

Forum: [Hack Forums](#)

Thread: [TOR Vs. VPNs = TOR wins](#)

?Criminal - August 19, 2017, 11:07 am

Heres a simple fact on why TOR beats VPN's:

- it's infrastructure is safe and sound it's basically FED proof the only way you can get busted on tor is human failure also known as opsec slips, another way is zero days in the tor browser but if you're smart your gonna use a different browser with TOR or just run it in a VM for even more security. VPN's on the otherhand provide privacy only not anonymity because it's not decentralized like TOR theres always someone that owns the VPN server where as no one owns TOR and centralized things aren't smart to use if the FBI wants you they will attempt to contact the owner of the VPN server if that fails they will then go up the ladder to the datacenter owner and ask where that rack is located and some details about the rack asking nicely and if they still don't get there way the last resort is them getting an MLAT traveleing to that offshore country, busting the door down of the datacenter, inserting a ram scraping device while the boxs are online and then imaging the boxs HDD if need be. VPN's are not unbreakable as people seem to think, even the so called no log vpns aren't exactly safe. Not only that but theres various client side attacks you can use against your target to bypass vpns which I made a thread on covering all reasonable methods to get your targets home IP which in theory would work on TOR as well since you're relying on the human element for a lot of them but you should always be vigilant to protect your self from attackers that want to deanonymize you.

'OverSight - August 19, 2017, 11:14 am

This should be pinned because everyone in here seems to think VPNs are god tools.

lwristis - August 19, 2017, 11:16 am

Even "no-log" VPNs' ISPs log.

?Criminal - August 19, 2017, 11:34 am

(Aug 19, 2017 11:16 AM)oxid Wrote: [\[CITE\]](#) Even "no-log" VPNs' ISPs log.

Well most people know what I mean by "no log" have to keep it understandable for the masses, most people don't think about the ISP of the datacenter keeping logs but even outside of that the feds would go for the rack it self it's happened with earthvpn and PIA and it will continue to happen with more providers in the coming years, the ISP keeping logs is the least of the customers worries when the entire box gets seized and all customers get exposed all because one customer was a bad apple.

notluther - August 19, 2017, 2:40 pm

(Aug 19, 2017 11:07 AM)?Criminal Wrote: [\[CITE\]](#) - it's infrastructure is safe and sound it's basically FED proof

How exactly is Tor's infrastructure "fed proof"? The decentralized nature of Tor makes it hard to attack in this way but by no means does it make it impossible. Do you think that if a nation state was interested in attacking Tor in this way, that they'd be unable to?

(Aug 19, 2017 11:07 AM)?Criminal Wrote: [\[CITE\]](#) the only way you can get busted on tor is human failure also known as opsec slips, another way is zero days in the tor browser

I'd try to steer clear of making such claims in the future. There are plenty of attacks against Tor that don't rely on poor OPSEC or Firefox 0days. Find them here:

https://en.wikipedia.org/wiki/Tor_%28anonymity_network%29#Weaknesses

(Aug 19, 2017 11:07 AM)?Criminal Wrote: [\[CITE\]](#) but if you're smart your gonna use a different browser with TOR

DON'T do this. Please DON'T do this. You will deanonymize yourself unintentionally. The Tor Browser has been hardened in the sense that many forms of active content (flash, js, java, etc) are at the very least click-to-play by default (not so in the case of javascript due to usability concerns). You put yourself at risk of having your real IP exposed by allowing these things to run in your browser.

(Aug 19, 2017 11:07 AM)?Criminal Wrote: [\[CITE\]](#) just run it in a VM for even more security.

Running the Tor Browser inside of a VM will protect you from malware (even then, advanced malware can escape hypervisors, and then you're fucked) and that's about it. All other attacks against Tor are still on the table and you can still be deanonymized.

How you use Tor comes down to your threat model, which is something I would recommend to everybody interested in privacy/anonymity to have a very strong understanding of. It boils down to three things:

- 1) What information are you protecting?
- 2) Who are you protecting this information from?
- 3) What risks do you face if this information is leaked?

