

Forum:[Hack Forums](#)

Thread: ["NSA wants you to use Tor!"](#)

splunk - August 4, 2014, 3:34 pm

Q: Should we trust Tor?

A: No. Do NOT trust Tor with your anonymity.

Tor users often make a big deal of the fact that the NSA admits in its own internal documents that Tor makes surveillance more work-intensive for them. What these proponents fail to acknowledge is that the spies at the NSA also worry that Internet users will abandon Tor. Reason is:

“A critical mass of targets use Tor. Scaring them away from Tor might be counterproductive”

Tor is a signal to spies, a big waving flag that gets their attention and literally draws them to your network traffic. Certain aspects of Tor might be hard to trace, but ultimately the NSA wants people to keep using Tor. This highlights the fact that security services, like the FBI, have developed sophisticated tools to remove the veil of anonymity that Tor aims to provide.

For example, the Washington Post reports:

“One document provided by Snowden included an internal exchange among NSA hackers in which one of them said the agency’s Remote Operations Center was capable of targeting anyone who visited an al-Qaeda Web site using Tor.”

It’s well known that Tor is susceptible to what’s called a traffic confirmation attack (AKA end-to-end correlation), where an entity monitoring the network traffic on both sides of a Tor session can wield statistical tools to identify a specific communication path. Keep in mind that roughly 90 percent of the world’s internet communication flows through the United States, so it’s easy for U.S. intelligence to deploying this approach by watching data flows around entry and exit points.

SOURCES:

Spoiler ([Click to View](#)) 1 Cooper Quintin, “7 Things You Should Know About Tor,” Electronic Frontier Foundation, July 1, 2014,

<https://www.eff.org/deeplinks/2014/07/7-things-you-should-know-about-tor>

2 'Tor Stinks' presentation, Guardian, October 4, 2013,

<http://www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document>

3 J. Appelbaum, A. Gibson, J. Goetz, V. Kabisch, L. Kampf, L. Ryge, “NSA targets the privacy-conscious,”

http://daserste.ndr.de/panorama/aktuell/nsa230_page-1.html

4 Kevin Poulsen, “FBI Admits It Controlled Tor Servers Behind Mass Malware Attack,”

Wired, September 13, 2013, <http://www.wired.com/threatlevel/2013/09/freedom-hosting-fbi/>

5 Barton Gellman, Craig Timberg, and Steven Rich, “Secret NSA documents show campaign against Tor encrypted

network," Washington Post, October 4, 2013

6 James Ball, "NSA stores metadata of millions of web users for up to a year, secret files show," Guardian, September 30, 2013,
<http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year/documents/print>

7 Maxim Kammerer, [tor-talk] End-to-end correlation for fun and profit, August 20, 2007,
<https://lists.torproject.org/pipermail/tor-talk/2012-August/025254.html>

TL;DR: Don't keep your eggs in one hand basket. Mix up your setup, Don't rely on Tor.

If you EVER need help with anonymity, pm me

ThrobinHood - August 4, 2014, 3:36 pm

Nice post man always worth a read :)

Hunting Rifle - August 4, 2014, 3:38 pm

This is what they want you think. They know that the stupid people will still use it, and they don't care about them. They want you to move over. They can't crack tor.

What do you say about this OP?

splunk - August 4, 2014, 3:52 pm

(Aug 4, 2014 03:38 PM)Hunting Rifle Wrote: [\[CITE\]](#) This is what they want you think. They know that the stupid people will still use it, and they don't care about them. They want you to move over. They can't crack tor.

What do you say about this OP?

Of course they can't "crack" or even "stop" Tor. Your identity has potential to be leaked or intercepted while using Tor, however, and they have the technology to do this.

Jake Miller - August 4, 2014, 4:12 pm

(Aug 4, 2014 03:52 PM)PARTYNEXTDOOR Wrote: [\[CITE\]](#) Of course they can't "crack" or even "stop" Tor. Your identity has potential to be leaked or intercepted while using Tor, however, and they have the technology to do this.

Wrong Tor is indeed crackable. Their bounty just isn't big enough for the major hackers to even think about trying to crack tor.

logging*machine - August 4, 2014, 4:16 pm

Tor is 3 layered, and the routers they use is constantly changing, the only thing they could potentially get from Tor is the data they send over

splunk - August 4, 2014, 4:17 pm

(Aug 4, 2014 04:12 PM)Jake Miller Wrote: [\[CITE\]](#) Wrong Tor is indeed crackable. Their bounty just isn't big enough for the major hackers to even think about trying to crack tor.

It's not "hackers" they're worried about.

terrorism groups, fraudsters, hitmen, drug lords, weapons traffickers.

hackers are the least of their worries

ThrobinHood - August 4, 2014, 4:26 pm

Ye for those who say its unbreakable just read their blog <https://blog.torproject.org/>

Omniscient - August 4, 2014, 5:53 pm

IMHO if you need TOR to hide your activity then you're likely doing something maybe you shouldn't be in which case you're not safe. You're only truly safe when you're not doing things you shouldn't be.

But to speak directly about TOR being unsafe for use because of the NSA. I don't believe TOR can be trusted simply because anyone can setup a node. For all anyone knows the NSA might control dozens or even hundreds of nodes.

Light Yagami - August 4, 2014, 5:59 pm

(Aug 4, 2014 05:53 PM)Omniscient Wrote: [\[CITE\]](#) IMHO if you need TOR to hide your activity then you're likely doing something maybe you shouldn't be in which case you're not safe. You're only truly safe when you're not doing things you shouldn't be.

But to speak directly about TOR being unsafe for use because of the NSA. I don't believe TOR can be trusted simply because anyone can setup a node. For all anyone knows the NSA might control dozens or even hundreds of nodes.

I think you just nailed it!

