

## Forum:[Hack Forums](#)

Thread: [Tor and reveal real IP.](#)

**hack3rcon** - January 15, 2019, 12:13 am

Hello.

In some websites you can chat with support. In the chat window, they show your IP address, if use Tor to chat with them then can they find my real IP address? If I use VPN then launch Tor?

Thank you.

**Asdethprime** - January 15, 2019, 12:22 am

Rather than asking why not try. It won't be able to tell your real IP address when u use tor.

For an easy test try it out. Open a normal web browser. Go to google and search what is my IP address. Save that. Then open a tor browser ; do exactly that and see how different your IP looks.

**hack3rcon** - January 17, 2019, 10:38 pm

(Jan 15, 2019 01:22 AM)Asdethprime Wrote: [\[CITE\]](#) Rather than asking why not try. It won't be able to tell your real IP address when u use tor.

For an easy test try it out. Open a normal web browser. Go to google and search what is my IP address. Save that. Then open a tor browser ; do exactly that and see how different your IP looks. But I guess governments can bypass Tor!!!

**Asdethprime** - January 17, 2019, 10:42 pm

(Jan 17, 2019 11:38 PM)hack3rcon Wrote: [\[CITE\]](#) But I guess governments can bypass Tor!!! Sorry, what do you mean by "bypass" ?? Unsure what you are trying to say, would you mind elaborating?

**Mikutype** - January 17, 2019, 10:48 pm

Get into tor browser and done. This is a basic question.

Download Tor Browser. Go to website. Done. They won't find your ip.

First vpn then tor it is a better formula though, but you do not need to be that paranoid.

Gov could potentially use deep packet inspection to find your browsing habits even behing vpn + tor or tor alone, yes.

**hack3rcon** - January 21, 2019, 1:12 am

(Jan 17, 2019 11:42 PM)Asdethprime Wrote: [\[CITE\]](#) Sorry, what do you mean by "bypass" ?? Unsure what you are trying to say, would you mind elaborating?

I mean is "broke" Tor.

(Jan 17, 2019 11:48 PM)Mikutype Wrote: [\[CITE\]](#) Get into tor browser and done. This is a basic question.

Download Tor Browser. Go to website. Done. They won't find your ip.

First vpn then tor it is a better formula though, but you do not need to be that paranoid.

Gov could potentially use deep packet inspection to find your browsing habits even behind vpn + tor or tor alone, yes.

No way to protect?

**Asdethprime** - January 21, 2019, 1:49 am

(Jan 21, 2019 02:12 AM)hack3rcon Wrote: [\[CITE\]](#) I mean is "broke" Tor.

No way to protect?

There is no way to get your real IP when u are using Tor.

But what they can do though is block all connection from Tor.

And unless u give out your own details even government can't track it. Even NSA ( USA ) and GCHQ ( UK government ) have been having trouble with Tor.

If used properly that is :)

**GutsBS** - January 21, 2019, 8:56 pm

(Jan 15, 2019 01:13 AM)hack3rcon Wrote: [\[CITE\]](#) Hello.

In some websites you can chat with support. In the chat window, they show your IP address, if use Tor to chat with them then can they find my real IP address? If I use VPN then launch Tor?

Thank you.

The fact you are using Tor is the only thing visible which you can hide with a bridge or VPN. If everything is configured correctly and you don't land on a malicious exit node, no one can see what you're doing. Including governments.

**hack3rcon** - January 22, 2019, 1:19 am

(Jan 21, 2019 09:56 PM)GutsBS Wrote: [\[CITE\]](#) The fact you are using Tor is the only thing visible which you can hide with a bridge or VPN. If everything is configured correctly and you don't land on a malicious exit node, no one can see what you're doing. Including governments.

How can I sure my exit node is not malicious?

**SIM-4065785** - January 22, 2019, 1:49 am

Tor is used a lot by hackers. The only thing to care is flash objects, your browsers special footprints

**Asdethprime** - January 23, 2019, 4:20 am

Contrary to what people repeat here over and over again, VPN is NOT RECOMMENDED with TOR. Just don't you are not getting extra security you are risking your privacy because now there are 2 ways to track who you are from 1) break Tor or 2) break into VPN's log.

I know this sounds counterproductive, you have seen so many website, so many articles ; but the truth remains. The only viable way to knowing who you are behind tor ( provided you are using it properly) is a correlation attack; and that's checked based on VPN.

