The Dangers Of Using Tor On The Darknet And How To Fix It.

Contents

The Dangers of Using Tor on the Darknet

Intro to Tor and the Darknet

The darknet is a notion most internet users have heard about at least once in their lifetime. Its emergence imbued with illegal activities can be roughly dated back to the millennial year of 2000. Since then, an insurmountable number of internet users have explored these “deep waters”, which enable illegal activities of all kinds. Some of the highest ranking ones include weapon and drug dealing, pornography, abuse etc.

Simply described, the dark net is a computer network, which uses another network as its base—it is built on top of it. It is also referred to as an overlay network. What makes this phenomenon exclusive is that it is exceptionally accessed via specific software, configurations, and/or authorization. In addition, non-standard communication protocols and ports are also frequently implemented.

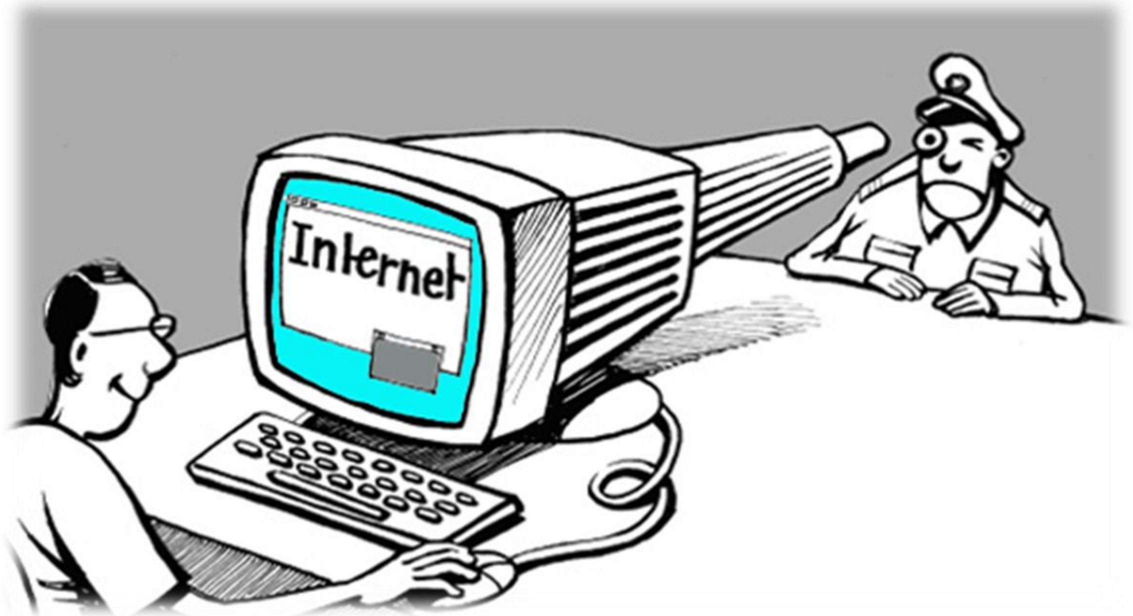
How Tor Works

Tor, or The Onion Router is a software which enables a certain level anonymity while surfing the darknet.

It serves to conceal the users' location and activities by directing internet traffic through a volunteer network, which is pro bono and global, and comprises of thousands of relays. Using Tor can help prevent the surveillance and traffic analysts from tracking illegal activities performed on the darknet.

Its secret lies in its design, which allows information to go through a few nodes, making it almost impossible to trace all the different IP addresses. Thus, because of this diversion, the starting and the end point of the transaction cannot be traced.

How ISP and Governments Can See You Using Tor Even When It Works

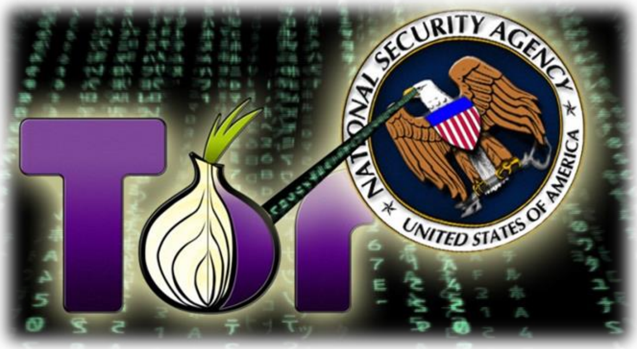


However, it has been purported that Tor is no longer the safe haven it once used to be. Turns out, ISP's (Internet Service Provider) and the Government are now able to track illegal activities on the darknet, regardless of Tor usage. Initially, Tor started out as Naval project, which included military purposes. The plan was to gain the ability to trace communications and disrupt the operation by destroying the target.