I never trusted tor either, but wasn't sure how to put it.

peace

FFO

Machiavellian101 - August 4, 2014, 5:59 pm

(Aug 4, 2014 05:53 PM)Omniscient Wrote: [\[CITE\]](#) IMHO if you need TOR to hide your activity then you're likely doing something maybe you shouldn't be in which case you're not safe. You're only truly safe when you're not doing things you shouldn't be.

But to speak directly about TOR being unsafe for use because of the NSA. I don't believe TOR can be trusted simply because anyone can setup a node. For all anyone knows the NSA might control dozens or even hundreds of nodes.

Tor was once used by the military. There's obviously a reason they no longer use it don't you think?

Furthermore it's been know to be exploited before.

Jay? - August 4, 2014, 6:05 pm

(Aug 4, 2014 05:53 PM)Omniscient Wrote: [\[CITE\]](#) IMHO if you need TOR to hide your activity then you're likely doing something maybe you shouldn't be in which case you're not safe. You're only truly safe when you're not doing things you shouldn't be.

But to speak directly about TOR being unsafe for use because of the NSA. I don't believe TOR can be trusted simply because anyone can setup a node. For all anyone knows the NSA might control dozens or even hundreds of nodes.

You are exactly right in the sense that anyone can setup a node. However you can take certain steps in helping to prevent yourself from being exploited through a form of a honey pot node.

I agree however that true safety will only ever be obtained when you are doing something that doesn't go against any form of written law.

However, there are plenty of people who do use TOR as a means of ensuring their privacy. People who have no fear of the law, but rather a government who believes it can track, collect, and store our data without any limitations under the excuse "if you have nothing to hide then it shouldn't be a problem".

At the end of the day, if you are doing something illegal you run the risk of getting caught. People need to understand this before doing anything. It is part of being an adult and making a conscious decision. Every action has the potential to have consequences.

Using TOR is surely no different.

Machiavellian101 - August 4, 2014, 6:18 pm

If you are doing anything illegal it's only a matter of time before you get caught anyway. You can't realistically commit illegal acts online without setting digital footprints for yourself.

Jay? - August 4, 2014, 6:20 pm

(Aug 4, 2014 06:18 PM)Machiavellian101 Wrote: [\[CITE\]](#) If you are doing anything illegal it's only a matter of time before you get caught anyway. You can't realistically commit illegal acts online without setting digital footprints for yourself.

Technically speaking you could.

It is sort of like the 1% out of 99% though.

Machiavellian101 - August 4, 2014, 6:24 pm

(Aug 4, 2014 06:20 PM)Rem?rse Wrote: [\[CITE\]](#) Technically speaking you could.

It is sort of like the 1% out of 99% though.

I guess that's what many criminals thought until they got caught.

Narvikz - August 4, 2014, 6:27 pm

(Aug 4, 2014 05:53 PM)Omniscient Wrote: [\[CITE\]](#) IMHO if you need TOR to hide your activity then you're likely doing something maybe you shouldn't be in which case you're not safe. You're only truly safe when you're not doing things you shouldn't be.

But to speak directly about TOR being unsafe for use because of the NSA. I don't believe TOR can be trusted simply because anyone can setup a node. For all anyone knows the NSA might control dozens or even hundreds of nodes.

If I understand correctly the protocol everyone can set up nodes and when a user connects to TOR their data is send through all these nodes, without being possible to discover when it came from or where it is going, just the previous and next node. If I am right of course.

What if the NSA injects thousands of honeypot nodes into the network? They still wouldn't be able to realize where the packets are coming from or where they're heading but the packets should be the same at every node they pass through. Again I could be completely wrong and my thinking be complete bullshit but what happens if there's a high enough percentage of NSA nodes to track people down?

Jay? - August 4, 2014, 6:31 pm

(Aug 4, 2014 06:27 PM)ThatGuyPT Wrote: [\[CITE\]](#) If I understand correctly the protocol everyone can set up nodes and when a user connects to TOR their data is send through all these nodes, without being possible to discover when it came from or where it is going, just the previous and next node. If I am right of course.

What if the NSA injects thousands of honeypot nodes into the network? They still wouldn't be able to realize where the packets are coming from or where they're heading but the packets should be the same at every node they pass through. Again I could be completely wrong and my thinking be complete bullshit but what happens if there's a high enough percentage of NSA nodes to track people down?

You are along the correct thought process.

It would be safer to assume that the government has already begun to roll out hundreds of honeypot nodes.

However for the most part, assuming the data you are transmitting through that last node is nothing of importance you should theoretically be safe.

It would also be safe to assume that ISP's are now beginning to mark everyone who uses TOR. It is easy to detect. They still won't know exactly what you are using it for though.

Revenue - August 4, 2014, 6:36 pm

People try so hard to be anonymous and often fail. I know multiple ways to be truly anonymous. I don't have a reason to be anonymous though, so I am not.

Jay? - August 4, 2014, 6:38 pm

(Aug 4, 2014 06:36 PM)Revenue Wrote: [\[CITE\]](#) People try so hard to be anonymous and often fail. I know multiple ways to be truly anonymous. I don't have a reason to be anonymous though, so I am not.

Most people do, but for the others it is more so the fact that they get lazy and slip up.

Narvikz - August 4, 2014, 6:39 pm

(Aug 4, 2014 06:31 PM)Rem?rse Wrote: [\[CITE\]](#) You are along the correct thought process.

It would be safer to assume that the government has already begun to roll out hundreds of honeypot nodes.

However for the most part, assuming the data you are transmitting through that last node is nothing of importance you should theoretically be safe.

It would also be safe to assume that ISP's are now beginning to mark everyone who uses TOR. It is easy to detect. They still won't know exactly what you are using it for though.

Oh and having magnets just in case, even though if truecrypt's secure you're probably fine. Which means that if there's a coincidence and the first node is a honeypot, the one before the last and the last you're totally compromised. Am I right about this?

(Aug 4, 2014 06:36 PM)Revenue Wrote: [\[CITE\]](#) People try so hard to be anonymous and often fail. I know multiple ways to be truly anonymous. I don't have a reason to be anonymous though, so I am not.

