

TACTICS AND PREPAREDNESS



SKILLS AND SURVIVAL FOR ALL SITUATIONS

the dark web

BY: CHRIS MARK



Over the past several years, the presence of the Deep Web and Dark Web have been increasingly highlighted in books, movies and articles.

It was Edward Snowden's use of the "deep web" that captured many people's attention (including mine.) It should be noted that all users must understand the risk of using such technologies. When people learn about the deep web and associated technologies it is not uncommon to hear questions like: "how is this legal!?" It is important to

remember that technology is benign. It is the application of the technology that can be problematic. A firearm in a responsible citizen's hands is a valuable tool to prevent crime and provide protection. The same firearm in the hands of a criminal can be a very bad combination. The same concept exists with networking technology.

THE DEEP WEB

An easy way to think of the Deep Web is to compare it to what we all know: the *Clear Web*. The Clear Web employs TCP/IP Routing and consists of everything that can be indexed on the Internet. Consider your favorite search engines. They are indexing websites and files and those *continued on next page*

CONTENTS

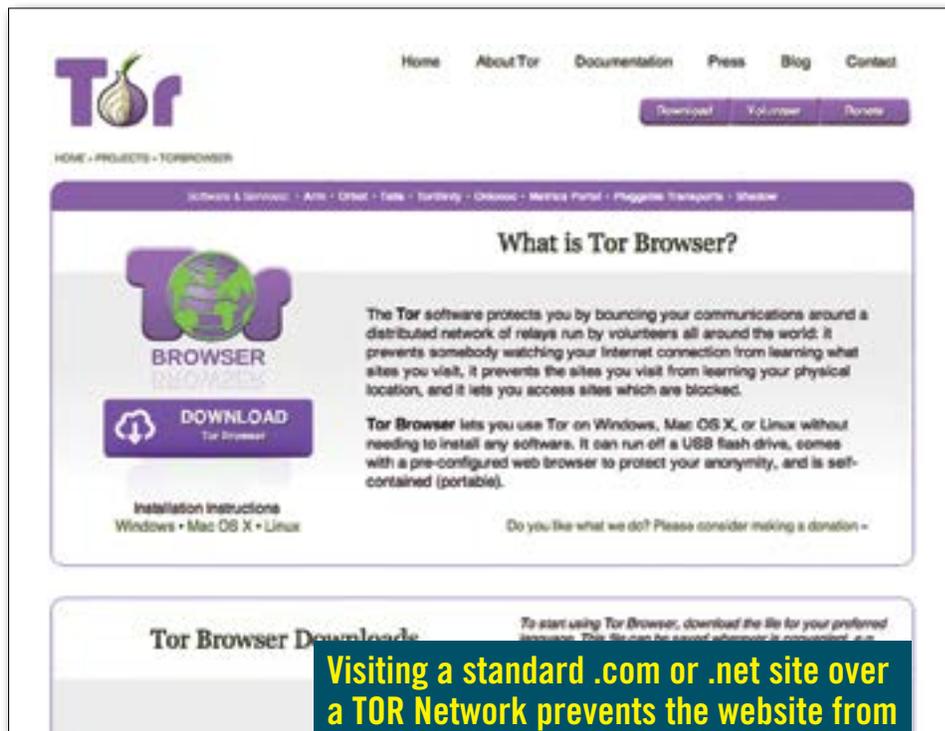
- 01** THE DEEP WEB AND THE DARK WEB
BY CHRIS MARK
- 04** TRUE NINJA TRADITIONS
*WRITTEN BY ANTONY CUMMINS
AND YOSHIE MINAMI
SUMMARY BY CHRIS GRAHAM*
- 05** GEAR REVIEW:
LAMZAC
- 06** ONE HANDED PISTOL:
HOW AND WHY
BY JAMES WASHINGTON
- 09** ANTIFRAGILE KIDS:
TRAINING AWARENESS
AND SELF DEFENSE
BY DAVE CADY
- 12** BUGOUT BAGS:
SUPPLEMENTS, BACKUPS
AND ALTERNATES
BY JIM LeBLANC
- 16** IMPROVISED WEAPONS:
CANE COMBAT
BY ANDREW CURTISS
- 20** PROFILES OF COURAGE:
MONSIEUR X