For many people, they simply don't feel comfortable with ad networks having the information necessary to target them and track them across the web. Others are worried about government surveillance, and even still others are literally at risk of death or imprisonment should their location be exposed through their IP address. Knowing where you fall on this spectrum will help you to make more educated decisions about how you use a piece of software like Tor.

lwristis - August 19, 2017, 7:32 pm

(Aug 19, 2017 02:40 PM)Ed25519 Wrote: [\[CITE\]](#) How exactly is Tor's infrastructure "fed proof"? The decentralized nature of Tor makes it hard to attack in this way but by no means does it make it impossible. Do you think that if a nation state was interested in attacking Tor in this way, that they'd be unable to?

I'd try to steer clear of making such claims in the future. There are plenty of attacks against Tor that don't rely on poor OPSEC or Firefox 0days. Find them here:

https://en.wikipedia.org/wiki/Tor_%28anonymity_network%29#Weaknesses

DON'T do this. Please DON'T do this. You will deanonymize yourself unintentionally. The Tor Browser has been hardened in the sense that many forms of active content (flash, js, java, etc) are at the very least click-to-play by default (not so in the case of javascript due to usability concerns). You put yourself at risk of having your real IP exposed by allowing these things to run in your browser.

Running the Tor Browser inside of a VM will protect you from malware (even then, advanced malware can escape hypervisors, and then you're fucked) and that's about it. All other attacks against Tor are still on the table and you can still be deanonymized.

How you use Tor comes down to your threat model, which is something I would recommend to everybody interested in privacy/anonymity to have a very strong understanding of. It boils down to

three things:

- 1) What information are you protecting?
- 2) Who are you protecting this information from?
- 3) What risks do you face if this information is leaked?

For many people, they simply don't feel comfortable with ad networks having the information necessary to target them and track them across the web. Others are worried about government surveillance, and even still others are literally at risk of death or imprisonment should their location be exposed through their IP address. Knowing where you fall on this spectrum will help you to make more educated decisions about how you use a piece of software like Tor.

Could not have put it in better words myself.

lwristis - August 19, 2017, 7:40 pm

(Aug 19, 2017 07:38 PM)nekoz Wrote: [\[CITE\]](#) If you just want to surf the web anonymously, then Tor may be sufficient. But if you want better privacy protection, enhanced security from hackers, identity thieves and malware, and speed, then a VPN service is likely a better option. Since when do VPNs protect from MALWARE?

M3m3Destr0y3r - August 19, 2017, 7:42 pm

(Aug 19, 2017 07:40 PM)oxid Wrote: [\[CITE\]](#) Since when do VPNs protect from MALWARE? protection requires traffic inspection on VPN servers using anti-malware/virus/etc gateway software

c_-m - August 19, 2017, 7:45 pm

(Aug 19, 2017 07:42 PM)nekoz Wrote: [\[CITE\]](#) protection requires traffic inspection on VPN servers using anti-malware/virus/etc gateway software

I believe you have it wrong, vpn's offer privacy while tor "offers" anonymity. Sure it isn't some god like tool but I would trust it over some sellout vpn provider anyday.

?Criminal - August 19, 2017, 9:14 pm

(Aug 19, 2017 02:40 PM)Ed25519 Wrote: [\[CITE\]](#) How exactly is Tor's infrastructure "fed proof"? The decentralized nature of Tor makes it hard to attack in this way but by no means does it make it impossible. Do you think that if a nation state was interested in attacking Tor in this way, that they'd be unable to?

I'd try to steer clear of making such claims in the future. There are plenty of attacks against Tor that don't rely on poor OPSEC or Firefox 0days. Find them here:

https://en.wikipedia.org/wiki/Tor_%28anonymity_network%29#Weaknesses

DON'T do this. Please DON'T do this. You will deanonymize yourself unintentionally. The Tor Browser has been hardened in the sense that many forms of active content (flash, js, java, etc) are at the very least click-to-play by default (not so in the case of javascript due to usability concerns). You put yourself at risk of having your real IP exposed by allowing these things to run in your browser.

Running the Tor Browser inside of a VM will protect you from malware (even then, advanced malware can escape hypervisors, and then you're fucked) and that's about it. All other attacks against Tor are still on the table and you can still be deanonymized.