Discardable Laptop, public wifi, spoofed mac address, truecrypt volume, virtual machine inside the truecrypt volume. Working through that. ?

Machiavellian101 - August 4, 2014, 6:41 pm

(Aug 4, 2014 06:20 PM)Rem?rse Wrote: [\[CITE\]](#) Technically speaking you could.

It is sort of like the 1% out of 99% though.

Also I forgot to say can you explain this. You mean a person can go online and commit illegal activities and not set tracks/traces?

crazyycast13 - August 4, 2014, 6:42 pm

This is why botnets/slaves are so nice. If you have enough of them you can privately relay through a couple of them. You know for certain that the entry node is controlled by you, and after that you should be fine.

Jay? - August 4, 2014, 6:44 pm

(Aug 4, 2014 06:41 PM)Machiavellian101 Wrote: [\[CITE\]](#) Also I forgot to say can you explain this. You mean a person can go online and commit illegal activities and not set tracks/traces?

Yes it is possible. Plausible scenarios can be crafted in your head. It isn't as hard as you think.

People just rarely do it because they have no need to. They aren't doing anything they need to be that worried about.

Radical_ed - August 4, 2014, 6:44 pm

(Aug 4, 2014 03:38 PM)Hunting Rifle Wrote: [\[CITE\]](#) This is what they want you think. They know that the stupid people will still use it, and they don't care about them. They want you to move over. They can't crack tor.

What do you say about this OP?

They can control exit nodes and therefore view and control traffic.

The NSA has the funding and the drive to do a 51% attack on the TOR network, through multiple different means.

Trundle™ - August 4, 2014, 6:44 pm

Tor users are still susceptible to a lot of things if they're a single target.

I've heard from a lot of people that there are a lot of vulns in tor, but no one really cares because they feel like they aren't being directly targeted.

Jay? - August 4, 2014, 6:44 pm

(Aug 4, 2014 06:42 PM)crazyycast13 Wrote: [\[CITE\]](#) This is why botnets/slaves are so nice. If you have enough of them you can privately relay through a couple of them. You know for certain that the entry node is controlled by you, and after that you should be fine.

Except the fact that botnets themselves act as a trail to you.

Narvikz - August 4, 2014, 6:44 pm

(Aug 4, 2014 06:42 PM)crazyycast13 Wrote: [\[CITE\]](#) This is why botnets/slaves are so nice. If you have enough of them you can privately relay through a couple of them. You know for certain that the entry node is controlled by you, and after that you should be fine.

I successfully set up a socks 5 reverse proxy server for my private one. But I need to figure how UPnP works to open the port to use it as the port has to be opened for it to work.

Astr0J3su5 - August 4, 2014, 6:44 pm

Good read! Thanks for the post, m8.

Radical_ed - August 4, 2014, 6:45 pm

(Aug 4, 2014 06:41 PM)Machiavellian101 Wrote: [\[CITE\]](#) Also I forgot to say can you explain this. You

mean a person can go online and commit illegal activities and not set tracks/traces?
Go to a public access point on a clean computer with a mac spoofer and a traffic limiter

done

Jay? - August 4, 2014, 6:45 pm

(Aug 4, 2014 06:44 PM)Radical_ed Wrote: [\[CITE\]](#) They can control exit nodes and therefore view and control traffic.

The NSA has the funding and the drive to do a 51% attack on the TOR network, through multiple different means.

The only traffic they view is that in which you allow them to see though. If you are sending any information that could possibly lead to you through that TOR exit node than you are the one at fault.

Narvikz - August 4, 2014, 6:48 pm

(Aug 4, 2014 06:44 PM)Rem?rse Wrote: [\[CITE\]](#) Except the fact that botnets themselves act as a trail to you.

That depends. Unless there's any kind of logs I don't know of in their ISPs that would find your C&C you probably could make your virus delete itself.

(Aug 4, 2014 06:45 PM)Radical_ed Wrote: [\[CITE\]](#) Go to a public access point on a clean computer with a mac spoofer and a traffic limiter

done

I said that basically. But I also added that you need to clear your history track on your PC. That being said setting up a TrueCrypt Volume with a Virtual Machine inside it and working through there will leave no history logs or anything.

Jay? - August 4, 2014, 6:49 pm

(Aug 4, 2014 06:47 PM)Radical_ed Wrote: [\[CITE\]](#) People buy shit on the black market all the time without using PGP or any other encryption methods

It's your own fault, but everyone does mess up at one point or another.

uuh, a p2p botnet that routes through TOR would be worth literally a million dollars, what are you talking about.

Indeed. Like I stated before, those who know that what they are doing is highly illegal would understand how to secure themselves in their online activities. But that level of paranoia is nearly impossible to perfect and maintain at 100%. It is inevitable that they get caught.

logging*machine - August 4, 2014, 9:14 pm

If I've read right, you can only setup Tor Exit Nodes. Meaning it'll be EXTREMELY hard to get the originating location of the user. And now Tor is taking an extra step to make sure it's insanely difficult by possibly adding more layers of nodes.

But of course, it could just be a NSA honeypot for all we know.

But like Omni said, you shouldn't expect to never get caught if you're doing illegal things online, that's why I quit doing illegal things a while back.

Jay? - August 4, 2014, 9:15 pm

(Aug 4, 2014 09:14 PM)Sunlight Wrote: [\[CITE\]](#) If I've read right, you can only setup Tor Exit Nodes. Meaning it'll be EXTREMELY hard to get the originating location of the user. And now Tor is taking an extra step to make sure it's insanely difficult by possibly adding more layers of nodes.

But of course, it could just be a NSA honeypot for all we know.

But like Omni said, you shouldn't expect to never get caught if you're doing illegal things online, that's why I quit doing illegal things a while back.

Risk reward my friend. The risk just isn't worth the possible reward. ?

