O'REILLY®

Patrolling the Dark Net

What You Don't Know Will Hurt You

Mike Barlow & Gregory Fell

Patrolling the Dark Net

What You Don't Know Will Hurt You

Mike Barlow and Gregory Fell

Beijing • Boston • Farnham • Sebastopol • Tokyo

O'REILLY®

Patrolling the Dark Net

by Mike Barlow and Gregory Fell

Printed in the United States of America.

Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.

O'Reilly books may be purchased for educational, business, or sales promotional use. Online editions are also available for most titles (*http://safaribooksonline.com*). For more information, contact our corporate/institutional sales department: 800-998-9938 or *corporate@oreilly.com*.

Editor: Courtney Allen
Production Editor: Shiny Kalapurakkel
Copyeditor: Dianne Russell, Octal Publishing, Inc.

Interior Designer: David Futato
Cover Designer: Randy Comer
Illustrator: Rebecca Panzer

July 2016: First Edition

Revision History for the First Edition

2016-06-15: First Release

While the publisher and the authors have used good faith efforts to ensure that the information and instructions contained in this work are accurate, the publisher and the authors disclaim all responsibility for errors or omissions, including without limitation responsibility for damages resulting from the use of or reliance on this work. Use of the information and instructions contained in this work is at your own risk. If any code samples or other technology this work contains or describes is subject to open source licenses or the intellectual property rights of others, it is your responsibility to ensure that your use thereof complies with such licenses and/or rights.

978-1-491-94427-1

[LSI]

Table of Contents

Patrolling the Dark Net

If you've ever been burglarized, you know the drill: police officers arrive, they look briefly around your home, and then they ask you for a detailed list of the stolen items. In some cases, the stolen items are recovered within a few days and eventually returned.

When cops find stolen goods quickly, it's most likely because they know where to look. Burglars aren't interested in keeping your flat-screen monitor and Xbox; they want cash. They bring their loot to a middleman (also known as a *fence*) who specializes in reselling stolen goods. Usually, the stolen goods sit in the fence's shed or basement until a buyer is found.

Cybercrime is similar to burglary, except that cyber criminals steal electronic information rather than electronic gear, and the stolen information sits in hidden databases instead of someone's basement.

There's also another critical difference between cybercrime and ordinary burglary: when your home has been burglarized, you know it immediately. There are broken doors, smashed windows, and an open space on the wall where your widescreen television was mounted. When a cybercrime is committed, it often remains undetected for weeks or months. The time lag creates an advantage for cyber criminals, giving them an edge that ordinary criminals rarely enjoy.

Underneath the Surface

Detecting cybercrime and defending your organization from cyber criminals requires understanding how the bad guys operate and gaining a basic familiarity with the parts of the Internet they use to commit their crimes.

The part of the Internet we're most accustomed to using is the World Wide Web, or *surface web*. We use search engines such as Google, Yahoo, and Bing to find information on the surface web. The look, feel, and protocol (HTTP) of the surface web have become familiar.

Underneath the surface web is the *deep web*, a much larger pool of information that is largely untouched by search engines. No one exactly knows the size of the deep web, because most of it is beyond the reach of traditional search engines.

Typically, information resources on the deep web are accessed through direct queries. In other words, you need to know precisely what information you're looking for and you often need to have some kind of authorization to obtain the information. The vast majority of information on the deep web is public—it's just not as easy to find as the information on the surface web.

Examples of deep-web resources include court records, government records, medical and legal databases, economic data, election data, newspaper and magazine articles, scholarly content, corporate intranets, and content from older or inactive websites. On any given day, the majority of people using the deep web are likely to be librarians, archivists, and government workers.

The *dark net* is a smaller realm existing within the deep web. Information on the dark net is often intentionally obscured, hidden or anonymized. Accessing the dark net requires special tools and software—nobody accidentally "stumbles" into the dark net.

That makes the dark net an ideal place for people whose interests or careers require secrecy and anonymity. The dark net is where people go when they want to connect on the sly with political dissidents, whistleblowers, informants, undercover detectives, investigative reporters, espionage agents, cyber criminals, spammers, drug dealers, child pornographers, terrorists, and assassins.

Even if the dark net isn’t the nicest neighborhood on the deep web, many see it as a sacred bastion of privacy in a global culture of omnipresent computing, ubiquitous wireless access, high-speed digital networks, and continual surveillance.