How you use Tor comes down to your threat model, which is something I would recommend to

everybody interested in privacy/anonymity to have a very strong understanding of. It boils down to three things:

- 1) What information are you protecting?
- 2) Who are you protecting this information from?
- 3) What risks do you face if this information is leaked?

For many people, they simply don't feel comfortable with ad networks having the information necessary to target them and track them across the web. Others are worried about government surveillance, and even still others are literally at risk of death or imprisonment should their location be exposed through their IP address. Knowing where you fall on this spectrum will help you to make more educated decisions about how you use a piece of software like Tor.

The academic attacks you cite and this scenario you're describing is not realistic, most of these attacks require active recon not passive recon, if someone goes on tor and does a hypothetical black hat activity such as for example doing some sort of fraud and the web application logs his creation IP and last login IP as a tor exit node, the sysadmin then sends it to law enforcement and the case will go cold with law enforcement left scratching their heads, if the persons smart changes nodes frequently, doesn't make a tell tale consistent pattern of their tor usage most of these attacks would not be feasible, if all LE has on you is a tor exit node IP then how can any agency magically figure out the users location? you would have to be a threat to national security for a government agency to somehow compromise tor using things such as the sniper attack, traffic confirmation attacks, etc trust me I know about all of it your telling me stuff im aware of, if TOR was broken all drug onion owners would of been discovered and charged, literally the only reason the bay sites got seized was because they ran misconfigured apache and thats been known to be a problem when it comes to deanonymizing hidden services but if you cover all your bases even if it ever came down to your hidden service falling down if you registered the box with fake credentials and logged in to the box not on a home connection you should be fine, I know plenty of people that leverage TOR properly so im definitely right when I say it's safer compared to a VPN. TL;DR if you use TOR smartly, only use it when necessary then things like traffic confirmation becomes useless and if all they have on you is a tor exit node IP you are perfectly fine, this isn't even factoring the extra protection you get adding socks, a VPN and VM on top of TOR but I would never recommend using a VPN by it self for BH usage thats just asking to get busted down the line. Awhile back I made a post similiar to this on a thread that true demon also brought up a good point on but at the end of the day unless you're doing BH activity to the point where you have INTERPOL after you I highly doubt you have anything to worry about. if you're that paranoid use a dual band antenna or make a cantenna and use a food chains wifi on top of everything else as well but IMO thats over doing it. I also never said it was impossible but it's extremely difficult, theres ways around everything I mean I recently showed it was possible to get around ask fm anonymity and similiar sites using a very clever concept so I understand where you're coming from. I call it like I see it based on empirical evidence, till I see smoking gun proof of people getting busted on tor outside of OPSEC or 0days then my point will always be the same in that TOR will always supersede VPN's in my eyes. Also most people that will use TOR properly won't just use a mainstream browser you're obviously gonna use something hardened why would anyone in the world be dumb enough to use chrome or IE with TOR in the first place you act like people are dumb enough to run JS, but if they want a recommended browser choice the best is one like you stated one that has no dynamic content, in this case text based browsers like elinks can even be more secure then browsers with unnecessary features like chrome who needs all that when you're trying to obtain anonymity. None of these are claims btw it's all factual the only realistic way you can debunk TOR not being better then a VPN or not being fed proof is showing me a legal precedent where in the case they explicitly show they leveraged one of these network attacks against the TOR infrastruture it self to catch the person such as messing with guard nodes, sybil attacks by flooding the tor network with honeypot exit nodes, etc you get the picture.

EDIT: "In fact, as late as September 2016, FBI could not locate, de-anonymize and identify the Tor user who hacked into the email account of a staffer on Hillary Clinton's email server." straight from that wikipedia page just proves my point it's FED proof, the FBI themselves still haven't caught the guys behind the DNC breach either I believe since it was all the same guys involved in the clinton email server breach too.

relegoz19 - August 20, 2017, 11:33 am

vpn chaining is superior to Tor also the FBI wasn't allowed to inspect the services the DNC only allowed a private firm to inspect it .This was testified before a hearing. Another thing that should be noted is i believe it was the nation who provided more forensic evidence that the hacker was rather had physical access by providing detail logs of the metadata of the incident as compared to the FBI's evidence that a hacker did it because 17 agencies testified so including the coastguard and that's all they've provided. Thank god we weren't sure if it was a hacker or not until the coastguard weighed in .