Every move on the internet leaves a trace. Whether one uses Tor or does not, he or she leaves a trail. With adequate prudent work, the Government as well as ISP can in fact make the connection to the origin and ultimately to the destination of a given transaction or communication. Imagine crumbs that Internet users leave behind them, often times unaware that they are in reality leaving traces. Consequently, it may take months of hard and meticulous work for the Government to put these pieces together, but nonetheless, once the puzzle is complete, the investigators gain clearance to possibly make an arrest.

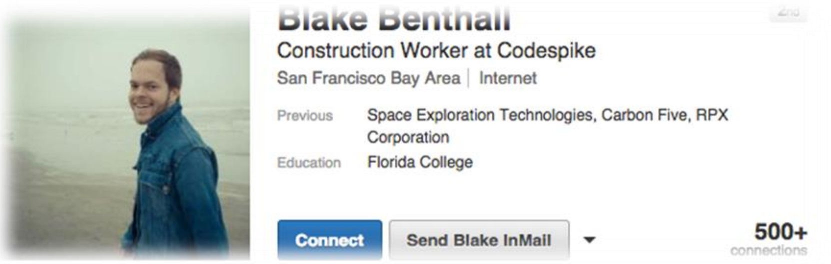
Another reason why Tor users' anonymity is no longer guaranteed is malware, which can be easily injected into the browser. The FBI has implemented this method in the past, which led to the revelation of hundreds of different IP addresses, all identified as child pornography users. As a result, they were able to make numerous significant arrests. Although I am personally glad that these scum bags were caught it still points out that Tor is not as private as you think. Additionally, they can also set up traps in the form of Government-controlled networks, which the users can easily fall into without any warning. Basically, the FBI computer serves as the entry node or the exit node, trough which a plethora of incriminating information can be revealed.

How ISP's and LE (Law Enforcement) Can Log Your Tor Usage to Later Decrypt



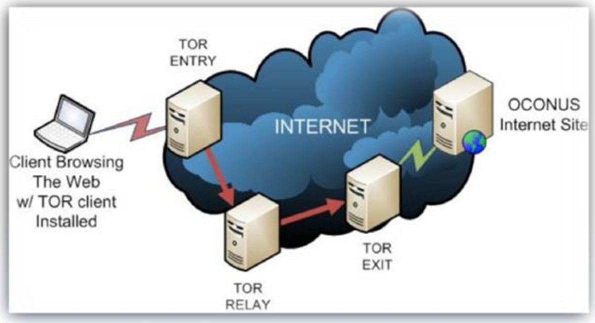
On the other hand, logging Tor usage requires a lot work but ISP are already logging everything for new data retention laws. The Law Enforcement and ISP would have to be able to have a physical back-trace of all the points a.k.a. nodes that the IP address has bounced to and fro. Continually, even though they might gain access to all those different nodes, which are often found on different continents, they would have to have a decryption key in order to start decrypting.

How Tor Sessions Can Be Logged and Cross Referenced And Linked With Darkweb Activity


Blake Benthall
2nd
Construction Worker at Codespike
San Francisco Bay Area | Internet
Previous Space Exploration Technologies, Carbon Five, RPX Corporation
Education Florida College

Edward Snowden, a former Central Intelligence Agency employee leaked documents that inform the public of the NSA surveillance program labeled X-Keyscore, which enables NSA personnel to acquire personal information such as, phone numbers and email address. They are also allowed to view the content of emails, and follow Internet activity, which includes browsing internet history without a warrant. Consequently, this way Tor sessions can also be easily logged and used as evidence to back up illegal activities being carried out on the darknet. An example of such a crossreference with the Darkweb was made in the Silk Road 2 admin's case, which led to its downfall.

How Tor Is Not 100% Private



One of the greatest drawbacks of Tor is that it gives a false sense of security; meaning that no matter how you twist or turn this software, there are loopholes that can reveal your anonymity. In other words, even though the software has been designed to create diversion by having the information pass through several relays, the nodes can be eventually identified, which ultimately leads to finding the user. The only way to avoid this is to use Tor within a VPN service, which enables P2P (peer to peer) networking, and also prevents you from being directly connected to the webpage you wish to visit.

How Tor Has Been Cracked By Universities

One of the most well known universities on the planet succeeded in cracking Tor. MIT used a method where they set up a computer and established connection via Tor. Afterwards, they simply waited for requests to pour in. The researchers used the computer as the entry node and implemented machine learning algorithms in order to observe data and keep account of the packets. With the application of this type of metric system they were able to gauge the different resources that the users were trying to access.

Furthermore, by the simple implementation of traffic fingerprinting, it was possible to conclude, which underground services the user was accessing merely based on the pattern of sent packets. However, one would still need an encryption key to fully identify the user.