Also a malicious exit node CAN ONLY SEE what website you are visiting. In this case, a malicious exit node will be able to see someone, using Tor is visiting the government website. It won't be able to trace it back to you.

A malicious entry node would have the opposite effect, if will be able to find who you are but not find out what you are seeing.

**Scaletta** - January 23, 2019, 5:27 am

(Jan 23, 2019 05:20 AM)Asdethprime Wrote: [\[CITE\]](#) Contrary to what people repeat here over and over again, VPN is NOT RECOMMENDED with TOR. Just don't you are not getting extra security you are risking your privacy because now there are 2 ways to track who you are from 1) break Tor or 2) break into VPN's log.

I know this sounds counterproductive, you have seen so many website, so many articles ; but the truth remains. The only viable way to knowing who you are behind tor ( provided you are using it properly) is a correlation attack; and that's checked based on VPN.

Also a malicious exit node CAN ONLY SEE what website you are visiting. In this case, a malicious exit node will be able to see someone, using Tor is visiting the government website. It won't be able to trace it back to you.

A malicious entry node would have the opposite effect, if will be able to find who you are but not find out what you are seeing.

I vouch for what he just said. Its better to trust tor alone than a vpn over tor. Chances are higher in theory that a vpn keeps logs and co-operates with cops than a tor node.

Though i will addon 1 way to find out real ip would be through javascript or downloading files to computer if the computer is using simply tor browser and not tails. Tor browser would only protect the browsing on tor not anything else on the computer

**Asdethprime** - January 23, 2019, 5:51 am

(Jan 23, 2019 06:27 AM)Scaletta Wrote: [\[CITE\]](#) I vouch for what he just said. Its better to trust tor alone than a vpn over tor. Chances are higher in theory that a vpn keeps logs and co-operates with cops than a tor node.

Though i will addon 1 way to find out real ip would be through javascript or downloading files to computer if the computer is using simply tor browser and not tails. Tor browser would only protect the browsing on tor not anything else on the computer

Glad there are people who are happy to actually analyze this. Cheers man!

Though unlike normal browsers Tor does not have WebRTC so you can't normally pull the real IP behind TOR through JavaScript unlike most browser. But, yeah if someone is dumb enough to actually download javascript code and execute it than you are a sitting duck.

That being said, that's just not using Tor properly. Same with say DNS leaks, or people trying to log into website with Tor. That just gives out the address.

Tails though would be awesome, but frankly, given people I normally meet her I highly doubt if any more than 1% of people use Tails here; but they seem happy to pay VPN providers money; despite you know Tails is free and so much better than any VPN out there ( and if anyone is even questioning this, you really don't understand Tails).

**Cytax** - January 23, 2019, 2:21 pm

(Jan 23, 2019 06:27 AM)Scaletta Wrote: [\[CITE\]](#) I vouch for what he just said. Its better to trust tor alone than a vpn over tor. Chances are higher in theory that a vpn keeps logs and co-operates with cops than a tor node.

Though i will addon 1 way to find out real ip would be through javascript or downloading files to computer if the computer is using simply tor browser and not tails. Tor browser would only protect the browsing on tor not anything else on the computer

I would like to add that you can and should disable JS from the Tor browser. Just a heads up for OP and anyone else who didn't know you could do that.

**Scaletta** - January 23, 2019, 7:26 pm

(Jan 23, 2019 06:51 AM)Asdethprime Wrote: [\[CITE\]](#) Glad there are people who are happy to actually analyze this. Cheers man!

Though unlike normal browsers Tor does not have WebRTC so you can't normally pull the real IP behind TOR through JavaScript unlike most browser. But, yeah if someone is dumb enough to actually download javascript code and execute it than you are a sitting duck.

That being said, that's just not using Tor properly. Same with say DNS leaks, or people trying to log into website with Tor. That just gives out the address.

Tails though would be awesome, but frankly, given people I normally meet her I highly doubt if any more than 1% of people use Tails here; but they seem happy to pay VPN providers money; despite you know Tails is free and so much better than any VPN out there ( and if anyone is even questioning this, you really don't understand Tails).

Tails is good but not practical for day to day stuff. If you want to search for a restaurant in your area, your exit note would pretty much be a country 10,000 miles away which means refining your search even more or dealing with exit node bans.