notluther - August 20, 2017, 8:55 pm

(Aug 19, 2017 09:14 PM)?Criminal Wrote: [\[CITE\]](#) The academic attacks you cite and this scenario you're describing is not realistic, most of these attacks require active recon not passive recon, if someone goes on tor and does a hypothetical black hat activity such as for example doing some sort of fraud and the web application logs his creation IP and last login IP as a tor exit node, the sysadmin then sends it to law enforcement and the case will go cold with law enforcement left scratching their heads, if the persons smart changes nodes frequently, doesn't make a tell tale consistent pattern of their tor usage most of these attacks would not be feasible, if all LE has on you is a tor exit node IP then how can any agency magically figure out the users location? you would have to be a threat to national security for a government agency to somehow compromise tor using things such as the sniper attack, traffic confirmation attacks, etc trust me I know about all of it your telling me stuff im aware of, if TOR was broken all drug onion owners would of been discovered and charged, literally the only reason the bay sites got seized was because they ran misconfigured apache and thats been known to be a problem when it comes to deanonymizing hidden services but if you cover all your bases even if it ever came down to your hidden service falling down if you registered the box with fake credentials and logged in to the box not on a home connection you should be fine, I know plenty of people that leverage TOR properly so im definitely right when I say it's safer compared to a VPN. TL;DR if you use TOR smartly, only use it when necessary then things like traffic confirmation becomes useless and if all they have on you is a tor exit node IP you are perfectly fine, this isn't even factoring the extra protection you get adding socks, a VPN and VM on top of TOR but I would never recommend using a VPN by it self for BH usage thats just asking to get busted down the line. Awhile back I made a post similiar to this on a thread that true demon also brought up a good point on but at the end of the day unless you're doing BH activity to the point where you have INTERPOL after you I highly doubt you have anything to worry about. if you're that paranoid use a dual band antenna or make a cantenna and use a food chains wifi on top of everything else as well but IMO thats over doing it. I also never said it was impossible but it's extremely difficult, theres ways around everything I mean I recently showed it was possible to get around ask fm anonymity and similiar sites using a very clever concept so I understand where you're coming from. I call it like I see it based on empirical evidence, till I see smoking gun proof of people getting busted on tor outside of OPSEC or 0days then my point will always be the same in that TOR will always supersede VPN's in my eyes. Also most people that will use TOR properly won't just use a mainstream browser you're obviously gonna use something hardened why would anyone in the world be dumb enough to use chrome or IE with TOR in the first place you act like people are dumb enough to run JS, but if they want a recommended browser choice the best is one like you stated one that has no dynamic content, in this case text based browsers like elinks can even be more secure then browsers with unnecessary features like chrome who needs all that when you're trying to obtain anonymity. None of these are claims btw it's all factual the only realistic way you can debunk TOR not being better then a VPN or not being fed proof is showing me a legal precedent

where in the case they explicitly show they leveraged one of these network attacks against the TOR infrastructure it self to catch the person such as messing with guard nodes, sybil attacks by flooding the tor network with honeypot exit nodes, etc you get the picture.

EDIT: "In fact, as late as September 2016, FBI could not locate, de-anonymize and identify the Tor user who hacked into the email account of a staffer on Hillary Clinton's email server." straight from that wikipedia page just proves my point it's FED proof, the FBI themselves still haven't caught the guys behind the DNC breach either I believe since it was all the same guys involved in the clinton email server breach too.

I don't disagree with you on Tor being better than a VPN. Perhaps I should have made it clear that being subject to any of these very targeted attacks requires you to be a very wanted person. Of course most people will never face that kind of heat.

I appreciate that you took the time to clarify your point of view on this, as it helped me to better understand exactly what your intentions were in creating this thread.

(Aug 20, 2017 11:33 AM)relegoz19 Wrote: [\[CITE\]](#) vpn chaining is superior to Tor
I'm interested in hearing what makes you think that.

relegoz19 - August 20, 2017, 9:25 pm

(Aug 20, 2017 08:55 PM)Ed25519 Wrote: [\[CITE\]](#) I don't disagree with you on Tor being better than a VPN. Perhaps I should have made it clear that being subject to any of these very targeted attacks requires you to be a very wanted person. Of course most people will never face that kind of heat.