You don’t need to be a libertarian or an anarchist to appreciate the value of privacy or to question the degree to which governments impose their authority. The dark net is a place where people are free to express their innermost thoughts and act on their desires. Most of those thoughts and desires are harmless. Some of them are dangerous.

Economic Whack-a-Mole

Resistance to authority is a common thread in history. Flouting rules, circumventing convention, and bending laws are human traits. When there’s an economic incentive, the urge to ignore or subvert the law becomes even stronger.

Black markets thrive when governments make it difficult for people to obtain goods and services needed for survival or enjoyment. In a sense, black markets are symptoms of dysfunctional free markets. If you could buy everything you wanted legally, there would be no need for black markets.

For example, we can view the proliferation of file-sharing networks as a natural reaction to the Digital Millennium Copyright Act (DMCA), which was enacted to curtail the rise of digital file sharing. In a similar way, the emergence of online markets for illegal drugs can be seen as a natural response to the “war on drugs,” which actually made it more dangerous for people to buy drugs on the street.

It’s a never-ending game of economic whack-a-mole in which governments pass laws restricting certain types of behaviors and black markets emerge to help people circumvent those laws.

There are also black markets for ideas. Those of us who are fortunate enough to live in free and open societies often forget that our freedoms of expression are not universal. In many parts of the world, expressing ideas that your government finds objectionable will get you thrown in jail—or worse. For people living under authoritarian regimes, the dark net provides a forum for sharing ideas anonymously.

Even in free societies, consumers are pushing back at being treated as raw material by large search engine firms, which create value by converting consumer browsing habits into digital marketing assets. Although it's marginally less creepy than the plot of *Soylent Green*, the process by which Internet companies now routinely collect our data, process it, and then sell it back to us as a product is troubling to many people.

It also raises the question of how much surveillance is too much. Companies that collect data about our online habits refer to their practices as *traffic analysis*. But in practice, there is little difference between traffic analysis and surveillance. Internet companies know what you're reading, listening to, and watching. They also know who you're communicating with, and when.

The dark net is a place where people can escape from that kind of routine surveillance. If the idea of sharing your browsing habits with a third party doesn't appeal to you, the dark net is a haven.

Not all security experts see the dark parts of the web as unredeemable minefields of existential danger. "The dark net isn't all bad. It provides anonymity, which means folks of all walks of life can be found there," says Justine Bone, an independent cyber security consultant. She agrees that large companies—especially large companies in highly regulated industries—should monitor the dark net for signs of information theft.

"It's no more risky than surfing the regularly accessible parts of the web," says Bone. "One could even argue there's less malware targeting folks over the dark net. And we're already seeing companies such as DarkSum, which provides products and services for navigating the dark net."

Anonymity Rules

The existence of the dark net is scarcely a secret. For dark net users, secrecy is less important than anonymity. That might seem like a fine point, but it makes all the difference. Anonymity is critical to the longevity of *sub rosa* networks, even after they become known to the public.

Ironically, the software most closely associated with dark net anonymity was developed at the United States Naval Research Laboratory in the mid-1990s. *Tor*, an acronym for "The Onion Routing," is free software that makes it very difficult to trace Internet activity back to a user. Tor essentially routes Internet traffic through an open volunteer network of about 10,000 nodes, encrypting data multiple times as it passes randomly through successive nodes. Here's a brief description from the Tor Project website:

> The idea is similar to using a twisty, hard-to-follow route in order to throw off somebody who is tailing you—and then periodically erasing your footprints. Instead of taking a direct route from source to destination, data packets on the Tor network take a random pathway through several relays that cover your tracks so no observer at any single point can tell where the data came from or where it's going.

What makes Tor incomparably useful is its ability to hide both the contents of a data packet and the header used for routing. As a result, the message itself is encrypted and it's difficult for a tracker to determine who sent the message or who received it.

The inventors of onion routing thought that it would be useful technology for open-source intelligence gathering and for protecting travelling Navy personnel, explains Paul Syverson, one of the researchers who pioneered Tor. Prior to the development of onion routing, Navy personnel could send encrypted messages while traveling, but had no practical way of completely concealing their Internet activities from watchful enemies.