**Zens** - January 23, 2019, 9:28 pm

(Jan 17, 2019 11:38 PM)hack3rcon Wrote: [\[CITE\]](#) But I guess governments can bypass Tor!!! they won't be able to but disable your js and don't be an idiot like clicking links randomly read this

<https://money.cnn.com/2016/01/25/technology/fbi-child-porn/>

"The exact method used by the FBI is detailed in other court records. Agents added Flash software to the hijacked porn site, exploiting the fact that Flash is notoriously vulnerable to hacking. If visitors used an outdated version of Tor -- and didn't set their computers to block Flash -- that Flash app was able to establish a direct connection and reveal their IP address. "

**Asdethprime** - January 24, 2019, 12:08 am

(Jan 23, 2019 08:26 PM)Scaletta Wrote: [\[CITE\]](#) Tails is good but not practical for day to day stuff. If you want to search for a restaurant in your area, your exit note would pretty much be a country 10,000 miles away which means refining your search even more or dealing with exit node bans.

Tails is NOT meant to be used for a day to day operation. It's meant to be on a boot drive (USB) and you are supposed to use that operating ONLY WHEN YOU ARE DOING PRIVACY SENSITIVE STUFF (I.e hacking ).

It was technically created so journalist / whistleblowers can disclose information safely without having to worry about reprecussions from their government / power that be.

If u are using Tails for day to day operation u have messed up.

**WiteWidow** - January 24, 2019, 4:43 am

(Jan 23, 2019 05:20 AM)Asdethprime Wrote: [\[CITE\]](#) Contrary to what people repeat here over and over again, VPN is NOT RECOMMENDED with TOR. Just don't you are not getting extra security you are risking your privacy because now there are 2 ways to track who you are from 1) break Tor or 2) break into VPN's log.

I know this sounds counterproductive, you have seen so many website, so many articles ; but the truth remains. The only viable way to knowing who you are behind tor ( provided you are using it properly) is a correlation attack; and that's checked based on VPN.

Also a malicious exit node CAN ONLY SEE what website you are visiting. In this case, a malicious exit node will be able to see someone, using Tor is visiting the government website. It won't be able to trace it back to you.

A malicious entry node would have the opposite effect, if will be able to find who you are but not find out what you are seeing.

Thx for this post. I`ve been looking for a while which is the most "safest" way to stay anonymous. And now i have to cancel my vpn while using tor ?

- Important Information in this thread!

**Scaletta** - January 24, 2019, 8:45 am

(Jan 24, 2019 01:08 AM)Asdethprime Wrote: [\[CITE\]](#) Tails is NOT meant to be used for a day to day operation. It's meant to be on a boot drive (USB) and you are supposed to use that operating ONLY WHEN YOU ARE DOING PRIVACY SENSITIVE STUFF (I.e hacking ).

It was technically created so journalist / whistleblowers can disclose information safely without having to worry about reprecussions from their government / power that be.

If u are using Tails for day to day operation u have messed up.

I know and agree. I was implying that most people here on HF don't use tails because they spend their spare time here while doing other stuff so its not practical or even expected to be a common tool among most members here.

**Riggs** - January 24, 2019, 8:54 am

(Jan 23, 2019 05:20 AM)Asdethprime Wrote: [\[CITE\]](#) Contrary to what people repeat here over and over again, VPN is NOT RECOMMENDED with TOR. Just don't you are not getting extra security you are risking your privacy because now there are 2 ways to track who you are from 1) break Tor or 2) break into VPN's log.

I know this sounds counterproductive, you have seen so many website, so many articles ; but the truth remains. The only viable way to knowing who you are behind tor ( provided you are using it properly) is a correlation attack; and that's checked based on VPN.

Also a malicious exit node CAN ONLY SEE what website you are visiting. In this case, a malicious exit node will be able to see someone, using Tor is visiting the government website. It won't be able to trace it back to you.

A malicious entry node would have the opposite effect, if will be able to find who you are but not find out what you are seeing.

Your point you've made about risking your privacy via Tor over VPN makes absolutely no sense at all. A correlation attack can be performed against your domestic ISP far easier than it can a remote-access VPN.

**Scaletta** - January 24, 2019, 9:12 am

(Jan 24, 2019 09:54 AM)Riggs Wrote: [\[CITE\]](#) Your point you've made about risking your privacy via Tor over VPN makes absolutely no sense at all. A correlation attack can be performed against your domestic ISP far easier than it can a remote-access VPN.

You make a valid point but that can be easily mitigated if the Tor without vpn is being run on a RDP.

Your own personal isp won't be exposed if there is a vpn connection to the rdp but that's a whole another level of game.