How Governments Have Hijacked Some Nodes to Find You

The government has the ability to hijack nodes by setting up and operating a big number of them. In essence, they set up traps for the users to fall into. If the user stumbles upon a government-controlled network, and falls into their snare, the user's identity is certainly revealed to the authorities and gives the FBI or other Law Enforcement agencies to do away with the culprit. There are no visual signs of government-controlled networks, so the user cannot be warned or determine whether he or she is being watched. The Government is highly equipped with skilled hackers; the FBI has an entire division dedicated to cyber crime and can easily infiltrate and hijack nodes to find the information they need. Continually, Tor users are highly advised to keep this in mind the next time they use Tor.

How Governments Are Tracking Who Downloads Tor and Getting Digital Fingerprint

With their highly equipped team of experts the Government has the ability to observe and list anyone who not only downloads but simply does some harmless research on privacy-protection tools. Tor usage is not illegal. However, the activities performed using this software *can* entail a variety of illegal activities. The authorities therefore, can use this list as a starting point when doing an investigation. Digital fingerprints are also of great value to the Government. Just like we leave fingerprints on everything we touch, so does the data our computer processes. In essence, the digital fingerprint is a shorter bit string of the large data we access or file. Thus, leaving digital fingerprints is akin to leaving suspicious trails at the crime scene, which the authorities can use to identify the user. It is a very good idea to get a VPN and turn it on BEFORE downloading the Tor browser otherwise you WILL be on a database of the feds as a Tor user and have possible further increased monitoring of your online and offline actiities.

How Certain Settings On Tor Will Make You Visible (JS)

Java, JavaScript, Adobe Flash, QuickTime, Adobe Shockwave, RealAudio, ActiveX controls, and VBScript are all active content and binary applications, which can be run through a personal user account. With the user’s permission they are used to access different web sites. Tor is naturally one of them, and JavaScript will definitely reveal personal account information. Tor usually has this setting off, however the user can turn it back on, or leave it on by accident after browsing different websites like YouTube.

How Some OS (Windows 10) Can Leak Your Info

Windows 10 has finally arrived. However, its privacy settings caused some concern among users. Apparently, it, the system is built to know *everything.* Kevin Lee in his article titled ***Stop Cortana from spying on you*** had the following to say, *"*By default, the OS is programmed to watch the words you type and listen to your speech so it can personalize the experience for you. These features can be convenient, but also raise privacy concerns." Users are highly advised to choose the Custom Settings where they can prevent any unwanted information from leaking out. Choosing the easy shortcut, however and opting for Express Settings can lead to Windows 10 sharing a plethora of info that perhaps you do not wish to share online. Creating a local account can also keep certain valuable data offline.

How DNS Leaks Can Leak Your Info

The domain name system serves to translate domain names, i.e. links to websites into IP addresses. When we browse the net and contact a URL server, the computer also comes in contact with a DNS server, which requires the computer's IP address. Given that using an anonymity service will keep confidential information unrevealed, DNS leaks are seen as a huge privacy concern, since in case the leak does occur, the IP address will be automatically revealed.

Tor Is Not As Private and Anonymous As You Think

At first glance Tor may appear to be a safe tool to preserve anonymity; however that is not entirely the case. There are definitely some perks to using the software, but 100% anonymity is far from guaranteed. There are way too many loopholes in its design, which can be used to infiltrate the users' system, and have more than a sneak peak into all the different activities that take place on the darknet.

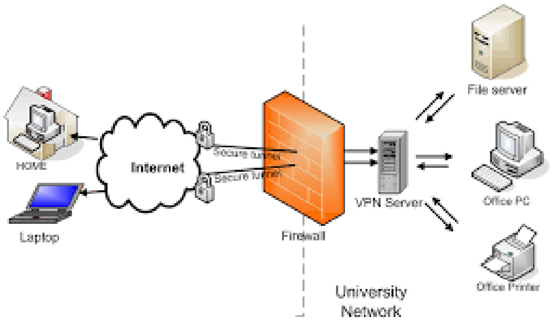
KEEP READING BOLOW FOR THE SPECIAL BONUS SECTION

SPECIAL BONUS SECTION

Use a VPN to Minimize your Exposure

As showed above, Tor has its flaws and many users are concerned about the DNS leaking. This leakage happens when certain applications, such as flash or javascript are active. They use DNS connections directly via your computer and they are not routed via Tor Network; meaning that your IP address can be compromised and visible to anyone observing the connection. Therefore, the safest way to stay anonymous online, for now at least, is by using VPN in combination with Tor.

VPN companies are usually exempt from data retention laws



VPN stands for Virtual Private Network, and what it does is hide your IP address. However, it can sometimes be traced. Many VPN providers offer a special feature – they do not keep logs of users' activities. Still, a few times in modern history it happened that they were forced to disclose data to LE who managed to track down certain suspicious activities back to the VPN. However, most decent VPN work great in combination with Tor and here is the basic principle.