I appreciate that you took the time to clarify your point of view on this, as it helped me to better understand exactly what your intentions were in creating this thread.

I'm interested in hearing what makes you think that.

.It's chaining multiple IPs to bounce one packet from the first hop to second hop to third hop just like TOR except you get to control your hops unlike Tor .With more choices you have the potential to make a better security setup but also a shittier setup if you choose shitty hops like hidemyass.

How about you try convincing me how anybody thinks security against the most advanced agency in human history just involves downloading an exe file off the internet and double clicking it.

?Criminal - August 20, 2017, 9:41 pm

(Aug 20, 2017 09:25 PM)relegoz19 Wrote: [\[CITE\]](#) .It's chaining multiple IPs to bounce one packet from the first hop to second hop to third hop just like TOR except you get to control your hops unlike Tor .With more choices you have the potential to make a better security setup but also a shittier setup if you choose shitty hops like hidemyass.

How about you try convincing me how anybody thinks security against the most advanced agency in human history just involves downloading an exe file off the internet and double clicking it.

a multi hop VPN is better then a single hop vpn but it just makes it a bit harder for the feds in the fact that they have to wiretap multiple data centers and as we seen recently with the lizardstresser criminal complaint the feds have no problem issuing an MLAT to an offshore hosting provider just to nail someone down, TOR takes the centralized nature of VPN's out of the equation with TOR, the feds can't MLAT offshore servers to find you and most APT groups don't breach things with normal exe files anymore due to mail filters, they utilize other file formats that by nature allow code execution or file format memory corruption exploits and use these as droppers which DL and execute the exe file onto disk unless it's a fileless payload that runs completely in RAM. But anyways the feds can literally just sit and wait for the home connection to be logged on each box

you hop through it's just a game of cat and mouse at that point for them.

relegoz19 - August 20, 2017, 9:56 pm

(Aug 20, 2017 09:41 PM)?Criminal Wrote: [\[CITE\]](#) a multi hop VPN is better then a single hop vpn but it just makes it a bit harder for the feds in the fact that they have to wiretap multiple data centers and as we seen recently with the lizardstresser criminal complaint the feds have no problem issuing an MLAT to an offshore hosting provider just to nail someone down, TOR takes the centralized nature of VPN's out of the equation with TOR, the feds can't MLAT offshore servers to find you and most APT groups don't breach things with normal exe files anymore due to mail filters, they utilize other file formats that by nature allow code execution or file format memory corruption exploits and use these as droppers which DL and execute the exe file onto disk unless it's a fileless payload that runs completely in RAM. But anyways the feds can literally just sit and wait for the home connection to be logged on each box you hop through it's just a game of cat and mouse at that point for them.

random thing was reading about lizardstresser on krebonson security and somewhere down the article it screen shots this website as being monitored lol

SIM-1073426 - August 21, 2017, 2:59 am

You shouldn't configure Tor with another browser other than the Tor Browser, this is because the Tor community has given A LOT of configurations in their modified Firefox browser to prevent IP leaks. If you setup your own you can create a mistake.

Criminal is right and everyone here should also benefit from checking out what The Grugq has to say about OPSEC.

.Hydra - August 21, 2017, 5:30 am

Why not use both?

/threadkek

notluther - August 21, 2017, 2:33 pm

(Aug 20, 2017 09:25 PM)relegoz19 Wrote: [\[CITE\]](#) .It's chaining multiple IPs to bounce one packet from the first hop to second hop to third hop just like TOR except you get to control your hops unlike Tor .With more choices you have the potential to make a better security setup but also a shittier setup if you choose shitty hops like hidemyass.

How about you try convincing me how anybody thinks security against the most advanced agency in human history just involves downloading an exe file off the internet and double clicking it.

I see what you're saying about getting to choose your hops but I'm failing to see how that's a benefit and not a burden to you as a user. You have no way of knowing if the hops you're using are compromised regardless of whether you chain VPNs or use Tor, and in the case of Tor, while obviously I can't confirm this, I'd wager to guess that the majority of tor nodes are not compromised. Rogue entries don't stand to gain much except a bunch of Tor users' IP addresses, and rogue exits get marked with the BadExit flag and then ignored when Tor builds a circuit, and middle nodes don't see anything except other Tor nodes.