A more common risk is that the VPN ip address being exposed. Any website visited exposes the VPN ip address where with tor you can have hops that can protect your true identity. If you are doing something not approved by the government and the VPN keeps logs + shares with LE then you are very easily fucked. If the vpn provider does not keep logs then use tor with vpn by all means but question is how much are you willing to trust a vpn seller when they say they do not actually keep any logs.

Edited

With correlation attack, two servers (nodes) need to be targeted. With vpn just the server (1) user is connected to thus making the correlation attack a more complicated attack than vpn. Common attack point would be vpn

**Riggs** - January 24, 2019, 9:31 am

(Jan 24, 2019 10:12 AM)Scaletta Wrote: [\[CITE\]](#) If you are doing something not approved by the government and the VPN keeps logs + shares with LE then you are very easily fucked. If the vpn provider does not keep logs then use tor with vpn by all means but question is how much are you willing to trust a vpn seller when they say they do not actually keep any logs.

Your domestic ISP keeps logs. A remote VPN seller claims they don't. Which is the more logical trust option of the two?

(Jan 24, 2019 10:12 AM)Scaletta Wrote: [\[CITE\]](#) With correlation attack, two servers (nodes) need to be targeted. With vpn just the server (1) user is connected to thus making the correlation attack a more complicated attack than vpn. Common attack point would be vpn

Scenario A:

- >Use Tor alone.
- >ISP logs you using Tor.
- >Government correlates your logs against Tor node/third-party server access logs.
- >Government identifies you as suspect.

Scenario B:

- >Use Tor over VPN.
- >ISP logs your VPN use.
- >Government hopes VPN provider keeps logs.
- >Government applies for international court order.
- >Government waits 2 - 4 months for court order approval.
- >Government hopes VPN provider still keeps logs.
- >Government hopes VPN provider will not dispute court order.
- >If captured log data is decipherable, Government correlates logs to identify you as user.
- >50 years have passed and you die of old age before investigation can continue.

**Scaletta** - January 24, 2019, 9:41 am

(Jan 24, 2019 10:31 AM)Riggs Wrote: [\[CITE\]](#) Your domestic ISP keeps logs. A remote VPN seller claims they don't. Which is the more logical trust option of the two?

Scenario A:

- >Use Tor alone.
- >ISP logs you using Tor.
- >Government correlates your logs against Tor node/third-party server access logs.

>Government identifies you as suspect.

Lets clarify some confusion that I'm facing now. In both the cases mentioned why would someone not be using a freely provided highly recommend option of "Bridges" in which your domestic ISP would not know of your tor usage?

Any true hacker or blackhat would know never commit crimes on their home computer. Always do it on a disposable RDP in which case it doesn't matter if correlation attack takes place because the IP address that would be revealed is of the RDP server which if configured and used properly (VPN connection to RDP) would not expose your home ip address.

**Agent Shark** - January 24, 2019, 9:46 am

(Jan 17, 2019 11:38 PM)hack3rcon Wrote: [\[CITE\]](#) But I guess governments can bypass Tor!!!

There is no 'bypass' per say. How TOR works is that a circuit is established when you wish to connect to the network. When visiting a website, a random circuit (utilizing various nodes) is established. Data is encrypted at each node and a key is generated between each communication hop. Your data can't be intercepted solely off of your connection due to the keys being different at each hop.

Ex. Hop 1 and Hop 4 can't communicate. Data must be reverse engineered via the keys exchanged between each hop. What compromises users is mistakes in exposing yourself via:Public information released while connected

Modifying the size window for your TOR connection

Utilizing personal information while using the TOR network.

I hope that clarifies your worries.

**Asdethprime** - January 24, 2019, 9:55 pm

(Jan 24, 2019 10:31 AM)Riggs Wrote: [\[CITE\]](#) Your domestic ISP keeps logs. A remote VPN seller claims they don't. Which is the more logical trust option of two?

Of course the ISP will be more secured for various reason.

REASON 1 = Logs that ISP keeps is based on you public IP address / I.e the IP address of your wifi access point. Your PC doesn't have its own IP address.

From ISP's point of view unless we are talking deep packet injection and other stuff ; which most ISP don't do ; their log will not be individualised. It's not your log it's the log for your whole network.

VPN on the other hand has username and password and is specific to you.

Not to mention if more than 1 person from the same house , for example , use TOR ISP has no way of differentiating it.