Distributing Trust

Cyber criminals look for the most vulnerable parts of your systems, and attack you there. Every segment of every system should be considered vulnerable and susceptible to attack, even the parts that are designed to be secure, such as virtual private networks (VPNs).

The problem with a VPN is that other people can still "see" when you are using it. Messages going in and out of VPNs are recognizable, which means you can be identified by people who want to violate your privacy or steal your secrets.

"Your VPN is a single point of trust, which means it can also become a single point of failure," says Syverson. "Maybe someone hacked into it. Or, if it's a commercial VPN, they might be selling your data. Or maybe your VPN is bought by another company that will sell your data. So you have to worry about your VPN. And even if your traffic is encrypted, other people can still see that you're logging into a secure network, which identifies your interests."

Syverson and his colleagues set out to develop a practical alternative to the single point of trust/failure scenario facing agents in the field or anyone who requires anonymity to remain safe and secure.

"We came up with the idea of separating identification from routing so the data packet can get where it's going without the network automatically knowing who sent what to whom," Syverson explains. "Onion routing distributes the trust around the network so even if one point is compromised, your identity isn't revealed."

Onion routing preserves the anonymity of the sender and the receiver of a message, creating an end-to-end continuum of privacy.

Because Tor is an open source project, anyone can download it and begin using it. By design, each additional node adds strength to the Tor community of users.

From Niche to Mainstream

What can we learn from the dark net and the technologies that enable it? A fair amount, as it happens. "There's a whole group of companies out there developing or providing services designed to answer growing concerns about privacy and security," says Dr. Shaun Brady, an expert on risk and data management who consults regularly for government and the private sector.

"Allowing your emails, searches, location, and transactions to be monitored and monetized in return for free services may remain appealing to many," says Brady. "But more people are waking up to the reality that in order to truly protect their privacy, they need to take back control of their digital identities."

A new generation of email servers and browsers provides anonymity to everyday users. New password management systems offer both security and manageability. "We're seeing new privacy services that are easy to navigate and easy to use. People are picking up on these services and they're becoming mainstream," says Brady.

Brady is among a group of security experts and cryptologists that recently formed the Identity Wallet Foundation, a nonprofit organization focused on grassroots-level privacy.

“We’re trying to make it easier for the average citizen to take advantage of the tools that are available,” he says. “You can’t preserve your privacy unless you have control over what you release into the world about yourself.”

Online privacy begins with hiding your computer’s IP address. That will require installing Tor or similar software. After you’ve done that, there are email services you can use that will keep you anonymous, such as TorGuard Anonymous Email, Secure Mail, Guerrilla Mail, The AnonymousEmail, and Tutanota.

For anonymous purchasing, there are cryptocurrencies such as Bitcoin, Auroracoin, BlackCoin, Mastercoin, Ether, PotCoin, and others. Password management tools include Enpass, Keychain, LastPass, and mSecure.

Do any of those products or services, by themselves or in combination, offer total privacy and security? It would seem unlikely. But like seat belts and airbags in cars, they represent our common desire for greater safety.

The emergence of “privacy as a business model” also reflects our rejection of the idea that it’s okay to trade our innermost personal secrets for the privilege of using products that are free or reasonably priced.

Slowly but surely, we’re developing a more nuanced view of privacy. Back in 1999, when Scott McNealy, then the CEO of Sun Microsystems, told a group of reporters, “You have zero privacy anyway…Get over it,” it seemed like a shocking statement. Now it seems misinformed and short-sighted.

Most of us accept the fact that technology has transformed our lives. But that doesn’t mean we want to be treated as “data generators” for the information economy. Somewhere between total transparency and total secrecy is a balancing point. The dark net offers clues for finding that balance.

More immediately, the dark net and the dark web are the places to look for signs that your organization’s information systems have been hacked. If your confidential data has been stolen and is for sale, the dark parts of the Internet are where you can find it. That makes a dark net and the dark web worth patrolling, whether you do it yourself or with the help of experts.

Conducting Reconnaissance

Sometimes, months or even years can pass before stolen data surfaces publicly. According to the rumor mill in cyber security circles, stolen data from the Target and Sony breaches sat on the dark web—which is a collection of secretive websites operating within the dark net—for months before making headlines.