Coiner - August 5, 2014, 4:07 am

Tor is not safe only when used outside hidden services.

Using Tor to browse your porn sites is definitely not safe, but this doesn't apply to hidden services.

All IP inside hidden service is 127.0.0.1 and you cannot be traced only through Javascript vulnerabilities which have been fixed for a long time. To be 100% safe, you are recommended to use NoScript.

This is the reason why Drug markets are still online and no one can do anything about them, however using Tor as a Socks5 proxy puts you at risk and is not even recommended to do so.

TheyCallMeFox - August 5, 2014, 5:45 am

I use all the recommended plugins for TOR. Does it really matter or am i not safe at all?

CrypticX - August 5, 2014, 2:51 pm

(Aug 4, 2014 04:17 PM)PARTYNEXTDOOR Wrote: [\[CITE\]](#) It's not "hackers" they're worried about.

terrorism groups, fraudsters, hitmen, drug lords, weapons traffickers.

hackers are the least of their worries

There are plenty of scams on tor like hitmen,... right?

I actually don't think you can ever find a hitman on the internet, because that would be crazy and those hitman's could easily get caught.

Jay? - August 5, 2014, 2:53 pm

(Aug 5, 2014 02:51 PM)Str8ballin Wrote: [\[CITE\]](#) There are plenty of scams on tor like hitmen,... right?

I actually don't think you can ever find a hitman on the internet, because that would be crazy and those hitman's could easily get caught.

Most of the sales on TOR are scams. Afterall there is really nothing you could do after they take your money.

Jake Miller - August 5, 2014, 3:06 pm

(Aug 5, 2014 02:51 PM)Str8ballin Wrote: [\[CITE\]](#) There are plenty of scams on tor like hitmen,... right?

I actually don't think you can ever find a hitman on the internet, because that would be crazy and those hitman's could easily get caught.

All hitmen services are fraud on Tor. What they want to hit is C&CP distributers, ML's and DW forums.

xploD - August 5, 2014, 11:22 pm

Good info, will be helpful for newcomers.

Abdilo - August 6, 2014, 12:51 am

Congradz, the nsa can own all the exit nodes for all i care(you have to own more then just an exit node to get the original ip of the user who did what you are trying to log even though sslstrip is next to impossible with tor(go look at torproject.org if you dont believe me).
if you do not leave tor aka go to google instead of an onion site, you do not go through an exit node no?

That is to my understanding.
I like tor, you always find messed up shit that you wouldn't find on the clearnet.
reward > risk in my eyes.

By the way, it would be better if you did not take snippets and just linked everyone to the sources instead of trying to scare people.

This thread is more HOLY SHIT RUN, instead of look and decide for yourself.

<https://www.eff.org/torchallenge/>

cite that as well.

the eff supports tor.

thats good enough for allot of people considering the eff are the ones who sue nsa.

Ryan Cleary - August 6, 2014, 3:19 am

And what if they're trying to scare us so we stop using TOR? :O

I don't believe what you're saying & showing us.
I've never got caught after doing illegal shit on TOR.(been a year too)

Abdilo - August 6, 2014, 3:49 am

(Aug 6, 2014 03:19 AM)PH?x Wrote: [\[CITE\]](#) And what if they're trying to scare us so we stop using TOR? :O

I don't believe what you're saying & showing us.
I've never got caught after doing illegal shit on TOR.(been a year too)
2 years for me and counting ?.
btw you make so much money on deepweb sites *evolu*, dumbass russians buy anything nowadays XD?

Jay? - August 6, 2014, 9:35 am

(Aug 6, 2014 03:19 AM)PH?x Wrote: [\[CITE\]](#) And what if they're trying to scare us so we stop using TOR? :O

I don't believe what you're saying & showing us.
I've never got caught after doing illegal shit on TOR.(been a year too)
It is a known fact that the governments are creating honeypot nodes in hopes of catching people.

It just isn't implemented in an effective manner yet to do any damage.

CrypticX - August 6, 2014, 11:01 am

Did you guys read this article:

http://thehackernews.com/2014/08/warrant-authorized-fbi-to-track-and_16.html

That scares a bit, can that be true?

Abdilo - August 6, 2014, 7:21 pm

(Aug 6, 2014 11:01 AM)Str8ballin Wrote: [\[CITE\]](#) Did you guys read this article:
http://thehackernews.com/2014/08/warrant-authorized-fbi-to-track-and_16.html

That scares a bit, can that be true?>thehackernews
yeah i personally do not trust them. why? they won't post anything that could get them in the slightest of trouble.

logging*machine - August 6, 2014, 7:48 pm

(Aug 6, 2014 11:01 AM)Str8ballin Wrote: [\[CITE\]](#) Did you guys read this article:
http://thehackernews.com/2014/08/warrant-authorized-fbi-to-track-and_16.html

That scares a bit, can that be true?

Infecting the servers the hidden service is hosted on won't do jack shit. You connect using router>router>exit node and nearly impossible to figure out where the main connection started. All the server will see is the exit node.

JaimeLannister - August 7, 2014, 12:48 pm

I think the biggest thing, and maybe I'm naive, is that you would have to be doing something pretty bad for the NSA to want to catch you on Tor. Why? I would think they would want small fish to get away (like people selling small amounts of drugs or whatever off Tor marketplaces) so that people continue to use Tor. I think the people that they would go after would be anti-government (terrorists) and they would want them to believe Tor is "unstoppable". I don't think the NSA would actually concern themselves with a lot of things that go on on Tor bc it is not their job. They gather intel on threats to national security. Sorta like the IRS if what I have heard is true, supposedly there was a madam who declared her income for what it was and even took deductions for things like lingerie. She eventually was caught and this came out, the IRS did nothing because all they wanted was their taxes, what she was doing was out of their jurisdiction. Now once she was caught it was a different story and they were able to get that information. Not even 100% sure it is a true story but my father told me it and he isn't the type that makes up stuff and was a physicist with secret clearance who worked on weapons systems (he is retired now and has been for almost 10 years, there is still a lot he isn't allowed to say but that is getting off topic, just saying he is a fairly reliable source).

