data, drop cookies, and share IP data. Examples of the clearnet are corporate intranet pages, secure bank pages, private social media accounts, and any site that does not use SSL.
- **What is the deep web?** The Dark Web and the deep web are often confused with one another. The deep web is a term applied to millions of pages that are not accessible to the public and not indexable by search engines like Google and Bing. Examples of deep web sites are corporate intranet pages and wikis, secure bank pages, and private social media accounts.
- **Are encrypted email technologies like PGP part of the Dark Web?** Not really, but PGP in particular is frequently used to obfuscate communication. PGP email tools and encrypted webmail services allow Dark Web site operators and users to communicate anonymously.
- **How are Bitcoin and the Dark Web related?** Bitcoin is not inherently anonymous, but scrambling the origin of a Bitcoin is a relatively nominal task. For this reason the virtual currency is the most popular currency used on the Dark Web and can enable criminal activity.
- **What is .onion?** To denote that the domain points to an encrypted site, Dark Web URLs end with the .onion suffix and are inaccessible to traditional browsers that lack proper security plugins.
- **How big is the Dark Web?** Not very big. The total population of Dark Web sites numbers only in the hundreds of thousands. Dark Web sites frequently disappear or are discovered and yanked from servers for violating local law. Security experts estimate that at any given moment there are between 10,000 and 100,000 active sites.

Additional resources

- How the Dark Web works (ZDNet)
- 10 things you didn't know about the Dark Web (ZDNet)
- This dark web market is dedicated to compromising your emails (ZDNet)
- Dark Web 101: Your guide to the badlands of the internet (CNET)
- The United Nations: "We're all facing the same global cyber-threat" (TechRepublic)
- Four misleading myths about the Dark Web (TechRepublic)
- The light side of the Dark Web (TechRepublic)
- IBM Security takes us on a tour of the Dark Web (TechRepublic)

WHY DOES THE DARK WEB MATTER?

Though the name sounds ominous, the Dark Web did not hatch from some evil hacker lab. The Dark Web is simply a network of websites that require basic encryption technologies to be enabled before users can load content. These are the same technologies that protect passwords when users log on to bank portals and sites like Gmail and Facebook.

For this reason, the Dark Web is used by proponents of privacy and encryption. Organizations as diverse as the Electronic Frontier Foundation, Facebook, the US State Department, and the United Nations all argue vociferously that encryption is a fundamental human right.

The Dark Web is practical. The anonymity and security provided by the encrypted internet means the Dark Web is a haven for criminals, law enforcement agencies, freedom fighters, journalists, neo-capitalists, and curiosity seekers. The Dark Web is unlikely to vanish any time soon.

Additional resources

- Campaign 2018: How the dark web could hurt the midterm elections (CNET)
- Starting at $40, hackers can attack your business with services bought on the dark web (TechRepublic)
- Stolen data on the dark web is cheaper than you might think (ZDNet)
- Cryptocurrency theft malware is now an economy worth millions (ZDNet)
- A hacker is advertising millions of stolen health records on the dark web (ZDNet)
- The Dark Web: How much is your bank account worth? (ZDNet)

- Video: Here's why Facebook is buying passwords from the dark web (ZDNet)
- How hackers steal EHR data and sell it on the Dark Web (TechRepublic)
- How the cyber insurance industry detects the next big attacks (TechRepublic)

WHO DOES THE DARK WEB AFFECT?

Using the clearnet generates data. Consumers generate data every time they create a social media account, send a webmail message, or upload a photo from a smartphone. Governments and large corporations generate and oversee billions of records and sensitive files. This makes governments and companies theft targets, and today, data breaches are common.

Consumers and companies need to be aware that sensitive records are bought and sold routinely in anonymous markets. If you've been part of a corporate or government hack, your data is on the Dark Web.

The Dark Web is also a small haven for terrorists and organized crime. Most Dark Web-focused security firms, however, caution against exaggerating the risks and size of the encrypted internet. Global law enforcement is aware of, operates on, and works to combat illicit Dark Web activity.

Additional resources

- Access data for 70% of top US and EU websites is being sold on dark web (TechRepublic)
- Hackers peddle thousands of air miles on the Dark Web for pocket money (ZDNet)
- Software code signing certificates worth more than guns on the Dark Web (ZDNet)
- Dark web vendors are selling remote access to corporate PCs for as little as $3 (ZDNet)
- Publicity surrounding data sold on the dark web isn't always accurate (TechRepublic)
- Programmer tried to sell cyberweapon on dark web for $50M: Reminder to secure employees (TechRepublic)
- From the dark web to the "open" web: What happens to stolen data (TechRepublic)
- The price of your identity in the Dark Web? No more than a dollar (ZDNet)

HOW IS THE DARK WEB ACCESSED?

The best way to access the Dark Web is with Tor. An acronym for *the onion router*, Tor is an open source protocol and suite of plugins built on top of Mozilla's Firefox web browser. Tor helps anonymize the source and destination of web traffic by passing the machine's IP address through a network of similarly encrypted

IP addresses. The result is that web browsing slows down a bit as each request is bounced around the world, obfuscating user traffic.

For additional security, power users and experts also use anonymity-protecting operating systems like Tails. Tails is a Linux distribution that specializes in security and convenience. The operating system takes about 20 minutes to install on a flash drive and can be booted from the USB drive on nearly any machine in the world. Tails comes preconfigured with Tor and offers dozens of other security features.

There is no guarantee of privacy on the Dark Web. Tor recently warned users not to expect complete end-to-end privacy while using the network.

Additional resources

- How to safely access and navigate the Dark Web (TechRepublic)
- How to access Tor, even when your country says you can't (ZDNet)
- 10 Dark Web warning signs that your organization has been breached (TechRepublic)
- Here's what happens during a social engineering cyber-attack (TechRepublic)
- Gallery: The top zero day Dark Web markets (TechRepublic)
- Gallery: The top 10 Dark Web search engines (TechRepublic)

IMPORTANT CAVEATS

Both novices and experts should exercise care and caution when visiting the Dark Web. TechRepublic does not condone illegal activity or unethical activity. Offensive material can sometimes be just a click away. Browse at your own risk. Never break the law. Use the Dark Web safely and for legal purposes only.

CREDITS

Senior Director, B2B Editorial
Jason Hiner

Editor in Chief, UK
Steve Ranger

Senior Managing Editor
Bill Detwiler

Associate Managing Editor
Mary Weilage

Senior Editor
Alison DeNisco Rayome

Editor, Australia
Chris Duckett

Senior Features Editor
Jody Gilbert

Senior Writer
Teena Maddox

Chief Reporter
Nick Heath

Staff Writer
Macy Bayern

Associate Editor
Melanie Wachsman

Multimedia Producer
Derek Poore

Cover image: iStock/hunthomas

TechRepublic

ABOUT TECHREPUBLIC

TechRepublic is a digital publication and online community that empowers the people of business and technology. It provides analysis, tips, best practices, and case studies aimed at helping leaders make better decisions about technology.

DISCLAIMER

The information contained herein has been obtained from sources believed to be reliable. CBS Interactive Inc. disclaims all warranties as to the accuracy, completeness, or adequacy of such information. CBS Interactive Inc. shall have no liability for errors, omissions, or inadequacies in the information contained herein or for the interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.