VPNs on the other hand are quite the target, and by comparison it would be much easier to fuck with a VPN user or users by targeting their VPN company than it would be to fuck a Tor user.

(Aug 20, 2017 09:25 PM)relegoz19 Wrote: [\[CITE\]](#) How about you try convincing me how anybody thinks security against the most advanced agency in human history just involves downloading an exe file off the internet and double clicking it.

Are you not reading the thread or something? The point that I've been trying to make is that Tor is

NOT a magic bullet. If you are wanted by a nation state you will be caught. It is that simple. All Tor and any other piece of software will do is simply delay the inevitable.

(Aug 21, 2017 05:30 AM).Hydra Wrote: [\[CITE\]](#) Why not use both?
/threadkek

Using a VPN to connect to your entry guard doesn't actually provide you with any more security than not using one. The same goes for using Tor to connect to your VPN. I'd imagine that most people actually do use both though, but probably because they're using Tor while already connected to a VPN for other reasons. See this blog post for more info on why it isn't exactly a net gain for your security: <https://matt.traudt.xyz/posts/vpn-tor-not-mRikAa4h.html>

MuffinRag - August 21, 2017, 3:17 pm

Ahh I always thought "Onions" made you cry.

_bengi - August 22, 2017, 3:30 am

(Aug 19, 2017 02:40 PM)Ed25519 Wrote: [\[CITE\]](#) Do you think that if a nation state was interested in attacking Tor in this way, that they'd be unable to?

Yes. Read the Snowden documents. In 2013, Tor was giving the NSA a hard time.

(Aug 20, 2017 09:25 PM)relegoz19 Wrote: [\[CITE\]](#) just like TOR except you get to control your hops unlike Tor

You can control your hops with tor.

(Aug 21, 2017 02:33 PM)Ed25519 Wrote: [\[CITE\]](#) Are you not reading the thread or something? The point that I've been trying to make is that Tor is NOT a magic bullet. If you are wanted by a nation state you will be caught. It is that simple. All Tor and any other piece of software will do is simply delay the inevitable.

Not exactly.

(Aug 20, 2017 11:33 AM)relegoz19 Wrote: [\[CITE\]](#) also the FBI wasn't allowed to inspect the services the DNC only allowed a private firm to inspect it .This was testified before a hearing.

The DNC is based in the US and therefore is subject to US law. The FBI can do what they want and they don't need the permission of anyone.

(Aug 20, 2017 11:33 AM)relegoz19 Wrote: [\[CITE\]](#) Another thing that should be noted is i believe it was the nation who provided more forensic evidence that the hacker was rather had physical access by providing detail logs of the metadata of the incident as compared to the FBI's evidence that a hacker did it because 17 agencies testified so including the coastguard and that's all they've provided.Thank god we weren't sure if it was a hacker or not until the coastguard weighed in .

Fake news.

notluther - August 22, 2017, 6:23 am

(Aug 22, 2017 03:30 AM)_bengi Wrote: [\[CITE\]](#) Yes. Read the Snowden documents. In 2013, Tor was giving the NSA a hard time.

My question was more about a nation state attempting to attack the Tor infrastructure, i.e attacking Tor nodes and just grabbing the traffic from them. They could in theory also set up a shit ton of their own boxes but this is quite loud and would probably not work as well as they intended due to things like the BadExit flag as well as other variables.

Also, Snowden was 2013. It is now 2017, surely they've made some progress, no?

_bengi - August 22, 2017, 10:18 am

(Aug 22, 2017 06:23 AM)Ed25519 Wrote: [\[CITE\]](#) My question was more about a nation state attempting to attack the Tor infrastructure, i.e attacking Tor nodes and just grabbing the traffic from them. They could in theory also set up a shit ton of their own boxes but this is quite loud and would probably not work as well as they intended due to things like the BadExit flag as well as other

variables.

Also, Snowden was 2013. It is now 2017, surely they've made some progress, no?

Yeah, that's definitely possible, but very likely to be detected. And probably not by the looks of it.

newbiebewbie - *August 23, 2017, 11:56 am*

I thought vpn+tor is the best solution..