Also, I have never bought anything off a Tor market but I have been curious and looked around. They do use vendor rating systems similar to Ebay and some vendors have 100s or 1000s of transactions and are "verified vendors." Unless all their feedback is self generated I would tend to believe that there are some of them that are probably pretty reliable. Now I don't even know anyone who has ordered drugs off there, but I do tend to think if someone chose a vendor with tons of positive feedback they would probably receive unless the government seizes (which I would think would be a significant risk especially if something is shipped from another country)

Omniscient - August 7, 2014, 4:17 pm

Quote:Congradz, the nsa can own all the exit nodes for all i care(you have to own more then just an exit node to get the original ip of the user who did what you are trying to log even though sslstrip is next to impossible with tor(go look at torproject.org if you dont believe me).

The rumor is that the NSA knew about the OpenSSL exploit for a long time. I know it's a conspiracy theory but I don't see why it's not possible. I'm almost positive that a bunch of mobile/tablet apps are released by the governments to track mobile use. If you look at the permissions of most apps, even simple ones, they are way beyond the scope and need of the app. Like viewing your contacts, calls, and location. Why do games need this at all I wouldn't know.

But I'm getting off-topic. My point about the NSA and the OpenSSL exploit was to say that I don't doubt that TOR is already either backdoored or exploited. If I was NSA it would be top priority to crack their service in order to track their users. It's the #1 proxy service by far and very likely used by a variety of criminals including international terrorists.

So let's say you're the FBI, CIA or NSA. What is your top priority when it comes to computer intelligence gathering? TOR is not only an easy target but it's a legal one for them because it's technically not owned by a company like Google. Who would they serve a warrant or subpoena to? They'll just exploit the services open source code and gather data.

Tor is used by browsers, IM clients, there are mobile apps too. It's the PERFECT target for gathering intel.

So for that reason alone...I wouldn't trust it for any sort of anonymity. But you do what you want. This is all just my opinion on the matter.

Jake Miller - August 7, 2014, 4:33 pm

(Aug 7, 2014 04:17 PM)Omniscient Wrote: [\[CITE\]](#) The rumor is that the NSA knew about the OpenSSL exploit for a long time. I know it's a conspiracy theory but I don't see why it's not possible. I'm almost positive that a bunch of mobile/tablet apps are released by the governments to track mobile use. If you look at the permissions of most apps, even simple ones, they are way beyond the scope and need of the app. Like viewing your contacts, calls, and location. Why do games need this at all I wouldn't know.

But I'm getting off-topic. My point about the NSA and the OpenSSL exploit was to say that I don't doubt that TOR is already either backdoored or exploited. If I was NSA it would be top priority to crack their service in order to track their users. It's the #1 proxy service by far and very likely used by a variety of criminals including international terrorists.

So let's say you're the FBI, CIA or NSA. What is your top priority when it comes to computer intelligence gathering? TOR is not only an easy target but it's a legal one for them because it's technically not owned by a company like Google. Who would they serve a warrant or subpoena to? They'll just exploit the services open source code and gather data.

Tor is used by browsers, IM clients, there are mobile apps too. It's the PERFECT target for gathering intel.

So for that reason alone...I wouldn't trust it for any sort of anonymity. But you do what you want. This is all just my opinion on the matter.

Agreed, and with the bounty Russia just put out it doesn't make it safer. I've never used Tor before and I would never do it neither; I'll keep staying whitehat so the feds will never have a reason to dropkick my door.

splunk - August 7, 2014, 4:47 pm

(Aug 7, 2014 04:17 PM)Omniscient Wrote: [\[CITE\]](#) The rumor is that the NSA knew about the OpenSSL exploit for a long time. I know it's a conspiracy theory but I don't see why it's not possible. I'm almost positive that a bunch of mobile/tablet apps are released by the governments to track mobile use. If you look at the permissions of most apps, even simple ones, they are way beyond the scope and need of the app. Like viewing your contacts, calls, and location. Why do games need this at all I wouldn't know.

But I'm getting off-topic. My point about the NSA and the OpenSSL exploit was to say that I don't doubt that TOR is already either backdoored or exploited. If I was NSA it would be top priority to crack their service in order to track their users. It's the #1 proxy service by far and very likely used by a variety of criminals including international terrorists.

So let's say you're the FBI, CIA or NSA. What is your top priority when it comes to computer intelligence gathering? TOR is not only an easy target but it's a legal one for them because it's

technically not owned by a company like Google. Who would they serve a warrant or subpoena to? They'll just exploit the services open source code and gather data.

Tor is used by browsers, IM clients, there are mobile apps too. It's the PERFECT target for gathering intel.

So for that reason alone...I wouldn't trust it for any sort of anonymity. But you do what you want. This is all just my opinion on the matter.

Yeah, that's what I was saying. It's not necessarily that it's in any way "easy" to get Tor users' information, but since there is a large number of criminals who use Tor, it makes it a prime target. Whether you are using it for bad intentions, or you aren't.

Alvin - August 7, 2014, 6:04 pm

(Aug 7, 2014 04:17 PM)Omniscient Wrote: [\[CITE\]](#) The rumor is that the NSA knew about the OpenSSL exploit for a long time. I know it's a conspiracy theory but I don't see why it's not possible. I'm almost positive that a bunch of mobile/tablet apps are released by the governments to track mobile use. If you look at the permissions of most apps, even simple ones, they are way beyond the scope and need of the app. Like viewing your contacts, calls, and location. Why do games need this at all I wouldn't know.

But I'm getting off-topic. My point about the NSA and the OpenSSL exploit was to say that I don't doubt that TOR is already either backdoored or exploited. If I was NSA it would be top priority to crack their service in order to track their users. It's the #1 proxy service by far and very likely used by a variety of criminals including international terrorists.