REASON 2 : government contacts ISP , awesome , and who would it be easier to get logs out of. A smaller VPN company or a much larger ISP?

Whose logs are going to be harder to Get.

---

But let's actually have a more resonable debate on this.

Let's debate , with logic and argument, why oh think VPN is required and why I argue against having VPN.

Everyone seems interested to know ; will u be up for it ?

I am current at work - I finish in 4 hours and tomorrow is Saturday (day off Yay!).

I am looking forward to this :)

**J8fr0XCXK2wb** - January 25, 2019, 3:09 am

(Jan 17, 2019 11:38 PM)hack3rcon Wrote: [\[CITE\]](#) But I guess governments can bypass Tor!!!  
A lot of people were found due to human errors or some flaws in the Tor Network.

**Riggs** - January 25, 2019, 6:45 pm

(Jan 24, 2019 10:55 PM)Asdethprime Wrote: [\[CITE\]](#) Of course the ISP will be more secured for various reason.

REASON 1 = Logs that ISP keeps is based on you public IP address / I.e the IP address of your wifi access point. Your PC doesn't have its own IP address.

From ISP's point of view unless we are talking deep packet injection and other stuff ; which most ISP don't do ; their log will not be individualised. It's not your log it's the log for your whole network. From a legal perspective, you're responsible for your domestic network connection anyway. Thinking your 50 hypothetical housemates living with you are enough to obfuscate a third-party identifying your specific network traffic over the Internet would be foolish. Whether it's an ISP or VPN provider, session cookies make tracking incredibly easy in practice, and NAT logs that map to devices on the LAN are accessible from most routers. The only time this might not apply is if you're using a shared network service in a building with public access (library, coffee shop, airport etc).

(Jan 24, 2019 10:55 PM)Asdethprime Wrote: [\[CITE\]](#) VPN on the other hand has username and password and is specific to you.

^^^ Sample of my old PureVPN credentials (altered to exhibit here, but same format as original).

In summary of addressing the threat model with the most viable solution, I would conclude that a VPN provider is the safer option. The reason for this is because remote-access VPNs typically leverage both legal and technical protections. Legally, logs are more difficult for the Government to compel disclosure of when the logs being requested are stored as data at rest on physical servers in countries outside their jurisdiction. Technically, even if those logs exist, they are likely to be stored in an encrypted state and therefore disclosed in an unintelligible format.

An ISP, on the other hand, does keep logs. Their legal and technical protections are both naturally very limited, and their disclosure to Government on receipt of a court order is typically unchallenged.

**Asdethprime** - January 25, 2019, 8:57 pm

(Jan 25, 2019 07:45 PM)Riggs Wrote: [\[CITE\]](#) From a legal perspective, you're responsible for your domestic network connection anyway. Thinking your 50 hypothetical housemates living with you are enough to obfuscate a third-party identifying your specific network traffic over the Internet would be

foolish. Whether it's an ISP or VPN provider, session cookies make tracking incredibly easy in practice, and NAT logs that map to devices on the LAN are accessible from most routers. The only time this might not apply is if you're using a shared network service in a building with public access (library, coffee shop, airport etc).

But this is assuming you are already signed in to something on Tor.

That's not how a hacker would use it right? I have absolutely no need to sign into anything when I am ping hosts to see which are alive. No reason for me scan when I am looking for documentation/source code / binary of what's running on the port.

If you are signed in somewhere and carry around sticky cookie, you have messed up already.

But a solution to that is not a new network middleware like VPN. It's a problem specific to the core backend of what is being run on your device. A more likely, free, solution to this problem (tracking through session cookie) are solved by using an OS build ground up to prevent this [ assuming no hardware level exploits ]. Example would be Tails, Whonix, TorVM for Qubes etc.

VPN hasn't helped here though at least not regarding cookie.

But logs part though, I would much rather trust my ISP than VPN but I would rather mention that in a different section.

[ quote]

In summary of addressing the threat model with the most viable solution, I would conclude that a VPN provider is the safer option.

[ /quote]

I obviously do not agree with the idea.

There is NO way for you to be sure VPN providers don't log, specially when you consider at the end of the day, VPN providers are NOT there to help you, their core motivation is money. They would rather server you to earn that money, but it's self serving. It is ALWAYS in VPN providers best interest to hold log because not doing so will increase the chances that they get tangled in a legal conflict. At the end of the day, whatever VPN company you talk to, none of them want to get into legal trouble, that's bad for business - like really bad - fatal for business.