Experienced cyber investigators know the best place to begin looking for stolen information is on the dark web. Many security experts now recommend conducting regular, proactive reconnaissance of the dark web for the express purpose of making sure your company's confidential information isn't already out there, waiting to be bought and exploited by cyber criminals.

That said, you can't just go strolling across the dark web and blithely ask if anyone has seen your private data. Like a good undercover cop, you need to know how to ask questions without revealing your identity or accidentally breaking the law.

Mark Johnson is CEO of Sovereign Intelligence, one of several consulting firms specializing in helping companies deal with potential dangers posed by the dark net. A former Naval Criminal Investigative Service (NCIS) special agent and intelligence case officer, he understands the nuts and bolts of clandestine investigations.

It all begins with good defensive measures, but there's a catch: in the old days, the perimeter was much smaller and more manageable. Today, the perimeter is virtually limitless. "Companies should watch for conspiracies," says Johnson. "If you are able to extend the perimeter of your cyber security into these illicit domains, you can catch the conspiracy and potentially find out who's involved. Remember, it can be days, weeks, or months before an actual exploitation actually happens."

Johnson recalls an investigation in which a large firm learned that it had been hacked. The hacker had covered his tracks internally, but Johnson's team quickly discovered that one of the company's employees had offered to sell the stolen data on a criminal website in the dark web.

Plowing through the dark web and actually finding good information isn't easy, but it can be done with the right set of investigative skills and a certain amount of tradecraft.

“Part of it is just good old-fashioned research, where you’re doing search after search after search. Eventually, you start pulling in useful data and indexing the sites so you can go back,” he explains.

Last year, NASA and DARPA joined forces to index the deep web. If their partnership is successful and yields positive results, it will probably encourage entrepreneurs and investors to launch startups aimed at “commercializing” deep-web indexing. In the meantime, however, patrolling the dark web is mainly a job for cyber security professionals.

Does that mean every large company should set up a division to monitor the dark web? Probably not, says James Chappell, chief technology officer and cofounder of Digital Shadows, a firm that helps companies protect themselves from cyber attacks, loss of intellectual property, and loss of brand and reputational integrity.

“The dark web itself does not necessarily pose a direct risk to organizations,” Chappell notes in an email response to our questions. But because criminal syndicates now use the dark web, it would be foolhardy to simply ignore it.

“A whole criminal ecosystem has evolved over time, facilitating a growing new subversive economy,” writes Chappell. Different kinds of organizations face different kinds of risks from criminals specializing in various types of crime.

For example, banks need to worry about the theft and sale of financial data such as credit card numbers and bank accounts. Manufacturing companies need to worry about intellectual property theft that would compromise trade secrets. Hospitals and healthcare providers need to worry about keeping patient information secure and confidential.

“One of the best ways that organizations can mitigate those risks is to maintain a high level of awareness of the activities taking place online,” writes Chappell. Keeping an eye on the dark web can help you stay ahead of the criminals and align your security efforts more effectively to counter new and emerging tactics, techniques, and procedures (TTPs) used by the bad guys.

Gathering Threat Intelligence

Marc Goodman, a former LAPD investigator and author of *Future Crimes: Inside the Digital Underground the Battle for Our Connected World,* urges businesses to engage in "open-source intelligence gathering," which involves searching the dark web regularly for publicly available information that might provide indications of a breach.

"You need to be aware when your company data is floating around out there," says Goodman. "You need to be proactive and on the lookout. You need to know when people in chat rooms or channels are talking about hacking your company. The dark web is a great place to look for threat intelligence."

Goodman warns of an increasingly well-organized criminal infrastructure emerging within the dark web. It's all part of what he describes as a larger "technological arms race" between good guys and bad guys. From Goodman's perspective, it would be a mistake to rely primarily on law enforcement for protection from cyber criminals. It makes more sense, he says, for the burden of responsibility to be shared more widely across society.

But, he is not in favor of untrained individuals or small companies with limited resources conducting their own recon missions on the dark web. "You don't want people accidentally viewing child pornography on their corporate network," he says. "There's a level of investigative tradecraft required. The average systems administrator probably doesn't have the operational skills necessary to pass himself off as a hacker on the dark web."

DarkSum's website certainly appears to address mainstream concerns about the dark net:

> The DarkSum™ platform allows customers to safely search, monitor, and create custom alerts for information of interest in publicly available darknet systems.