So let's say you're the FBI, CIA or NSA. What is your top priority when it comes to computer intelligence gathering? TOR is not only an easy target but it's a legal one for them because it's technically not owned by a company like Google. Who would they serve a warrant or subpoena to? They'll just exploit the services open source code and gather data.

Tor is used by browsers, IM clients, there are mobile apps too. It's the PERFECT target for gathering intel.

So for that reason alone...I wouldn't trust it for any sort of anonymity. But you do what you want. This is all just my opinion on the matter.
And God has spoken.

Tor can be some what beneficial though because your average user still wouldn't be able to track you. Your local authority may not be able to either...

JaimeLannister - August 7, 2014, 8:03 pm

I still think the two best questions are:

1. How hard is it to spring the trap on someone on Tor? Has Tor even made it more expensive to eavesdrop on people? If it even makes it more confusing to decipher who the person is but could be routinely done by some expert(s) at the NSA that makes a big difference over no anonimity. Obviously, the more it costs to do something the less likely you are to do it and would have to have a greater reward involved than someone who is less anonymous.

2. Really just an extension of one: what are they willing to go through the trouble of exposing that they were spying for. I feel like if they really want someone they can get them. They can find footprints left somewhere at sometime. But when would they actually push them hard enough to expose what they are doing in an open court of law and provide the evidence needed to make a conviction beyond a reasonable doubt. Now there is the thought they could grab someone under

certain laws and not necessarily give them the right to a lawyer and a speedy trial, but as much as I have heard of the slippery slope

I do not hear about common criminals being put away in such a manner. I would think the most likely targets would be targeted due to having certain radical politics and certain goals. I'm not saying that's right, I do think a trial with legal representation is part of due process and something that should be done in any case, but unless you are radically politically dissident is maybe the level of paranoia high?

And to the people talking about getting away with things, and for a while, on the darknet do you think you would really still be leaving no footprints and not being possibly caught if you were the people at the top of their list? The people they REALLY want? I am sincerely asking because I don't know the answer, when it comes to that I am sure I know way less than you. But what I am getting at is who is it that would actually get grabbed due to "spying" done by people like the NSA. Could they decide to track down EVERYONE who has done stuff wrong on Tor, especially in the marketplaces that do keep certain feedback etc., at any point? That is a good question for those people to ask themselves and I certainly don't know the answer.

Sudowoodo - August 7, 2014, 8:17 pm

If you are trying to hide your identity with some sort of proxy server, do not. Your browsers have access to your local IP.

EPIXIA???? - August 7, 2014, 8:49 pm

(Aug 7, 2014 04:33 PM)Jake Miller Wrote: [\[CITE\]](#) Agreed, and with the bounty Russia just put out it doesn't make it safer. Kind of off topic but that bounty was only \$100k. You could sell it for much more, but you still have to pay \$5k to enter the contest. ?

Gearfried - August 7, 2014, 9:17 pm

(Aug 4, 2014 03:52 PM)PARTYNEXTDOOR Wrote: [\[CITE\]](#) Of course they can't "crack" or even "stop" Tor. Your identity has potential to be leaked or intercepted while using Tor, however, and they have the technology to do this.

What if you run a virtual machine on a computer that's only used for this, on top of that you use a vpn, and browse with Tor, changing your identity every time you load a web page, whilst using a local Starbucks internet in your van in the parking lot. Does this guarantee anonymity?

EPIXIA???? - August 7, 2014, 9:20 pm

(Aug 7, 2014 09:17 PM)Gearfried Wrote: [\[CITE\]](#) What if you run a virtual machine on a computer that's only used for this, on top of that you use a vpn, and browse with Tor, changing your identity every time you load a web page, whilst using a local Starbucks internet in your van in the parking lot. Does this guarantee anonymity? How about if I use a public wifi with my \$1500 throw away laptop which I stole from a thief that stole it who burned it so it can't be tracked to me because he stole off a drug dealer then use a proxy then connect to tor and use a rdp with a proxy then use tor and connect to another rdp and use a vpn to connect to rdp then use tor and a proxy and vpn to connect into a vps that's routed through tor then layer it with a proxy and then use public wifi and connect my bulletproof HMA vpn then use tor to connect to my [censored] then install 4g on my dog so they can never track me and I can ride and layer it off with my b u l l e t p r o f hotspotshield

splunk - August 7, 2014, 9:21 pm

(Aug 7, 2014 09:20 PM)testiclesplantar Wrote: [\[CITE\]](#) How about if I use a public wifi with my \$1500 throw away laptop then use a proxy then connect to tor and use a rdp with a proxy then use tor and connect to another rdp and use a vpn to connect to rdp then use tor and a proxy and vpn to connect into a vps that's routed through tor then layer it with a proxy and then use public wifi and connect my bulletproof HMA vpn then use tor to connect to my [censored] and layer it off with my b u l l e t p r o o f hotspotshield overkill, my friend, overkill ?

MD5 - August 7, 2014, 9:36 pm

Correct me if i'm wrong, but if the NSA/FBI secretly forces tor to make all their nodes unencrypted, wouldn't they be able to trace everything? I'm not sure where those nodes are located, but if it's in america, they should be able to do that legally (with permission of the government)

(Aug 7, 2014 09:20 PM)testiclesplantar Wrote: [\[CITE\]](#) How about if I use a public wifi with my \$1500 throw away laptop which i stole from a thief that stole it who burned it so it cant be tracked to me because he stole off a drug dealer then use a proxy then connect to tor and use a rdp with a proxy then use tor and conenct to another rdp and use a vpn to connect to rdp then use tor and a proxy and vpn to connect into a vps thats routed through tor then layer it with a proxy and then use public wifi and connect my bulletproof HMA vpn then use tor to connect to my [censored] then install 4g on my dog so they can never track me and i can ride and layer it off with my b u l l e t p r o o f hotspotshield

Then, my friend, your webpages will load slow as fuck.