STAFF

- DAVID MORRIS** and **"OX"** Publishers
- CHRIS GRAHAM** Editor
www.chrisgrahamauthor.com
- JOHN HIGGS** Copy Editor
www.junkyard-dog.net
- BETTY SHONTS** Graphic Designer

OUR LAWYERS INSIST WE MAKE THE FOLLOWING DISCLAIMER: You may die in an emergency, even if you follow this training to the letter. You might get hurt doing some of the exercises suggested, hurt someone else, or be subject to civil or criminal liability if you do anything mentioned in this newsletter. Verify that the actions mentioned are legal where you are before even considering them. This is presented as a tool to help increase your chance of surviving natural and manmade disasters. While we guarantee your satisfaction with the information, we can not guarantee your survival or well-being. The author provides information about his experiences and preparations and gives general information. He is not an accountant, doctor, investment advisor or attorney and is not in the business of advising individuals on their specific situation. If you need specific professional assistance, please contact a local professional.

©COPYRIGHT 2017 TACTICS AND PREPAREDNESS. ALL RIGHTS RESERVED. THIS PUBLICATION CONTAINS MATERIAL PROTECTED UNDER INTERNATIONAL AND FEDERAL COPYRIGHT LAWS AND TREATIES. ANY UNAUTHORIZED REPRINT OR USE OF THIS MATERIAL IS PROHIBITED. NO PART OF THIS PUBLICATION MAY BE REPRODUCED OR TRANSMITTED IN ANY FORM OR BY ANY MEANS, ELECTRONIC OR MECHANICAL, INCLUDING PHOTOCOPYING, RECORDING, OR BY ANY INFORMATION STORAGE AND RETRIEVAL SYSTEM WITHOUT EXPRESS WRITTEN PERMISSION FROM THE AUTHOR / PUBLISHER.



websites and files are associated with domain names and IP addresses. Every single user and system on the internet has a unique IP address associated with them. This article serves as a brief introduction, so subnets and obfuscation, etc. are not discussed. With an IP address you can theoretically access every single other IP address in the world. You can also search by IP and/or domain name. To quickly find your own IP address, a useful tool is the website: <http://whatismyipaddress.com/ip-lookup>. It is important to remember that in the Clear Web your usage is not protected and you have no true anonymity. In addition, your geolocation can typically be found with little effort.

By contrast, the Deep Web consists of non-indexed sites. A very loose description of the Deep Web would be a database that was not indexed. More specifically, when the term Deep Web is used it is referring to those hidden services and communications that use the TOR protocol and TOR Network. When you hear someone refer to the Dark Web this is focused on those very deep (and dark) recesses of the TOR Network (and a few others) where content can become very dark. To understand the Deep/Dark web it is important to know the history and a bit about TOR.

It is estimated that the Deep Web accounts for 95 percent of the data available and the Clear Web only accounts for 5 percent! There

is much, much more data and information on the Deep Web than on the Clear Web.

TOR

In 1994 the Naval Research Laboratory developed a routing protocol called "The Onion Router" (or TOR) with the objective of allowing intelligence agents to have a more secure means of communication than the traditional Clear Web and IP Routing protocols. In 1997 the project was adopted by the Defense Advanced Research Projects Agency (DARPA) and it was officially released as an alpha version in 2002. By 2006 the TOR Project was released as a 501(c)(3)¹. TOR works by leveraging a customized browser that encrypts traffic and sends to a random relay somewhere around the world. This relay sends the encrypted traffics to another relay and finally a third. The third relay decrypts the request and only the last link is unencrypted. There is no originating source IP address and the user is anonymous (generally, but read the disclaimers.) The TOR network does not use standard Top Level Domains (TLD) suffixes such as .com, .net and .edu and instead uses a proprietary domain name of .onion. The system does not use domain names and instead uses a component of an asymmetric cryptographic key for the name. As an example, if a person wants to search Google on the Clear Web they would simply type www.Google.



com and enter the search. To use a Deep Web search engine like TORCH one would need to have the TOR Browser installed and type: <https://xmh57jrznw6insl.onion>. Notice the HTTPS showing the link is encrypted and that it is a .onion address.

