Hacker Lexicon: What Is the Dark Web?
Por Andy Greenberg
Wired.com,19 noviembre 2014.

WITH THE RISE and fall of the Silk Road—and then its rise again and fall again—the last couple of years have cast new light on the Dark Web. But when a news organization as reputable as 60 Minutes describes the Dark Web as “a vast, secret, cyber underworld” that accounts for “90% of the Internet,” it’s time for a refresher.

The Dark Web isn’t particularly vast, it’s not 90% percent of the Internet, and it’s not even particularly secret. In fact, the Dark Web is a collection of websites that are publicly visible, yet hide the IP addresses of the servers that run them. That means anyone can visit a Dark Web site, but it can be very difficult to figure out where they’re hosted—or by whom.

TL;DR:
The Dark Web is a collection of thousands of websites that use anonymity tools like Tor and I2P to hide their IP address. While it’s most famously been used for black market drug sales and even child pornography, the Dark Web also enables anonymous whistleblowing and protects users from surveillance and censorship.

Hiding in plain sight
The majority of Dark Web sites use the anonymity software Tor, though a smaller number also use a similar tool called I2P. Both of those systems encrypt web traffic in layers and bounce it through randomly-chosen computers around the world, each of which removes a single layer of encryption before passing the data on to

its next hop in the network. In theory, that prevents any spy—even one who controls one of those computers in the encrypted chain—from matching the traffic's origin with its destination.

When web users run Tor, for instance, any sites they visit can't easily see their IP address. But a web site that itself runs Tor—what's known as a Tor hidden service—can only be visited by Tor users. Traffic from both the user's computer and the web server takes three hops to a randomly chosen meet-up point in the Tor network, like anonymous bagmen trading briefcases in a parking garage.

Just because the IP addresses of those sites are kept hidden, however, doesn't mean they're necessarily secret. Tor hidden services like the drug-selling sites Silk Road, Silk Road 2, Agora and Evolution have had hundreds of thousands of regular users; Anyone who runs Tor and knows a site's url, which for Tor hidden services ends in ".onion," can easily visit those illegal online marketplaces.

Not to be mistaken with the Deep Web

When news sites mistakenly describe the Dark Web as accounting for 90% of the Internet, they're confusing it with the so-called Deep Web, the collection of all sites on the web that aren't reachable by a search engine. Those unindexed sites do include the Dark Web, but they also include much more mundane content like registration-required web forums and dynamically-created pages like your Gmail account—hardly the scandalous stuff 60 Minutes had in mind. The actual Dark Web, by contrast, likely accounts for less than .01% of the web: Security researcher Nik Cubrilovic counted less than 10,000 Tor hidden services in a recent crawl of the Dark Web, compared with hundreds of millions of regular websites.

A few cracks of light

Though the Dark Web is most commonly associated with the sale of drugs, weapons, counterfeit documents and child pornography—and all those vibrant industries do in fact take advantage of Tor hidden services—not everything on the Dark Web is quite so "dark." One of the first high profile Dark Web sites was the Tor hidden service WikiLeaks created to accept leaks from anonymous sources. That idea has since been adapted into a tool called SecureDrop, software that integrates with Tor hidden services to let any news organization receive anonymous submissions. Even Facebook has launched a Dark Web site aimed at better catering to users who visit the site using Tor to evade surveillance and censorship.

Just how completely Tor can evade the surveillance of highly-resourced law enforcement and intelligence agencies, however, remains an open question. In early November, a coordinated action by the FBI and Europol known as Operation Onymous seized dozens of Tor hidden services, including three of the six most popular drug markets on the Dark Web. For now, just how the feds located those sites remains a mystery; Some security researchers speculate that government hackers used so-called "denial of service" attacks that flood Tor relays with junk

data to force target sites to use Tor relays they controlled, thus tracing their IP addresses. Or they may have simply used old-fashioned investigative techniques such as turning administrators into informants, or found other hackable vulnerabilities in the target sites.

Either way, the message is clear: Even on the Dark Web, it only takes a few small cracks to let the light in.

Hacker Lexicon is WIRED's explainer series that seeks to de-mystify the jargon of information security, surveillance and privacy.