Don't watch porn on that

Raijin - August 7, 2014, 9:44 pm

(Aug 4, 2014 06:39 PM)ThatGuyPT Wrote: [\[CITE\]](#) Discardable Laptop, public wifi, spoofed mac address, truecrypt volume, virtual machine inside the truecrypt volume. Working through that. ? I thought that's how everyone operated??

Don't forget to connect to a hacked RDP in Russia through your VPN and Socks5 proxy.

EPIXIA???? - August 7, 2014, 10:18 pm

(Aug 7, 2014 09:21 PM)PARTYNEXTDOOR Wrote: [\[CITE\]](#) overkill, my friend, overkill ?satire, my friend, satire ?

Abdilo - August 7, 2014, 11:04 pm

(Aug 7, 2014 04:17 PM)Omniscient Wrote: [\[CITE\]](#) The rumor is that the NSA knew about the OpenSSL exploit for a long time. I know it's a conspiracy theory but I don't see why it's not possible. I'm almost positive that a bunch of mobile/tablet apps are released by the governments to track mobile use. If you look at the permissions of most apps, even simple ones, they are way beyond the scope and need of the app. Like viewing your contacts, calls, and location. Why do games need this at all I wouldn't know.

But I'm getting off-topic. My point about the NSA and the OpenSSL exploit was to say that I don't doubt that TOR is already either backdoored or exploited. If I was NSA it would be top priority to crack their service in order to track their users. It's the #1 proxy service by far and very likely used by a variety of criminals including international terrorists.

So let's say you're the FBI, CIA or NSA. What is your top priority when it comes to computer intelligence gathering? TOR is not only an easy target but it's a legal one for them because it's technically not owned by a company like Google. Who would they serve a warrant or subpoena to? They'll just exploit the services open source code and gather data.

Tor is used by browsers, IM clients, there are mobile apps too. It's the PERFECT target for gathering intel.

So for that reason alone...I wouldn't trust it for any sort of anonymity. But you do what you want. This is all just my opinion on the matter.do you know what sslstrip is??

you are kind of confusing something that changes https to http via redirects etc with heartbleed

(Aug 7, 2014 08:17 PM)Sudowoodo Wrote: [\[CITE\]](#) If you are trying to hide your identity with some sort of proxy server, do not. Your browsers have access to your local IP.....

....

....

what the fuck? like honestly what the fuck? congratz they know that i am 10.0.0.1.... but honestly what the fuck?

(Aug 7, 2014 09:17 PM)Gearfried Wrote: [\[CITE\]](#) What if you run a virtual machine on a computer that's only used for this, on top of that you use a vpn, and browse with Tor, changing your identity every time you load a web page, whilst using a local Starbucks internet in your van in the parking lot. Does this guarantee anonymity? or just idk use a live usb stick... that would work allot better then a virtual machine. plus with a persistent usb stick with a truecrypt drive on it makes it so you can litterly peg the usb and voila it is gone and no one can see what was on it.

or my favorite,
raspberry pi + micro sdcard
cops smash down the door
i swallow micro sdcard
???
proffit

Also the matter of the fact is allot of people audit tor, majority of them do it because they love to use tor, not to break it.

While we have people trying to defend tor, it will never die.

Heartbleed for example, we did not try to audit openssl properly and we were like yup works great...

The more people looking into tor the better, nsa finds an exploit yeah for them... they cannot use it on a large scale though otherwise it would get detected, thus mass infection or surveillance is sorta flawed

JaimeLannister - August 8, 2014, 8:01 am

greyhat, if I am interpreting what you are saying at the end properly I think that is one of the biggest points of this thing, when you said they can't use it on a large scale. If they suddenly rounded up everyone who did something wrong on Tor it would give away what the NSA has up their sleeve, and even if they suddenly audited the whole thing that would be noticed too. Therefore I tend to believe what they can do to track someone on Tor is probably saved for extreme cases. Or based on what was said above maybe it is almost impossible to track someone on Tor without blowing the whole thing and letting the world know? If that is the case I would think it would only be done in the EXTREMEIST of cases, like literally if they believed it would prevent another 9/11? And that might even be questionable bc there are a lot of people who say they could have prevented the first one had they given it their all or even listened to a couple people. I mean we look at the government sometimes as a well oiled, smoothly and logically operating machine it seems, but there were memos before 9/11 that had the names of hijackers supposedly and that they were learning to fly and didn't seem to care about landing. I don't know if that is true but I'm just stating that sometimes paranoia leads people to believe the government is an omnipotent force. Now don't get me wrong, I definitely wish with all my heart that 9/11 had been stopped and similar events will be stopped, and that intelligence agencies will do their job in an efficient and effective manner that is also respectful of constitutional rights, but there is a saying that "military intelligence is an oxymoron" that I have heard from reading books by soldiers and from people who have worked in related industries. I think that is a bit of an exaggeration, but the thought that are government knows EVERYTHING that goes on is not true. And I think bc of politics if they dont know every thing the things they want to learn most are those concerning national security, not someone making some transaction for a small amount of marijuana on some Tor marketplace.

To many people on here is it simply the thought the NSA/government has the technical capabilities to do something that is the scary thing? I am definitely not mocking that idea if that is what it is because the "what if's" are important, sometimes things change politically to a point where what was once unimaginable that a government would do becomes reality. And I think they probably do have technical capabilities when it comes to surveillance that most people have no idea exist, that tends to be the case in a lot of fields. Hell, a lot of things that are now in the public record still seem to be

in the dark to 99% of the population.

I really love reading what people are posting here though because there is so much info for someone new to learn and there have been great opinions on what can be done. I guess my gut feeling is what I seem to hear from most mainstream experts: they could probably find/track/spy on someone on Tor but to do so is much more difficult, therefore requires more resources, and therefore will be done less often. That is just my guess from reading here and elsewhere on the subject but I am far from an expert.