VPN stop Tor leakages

If you are using VPN in combination with Tor, your connection looks like this:

Your computer → VPN Server → Tor → The Internet.

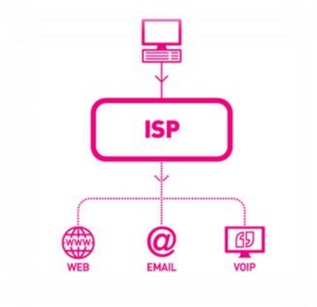
So if DNS leakage happens, your IP address still won’t be revealed since the application which is leaking is not connected directly to the internet but through the VPN, and the only visible address to anyone monitoring is the IP address of the VPN server.

Some VPN providers, very few though, enable you to connect to VPN via Tor. In this case, your connection looks like this:

Your computer → Tor → VPN → Tor → The Internet.

This is probably the safest way to browse possible; it is also the slowest. So, it’s safety over speed. This way, your VPN provider won’t see your actual IP address, but Tor’s exit node wont either.

ISPs won’t even know you are using Tor



ISP’s are capable of monitoring and recording all your connections. But all that a VPN is, is an encrypting tool and everything your ISP will be able to see is your connection to the VPN server. This in itself is pretty handy, since the Government doesn't like people using Tor or more precisely it's not so much that they have anything against people using Tor; it's just that they would like to have a list of people who do. So, the only way to hide your Tor usage from the government is if you use it in collaboration with a VPN.

Even if VPN and LE and ISP record your VPN usage, they won't be able to crack it down

Imagine VPN as just another way of encryption. So, if we know that Tor uses 3 layers of encryption and VPN uses one, it is almost impossible to decrypt it or crack it down. No matter to what point of your connection the LE or ISP has access to, whether it is VPN or some of the Tor's nodes - it would be practically impossible or at least very hard for them to decrypt the data and the info you send. This way, you are invisible, unless, of course, they have access to all decryption keys.

What to have in mind when picking the right VPN

Obviously, the LE or the FBI have become at least as much creative and efficient as criminals themselves when it comes to intercepting Tor connections; so when choosing a decent and reliable VPN, you should pay attention to certain important details.

1. **Logs:** The most important thing you want to make sure when picking the VPN provider is whether it logs data or not. Many of them claim they don't but they actually do. So pick your provider wisely. Check their TOS and Privacy Policy for this information.

2. **Tier:** Make sure that your VPN is Tier 1 provider, meaning that is owns all of its network and doesn't rent it servers from 3rd party companies. When they say they don't log then thety can be 100% certain of that fact. There are not many Tier 1 providers buy IPVanish VPN is one of them.
3. **Compatibility:** Not all VPN providers allow connections to Tor network, so make sure that your VPN provider is Tor compatible.
4. **Protocol:** You definitely want to use an Open VPN protocol mainly because they use OpenSSL encryption library and SSL v3/TLS v1 protocols. In short - you are much safer and the data is more efficiently encrypted; whereas, in the old protocol, PPTP, data is more easily cracked and decrypted.
5. **Kill Switch:** Only the top VPN providers offer this feature. It is a kill switch to prevent DNS leaks. Basically, it means that it will end your internet connection immediately at the slightest chance of your IP address being exposed. For example, if one of your apps is about to leak your IP through DNS or if VPN connection suddenly stops.
6. **Devices:** Also, make sure you can use the VPN on all of your devices like your iPhone or android and tablet so you can use the VPN all of the time and access services like Netflix on them.
7. **Price:** Some VPNs are free, some are cheap and some are neither; and, there's really not much room for being stingy when it comes to safety and anonymity. So, if you want a fast and private VPN software, (and - you do) it will probably cost a little but still usually cheaper than a Big Mac.

If you truly want to have your privacy while browsing sites on the Tor network then you really need to get a VPN. There are tons of other uses for them as well like unlocking Netflix for every country and accessing blocked sites on the clear web.

Now not all VPN's are created equal. A good resource I use when researching the latest VPN's is https://topvpnsoftware.com

I have done some background checking on the site and it is actually a computer programmer that has gone and downloaded and tested all of the VPN's listed. I have also found TONS of other review sites that you can tell have not even used the VPN's so it was nice to find a good one for once.

Another few good resources that you can use:

Internet Anonymity: http://internet-anonymity.com
My news site about the latest internet anonymity tactics.

Darkweb News: http://darkwebnews.com
Is a news site about the Darkweb and all of the Darknet marketplaces.

Total Bitcoin: http://totalbitcoin.org
A News site about Bitcoin with guides on how to buy and sell bitcoins. The best VPN's accept Bitcoin as payment which makes you even more anonymous.