=====

Now going back to the main argument, what exactly is VPN adding to the mix ?

=> Difficult for government entities to pull logs because they can be on a different country => You could have achieve the same result by setting up a 1 or multiple socks proxy on your path. You do not need VPN for that. If you need a tool to manage them proxychains-ng is awesome, allows you to natively set few proxies before reaching tor. You don't need VPN for that; well unless the debate breaks down to who do i now trust: the proxy server or VPN provider.

At least with proxy server a bit a headache to get up, but it does not really have much identification on you. Most allow you to create a few account and you can get proxychain to randomly pick a set number of proxies ( safe to stick with 1) but now you can specify a whole list of proxies all over the world and go with it. Proxies are free, slowly, vastly more likely to store logs, but they all get small pieces of the puzzle. None of them are centralized.

I would wager it would be harder to grab logs when you do not know which proxy the next request is going to before it reaches tor.

Does that make sense?

**Riggs** - January 26, 2019, 10:23 am

(Jan 25, 2019 09:57 PM)Asdethprime Wrote: [\[CITE\]](#) Does that make sense?  
No.

**Macroeconomics** - January 26, 2019, 12:52 pm

In general, TOR will protect your IP at all times. It's not foolproof though, there are times when you're still at risk. If the nodes you're using are compromised, nothing you do will be safe. That said, most of the time it's not a very big concern and you'll be protected. Also never use TOR in full-screen, your computer's resolution is now used to identify you as a user and assign it to a device you own.

If you're just looking to hide your IP, use a VPN like [censored] or PIA.

**Asdethprime** - January 26, 2019, 2:50 pm

(Jan 26, 2019 11:23 AM)Riggs Wrote: [\[CITE\]](#) No.

I understand that my english is not the greatest but if you could tell me which one did not make sense perhaps I could expand on that.

A reasonable debate, by defination, would go longer than a single word answer.

**Riggs** - January 26, 2019, 4:13 pm

(Jan 26, 2019 03:50 PM)Asdethprime Wrote: [\[CITE\]](#) I understand that my english is not the greatest but if you could tell me which one did not make sense perhaps I could expand on that.

A reasonable debate, by defination, would go longer than a single word answer.

If your ISP naturally retains logs and a VPN provider claims they do not, which option is more logically beneficial toward preserving user privacy/anonymity from Government access?

I say a VPN, you say your ISP.

Your English was fine, I just don't follow your logic and feel like I'm having to repeat myself.

**hack3rcon** - January 26, 2019, 10:23 pm

(Jan 24, 2019 10:31 AM)Riggs Wrote: [\[CITE\]](#) Your domestic ISP keeps logs. A remote VPN seller claims they don't. Which is the more logical trust option of the two?

Scenario A:

- >Use Tor alone.
- >ISP logs you using Tor.
- >Government correlates your logs against Tor node/third-party server access logs.
- >Government identifies you as suspect.

Scenario B:

- >Use Tor over VPN.
- >ISP logs your VPN use.
- >Government hopes VPN provider keeps logs.
- >Government applies for international court order.
- >Government waits 2 - 4 months for court order approval.
- >Government hopes VPN provider still keeps logs.

>Government hopes VPN provider will not dispute court order.

>If captured log data is decipherable, Government correlates logs to identify you as user.

>50 years have passed and you die of old age before investigation can continue.

I can't understand something. When a user use Tor then ISP and government can't see his/her real IP address, but when he/she use VPN and then Tor why it is bad? If Tor encrypt data all the time, then why worry?

(Jan 24, 2019 10:46 AM)Sh?rk Wrote: [\[CITE\]](#) There is no 'bypass' per say. How TOR works is that a circuit is established when you wish to connect to the network. When visiting a website, a random circuit (utilizing various nodes) is established. Data is encrypted at each node and a key is generated between each communication hop. Your data can't be intercepted solely off of your connection due to the keys being different at each hop.

Ex. Hop 1 and Hop 4 can't communicate. Data must be reverse engineered via the keys exchanged between each hop. What compromises users is mistakes in exposing yourself via:Public information released while connected

Modifying the size window for your TOR connection

Utilizing personal information while using the TOR network.

I hope that clarifies your worries.

As you know, governments use special packet filtering devices that are not publicly available. They ask networking companies for making these special devices for them, Then how you sure Tor is secure?