It's far too early to tell whether the dark net will emerge as a growth market within the tech industry. But it seems entirely fair to say the dark net is worth watching and warrants a deeper dive.

Lurking Within the Perimeter

Companies must also be watchful for illicit usage of their networks and IT resources by cyber criminals operating from sites on the dark net or dark web. “A question you should be asking is, ‘Are our networks being used to support a dark net operation?’ That’s a potential hazard,” says Richard Moore, a managing director specializing in cyber risk at Alvarez & Marsal, a global professional services firm. “There were companies that had dark nets running on their networks and they weren’t aware of it.”

Cyber criminals will look for companies with large, decentralized IT systems and lax security. After the bad guys are inside your network, they can be hard to spot.

In addition to posing liability and reputational risks, cyber criminals operating inside your networks can disrupt your business. “If you’re running a highly customized application that requires a certain bandwidth and there’s a criminal also consuming that bandwidth, the criminal’s activity might put you offline, and then you’re in breach of contract with your customers,” Moore explains.

Companies should inspect their networks and systems regularly to make sure they are used exclusively for their intended purposes and not being used by cyber criminals, says Moore. Finding unauthorized peer-to-peer or friend-to-friend applications, or discovering unrecognized VPNs, would be telltale signs of improper usage and warrant deeper probing.

Shining a Light into the Darkness

Because the dark parts of the Internet also provide safety for people and organizations with legitimate reasons for seeking privacy, it would be imprudent to simply advocate in favor of measures to abolish or eradicate the deeper and darker layers, even when those layers provide temporary or occasional havens for criminals.

A better strategy would be learning and understanding as much about the dark net as possible, and taking advantage of its positive qualities to improve the security, safety and privacy of law-abiding citizens and companies.

An excellent resource is *Building Security in Maturity Model Version 6* (BSIMM6), a document based on a multiyear study of software security at dozens of major firms. BSIMM6 also highlights the evolutionary nature of cyber security and cyber risk.

It's entirely possible to imagine a future in which individuals or organizations will use Tor (or similar secure networks) routinely, much the way we lock the doors of our homes and our automobiles today, without the neighbors wondering what we're trying to hide.

About the Authors

Mike Barlow is an award-winning journalist, author, and communications strategy consultant. Since launching his own firm, Cumulus Partners, he has worked with various organizations in numerous industries.

Barlow is the author of *Learning to Love Data Science* (O'Reilly, 2015). He is the coauthor of *The Executive's Guide to Enterprise Social Media Strategy* (Wiley, 2011) and *Partnering with the CIO: The Future of IT Sales Seen Through the Eyes of Key Decision Makers* (Wiley, 2007). He is also the writer of many articles, reports, and white papers on numerous topics such as collaborative social networking, cloud computing, IT infrastructure, predictive maintenance, data analytics, and data visualization.

Over the course of a long career, Barlow was a reporter and editor at several respected suburban daily newspapers, including *The Journal News* and the *Stamford Advocate*. His feature stories and columns appeared regularly in *The Los Angeles Times*, *Chicago Tribune*, *Miami Herald*, *Newsday*, and other major US dailies. He has also written extensively for O'Reilly Media.

A graduate of Hamilton College, he is a licensed private pilot, avid reader, and enthusiastic ice hockey fan.

Gregory Fell is a general partner in The Investors Collaborative, a Boston-based venture capital group. He is the former chief strategy officer at Crisply, an enterprise SaaS company that pioneered the algorithmic quantification of work. Previously, he served as vice president and chief information officer of Terex Corp., a global manufacturer of industrial equipment.

Before joining Terex, Fell spent nearly 20 years with Ford Motor Company. He started as a developer and worked his way through a variety of management roles supporting the global Engineering and Manufacturing functions of the company. He has domain expertise on CAD/CAM/CAE systems, lean manufacturing, and control systems.

Fell is a graduate of Michigan State University. He spent several years on staff in the College of Engineering as a senior research programmer and instructor.

He is active in the CIO community: the former chairman of the Fairfield Westchester Society of Information Managers, a former board member with Junior Achievement, and he has mentored high school students through the First Tee Program.

His book, *Decoding the IT Value Problem* (Wiley, 2013), is used widely by CIOs to calculate the economic value of IT projects.