A benefit of using the TOR Network is that a person can access a Clear Web site from the TOR Network but a TOR site cannot be accessed from the Clear Web. Visiting a standard .com or .net site over a TOR Network prevents the website from tracking your IP and geolocation.

ACCESSING TOR AND THE DEEP WEB

To access the TOR Network it is necessary to have very specific technology. Luckily this technology is available online and is free of charge. Generally, from a PC or MAC there are two ways to access the TOR Network. The first is easier but, arguably, much less secure. The second is more difficult and less convenient, but offers a much higher degree of anonymity and security. Be warned though, neither method will offset bad browsing habits. If you have your standard email open when browsing TOR your IP can be leaked. Read the disclaimers on the limitations of the technology.

1. Download the TOR Browser Bundle at <http://TORProject.org> The TBB is a bundle that includes a customized Firefox browser that connects to the TORNetwork. It is a very

quick and easy way to gain improved anonymity and security. Read the disclaimers.

2. Download The Amnesiac Incognito Live System (TAILS) from <https://tails.boum.org/> This is the very same system Edward Snowden used to bypass the NSA. It requires that the user have a passable degree of familiarity with how to boot to a live operating system and Linux, but the directions are solid. TAILS is the preferred method to access the Deep Web.

3. Find an entry point. A common entry point into the Deep Web is the Hidden Wiki. From the Clear Web one can simply type: <http://hiddenwikitor.com> which will provide various links that can only be accessed from the Tor Network or you can use the Hidden Wiki link on the TOR Network <https://xmh57jrznw6insl.onion>

THE DARK WEB

The Dark Web refers to the darker reaches of the Deep Web. As stated, the Deep Web simply refers to anonymous hosting and communication using particular security technologies. The same technologies that enable dissidents, spies and journalists to protect their identities can also be leveraged by those with illicit motivations. Unfortunately, child pornographers, drug dealers, hit men, hackers, jihadis and other criminals use the Deep Web for their purposes too. I often tell people "The deeper you go the darker it gets."

LEGITIMATE USES

Remember, technology is benign. In this case it is the illicit use of the technology that is illegal. The Deep Web provides a much higher (although not perfect) degree of anonymity and security when combined with good surfing habits. In 2014, even Facebook created their own TOR address for people who wanted to access from the TOR Network <https://facebookcorewwi.onion/> The right to privacy and anonymity only exists if you assert it. Being low profile is the first, arguably most valuable aspect of security. Using TOR to surf the web provides a much higher degree of protection.

Consider this real example: You are looking for a new job at a competitor and you visit their website from your home computer to do some research. Observers can, and often will, track your IP and location, which can tell them who you are. Is this a problem? Probably not, but do you want to show your hand? Again, probably not. Privacy and anonymity are simply tools to put in a toolbox to maximize your security.

CAUTION

The TOR Network and other technologies provide a much higher degree of anonymity that enables people with pure intentions and those with less pure intentions to conceal their activities. I always caution parents not to allow their teenagers to see how to access the TOR Network. While they may not be trying to find illegal and harmful material, it is simply too easy to encounter. ✓

BIO

Chris Mark (www.markconsultinggroup.com) worked with Visa on the development of the initial CISP standards. He was the industry's first PCI assessor. After selling his QSA firm, Chris joined MasterCard Worldwide working on their Site Data Protection team and later founded another company which focused on PCI DSS training and consulting. Chris was the worldwide QSA trainer and PCI trainer for Visa Inc. Prior to joining the private sector, Mr. Mark served as a Scout/Sniper and Force Recon Marine and later as a US Navy officer.

NOTES

1. [https://en.wikipedia.org/wiki/Tor_\(anonymity_network\)](https://en.wikipedia.org/wiki/Tor_(anonymity_network))