**Riggs** - January 26, 2019, 10:41 pm

(Jan 26, 2019 11:23 PM)hack3rcon Wrote: [\[CITE\]](#) I can't understand something. When a user use Tor then ISP and government can't see his/her real IP address, but when he/she use VPN and then Tor why it is bad? If Tor encrypt data all the time, then why worry?

Using a VPN and then Tor is not bad. Using Tor alone is not bad, it's just not as effective at preventing a correlation attack. Using Tor alone indicates to your ISP that your network was using Tor at a specific time. If the Government obtains these ISP logs and accesses the logs of the destination server, they can correlate this data to identify and understand your specific activities. This can be problematic.

ISP logs involve traffic metadata such as source and destination IP address, date and timestamp, size of the request etc. The destination server logs contains the same. If these are correlated, they can be used to identify your activities. Using a VPN and then Tor results in your ISP only seeing your tunneled connection to your VPN. Your ISP simply acts as a forwarder of the encrypted data being sent to/from your VPN. If served a court order, your ISP could only identify that you were using a VPN. They would be unable to identify what your activities were. This means a Government would ultimately need access to the VPN logs to identify and correlate your Tor activity, which may not be stored by the VPN provider anyway.

**Asdethprime** - January 27, 2019, 3:12 am

(Jan 26, 2019 05:13 PM)Riggs Wrote: [\[CITE\]](#) If your ISP naturally retains logs and a VPN provider claims they do not, which option is more logically beneficial toward preserving user privacy/anonymity from Government access?

I say a VPN, you say your ISP.

Your English was fine, I just don't follow your logic and feel like I'm having to repeat myself.  
Hehe so merely go based on VPN's word ??

The reason VPN is NOT recommend is quite simple, correlation attack itself relies on the idea of constant, something that is unchanging. Having a VPN on the link is not helping you.

If trust with ISP is a problem, you have a better alternative at hand, proxies, that are distributed , picked at random and no single proxy has enough information on it. Goes more hand in hand with the logic of tor.

The whole security of Tor , in regards to anonymity, can be broken down into the following concept:

- 1) Randomization Algorithm ( picking a random collection of node everytime)
- 2) Distrubition => node at not on any single contry under the control of any single organization ( and)
- 3) Encryption

Putting a centralized connection in the middle ( a VPN provider ) goes against the very principle of TOR.

If there was absolutely no other answer to the ISP log you have a better alternative Proxies. Proxychains-ng a technology used to simply adding proxies, is freely available. It lets you set a list of a whole lot of proxies and pick one at random before you reach TOR.

This is better simply because it works on EXACTLY the same principles as TOR - distributed network and no single proxy having enough information to help in correlation.

=====

You (Public IP = ISP) => VPN ( which is constant) => TOR ( where everything is randomized)

vs

You ( Public IP = ISP) => Proxy chains ( randomized) => TOR ( randomized )

=====

How is VPN going to be better suited against the correlation attack?

=====

Not to mention the main point stands, there is no reason to use VPN when you are using TOR. It's NOT an ideal solution, NOT recommended.

Stick with Tor and Tor related technologies 1) Proxychains-ng (ISP Logs) and 2) Tails ( persistent cookies).

What benefit do you see of VPN?

And now do you see why VPN makes it worse off?

Riggs - January 27, 2019, 1:29 pm  
(Jan 27, 2019 04:12 AM)Asdethprime Wrote: [CITE](#) What benefit do you see of VPN?

And now do you see why VPN makes it worse off?  
We're going in circles here. Let's just accept that we're never going to agree on this.

**Asdethprime** - January 27, 2019, 3:23 pm

Very well than ; let's just agree to disagree :)

**Scaletta** - January 27, 2019, 9:39 pm

(Jan 24, 2019 10:55 PM)Asdethprime Wrote: [\[CITE\]](#) Of course the ISP will be more secured for various reason.

REASON 1 = Logs that ISP keeps is based on you public IP address / I.e the IP address of your wifi access point. Your PC doesn't have its own IP address.

From ISP's point of view unless we are talking deep packet injection and other stuff ; which most ISP don't do ; their log will not be individualised. It's not your log it's the log for your whole network.

VPN on the other hand has username and password and is specific to you.

Not to mention if more than 1 person from the same house , for example , use TOR ISP has no way of differentiating it.

REASON 2 : government contacts ISP , awesome , and who would it be easier to get logs out of. A smaller VPN company or a much larger ISP?

Whose logs are going to be harder to Get.

---

But let's actually have a more resonable debate on this.

Let's debate , with logic and argument, why oh think VPN is required and why I argue against having VPN.

Everyone seems interested to know ; will u be up for it ?

I am current at work - I finish in 4 hours and tomorrow is Saturday (day off Yay!).

I am looking forward to this :)

Some government agencies have either a backdoor or specialized emergency hotlines to get access to user data without warrant. Its a known fact. Also shown in Mr. Robot

**PerfectStorm** - January 27, 2019, 9:41 pm

I highly doubt it would reveal your IP.

**shelled** - January 27, 2019, 9:49 pm

this thread makes me cut myself

**hack3rcon** - January 31, 2019, 10:49 pm

Thus VPN+Tor or Tor alone are not bad?

**CHICKENWING12** - February 1, 2019, 6:26 am

Tor is used a lot by hackers. The only thing to care is flash objects, your browsers special footprints

**hack3rcon** - February 2, 2019, 5:38 am

Thus, Tor is enough?

If the web site use flash then any solution?

**anonymous1988** - February 9, 2019, 11:58 am

No!

Tor gives a false IP address that is not related to its own

**meridian1** - February 9, 2019, 7:46 pm

(Jan 15, 2019 01:22 AM)Asdethprime Wrote: [\[CITE\]](#) Rather than asking why not try. It won't be able to tell your real IP address when u use tor.

For an easy test try it out. Open a normal web browser. Go to google and search what is my IP address. Save that. Then open a tor browser ; do exactly that and see how different your IP looks. vouch for this

**Scaletta** - February 9, 2019, 11:00 pm

(Feb 2, 2019 06:38 AM)hack3rcon Wrote: [\[CITE\]](#) Thus, Tor is enough?

If the web site use flash then any solution?

You could always use tails which won't reveal your ISP IP address even if javascript, webRTC, flash etc are turned on.

**SysAdmin** - February 10, 2019, 4:30 pm

(Jan 23, 2019 05:20 AM)Asdethprime Wrote: [\[CITE\]](#) Contrary to what people repeat here over and over again, VPN is NOT RECOMMENDED with TOR. Just don't you are not getting extra security you are risking your privacy because now there are 2 ways to track who you are from 1) break Tor or 2) break into VPN's log.

I know this sounds counterproductive, you have seen so many website, so many articles ; but the truth remains. The only viable way to knowing who you are behind tor ( provided you are using it properly) is a correlation attack; and that's checked based on VPN.

Also a malicious exit node CAN ONLY SEE what website you are visiting. In this case, a malicious exit node will be able to see someone, using Tor is visiting the government website. It won't be able to trace it back to you.

A malicious entry node would have the opposite effect, if will be able to find who you are but not find out what you are seeing.

He's correct.

In order for people to trace back any instances on what you're doing, they would have to control all of the nodes you go through.

**hack3rcon** - February 15, 2019, 10:07 pm

(Feb 10, 2019 12:00 AM)Scaletta Wrote: [\[CITE\]](#) You could always use tails which won't reveal your ISP IP address even if javascript, webRTC, flash etc are turned on. Really? "Tails" never reveal my real IP even if some plugins and extensions are enabled? Why Tor not added this feature?

**Asdethprime** - February 16, 2019, 2:39 am

(Feb 15, 2019 11:07 PM)hack3rcon Wrote: [\[CITE\]](#) Really? "Tails" never reveal my real IP even if some plugins and extensions are enabled? Why Tor not added this feature?

Because it's very difficult for a browser to enforce such separation ; For an operating system however it's trivial.

Tor is just the system when people say tor people think about a web browser , I.e the tor browser.

Tails is a full customised version of Linux to support tor. In essence Tails is an OS built with tor.

Is it really surprising that an Operating System can do more than a web browser ?

**aerohacker** - February 17, 2019, 9:19 pm

(Jan 17, 2019 11:48 PM)Mikutype Wrote: [\[CITE\]](#) Get into tor browser and done. This is a basic question.

Download Tor Browser. Go to website. Done. They won't find your ip.

First vpn then tor it is a better formula though, but you do not need to be that paranoid.

Gov could potentially use deep packet inspection to find your browsing habits even being vpn + tor or tor alone, yes.

Some questions about Tails:

- 1) It's safe to use Tails at home?
- 2) What precautions should I take when I'll use Tails at home?
- 3) There is any difference between to use Tails in dual boot, Virtual Machine or USB stick?