I also wanted to add in this quick edit I get it 100% if you are simply saying morally the NSA shouldn't be doing what we now know what it is doing. All I'm saying in my posts is wouldn't you probably have to be in a politically extreme position against the government to be dragged off by the CIA/NSA using the methods people are talking about here if it is possible at all?

Rofl Gun - August 8, 2014, 8:31 am

(Aug 7, 2014 04:17 PM)Omniscient Wrote: [\[CITE\]](#) The rumor is that the NSA knew about the OpenSSL exploit for a long time. I know it's a conspiracy theory but I don't see why it's not possible. I'm almost positive that a bunch of mobile/tablet apps are released by the governments to track mobile use. If you look at the permissions of most apps, even simple ones, they are way beyond the scope and need of the app. Like viewing your contacts, calls, and location. Why do games need this at all I wouldn't know.

But I'm getting off-topic. My point about the NSA and the OpenSSL exploit was to say that I don't doubt that TOR is already either backdoored or exploited. If I was NSA it would be top priority to crack their service in order to track their users. It's the #1 proxy service by far and very likely used by a variety of criminals including international terrorists.

So let's say you're the FBI, CIA or NSA. What is your top priority when it comes to computer intelligence gathering? TOR is not only an easy target but it's a legal one for them because it's technically not owned by a company like Google. Who would they serve a warrant or subpoena to? They'll just exploit the services open source code and gather data.

Tor is used by browsers, IM clients, there are mobile apps too. It's the PERFECT target for gathering intel.

So for that reason alone...I wouldn't trust it for any sort of anonymity. But you do what you want. This is all just my opinion on the matter.

Aren't all conspiracies possible by definition?

JaimeLannister - August 8, 2014, 9:44 am

(Aug 8, 2014 08:31 AM)Rofl Gun Wrote: [\[CITE\]](#) Aren't all conspiracies possible by definition? Of course, because while I know not so much about computers and anonymity at this time, it is impossible to prove a negative. You can only prove something is, not that it isn't.

Also, the big question no one ever seems to answer is: what do we do about spying and illegal intelligence gathering by the government? What is legal and what is not? Personally, I think to look at your computer the government should have to get a warrant just like any other invasion of privacy. And judges need to really look at the validity of certain claims before granting a warrant. I don't know why government officials ever bother doing something without a warrant bc when you look at the statistics judges almost always grant them.

If you ask me the real fight has to be in the legal system. Based on what was leaked by Snowden the NSA can and does keep records it probably shouldn't have. Also, I tend to doubt we can even stop intelligence agencies from gathering such information. I think the best we can hope for is

upholding constitutional rights and creating a legal system that truly does not tolerate illegal information gathering methods, puts limits on what can be done, and truly does not convict people based on information furnished illegally and gives everyone a trial with proper legal representation, and finally truly upholds the standard of beyond a reasonable doubt.

And as far as why what I am saying concerns criminal cases, that's what I guess I envision them using the information for in the end if they ever did, to arrest people. If it also came to some form of harassment of individuals who had committed no crime yet could reasonably prove (because I will be talking about civil courts here it wouldn't be beyond a reasonable doubt, but instead enough to simply sway the balance in one's favor) they were spied on their privacy was violated they should be able to file a suit against said agency.

Fjux - August 8, 2014, 1:29 pm

(Aug 7, 2014 04:17 PM)Omniscient Wrote: [\[CITE\]](#) The rumor is that the NSA knew about the OpenSSL exploit for a long time. I know it's a conspiracy theory but I don't see why it's not possible. I'm almost positive that a bunch of mobile/tablet apps are released by the governments to track mobile use. If you look at the permissions of most apps, even simple ones, they are way beyond the scope and need of the app. Like viewing your contacts, calls, and location. Why do games need this at all I wouldn't know.

But I'm getting off-topic. My point about the NSA and the OpenSSL exploit was to say that I don't doubt that TOR is already either backdoored or exploited. If I was NSA it would be top priority to crack their service in order to track their users. It's the #1 proxy service by far and very likely used by a variety of criminals including international terrorists.

So let's say you're the FBI, CIA or NSA. What is your top priority when it comes to computer intelligence gathering? TOR is not only an easy target but it's a legal one for them because it's technically not owned by a company like Google. Who would they serve a warrant or subpoena to? They'll just exploit the services open source code and gather data.

Tor is used by browsers, IM clients, there are mobile apps too. It's the PERFECT target for gathering intel.

So for that reason alone...I wouldn't trust it for any sort of anonymity. But you do what you want. This is all just my opinion on the matter.

i indeed think as well that NSA ect. are targeting tor massive.
and also because of the same reasons, as it is a good source of intelligence, and there is a higher percentage of traffic that is actually bad then on the "clearnet".

But i do not agree with the fact to simply not use it.

Tor uses multiple layers of encryption, every single node puts an extra layer on it. (i believe you can setup the minimal # of nodes).

And of course everything is crackable, but if we look at the past hacks:

1) The big SSL hack (SSL exploit went way further then the TOR network, but indeed tor was vulnerable to it. but so were a lot of servers)

2) lately a few researchers wanted to have a talk about a bug, but were called back by their university.

It is assumed that TOR found the bug (nothing concrete but clear enough.) and they solved it:
<https://blog.torproject.org/blog/tor-security-advisory-relay-early-traffic-confirmation-attack>

Still this bug was only working if they had the luck of having a few "bad" relays in the connection.

3) All other take-down's and concrete evidence of actually a successful action against some really bad things happening on the tor network (silkroad) were because of bugs in the browsers/server.

They try to hack the servers, install javascript on them to retrieve the information they want, because it is way harder to crack the tor network then cracking a webserver.

But in the end, with the power the NSA ect. have, there really is no safe way. only unplugging your internet cable and live in a bunker.

because if you go for a less know solution, and the NSA wants you. they will probably find the bugs faster in that solution as in the TOR solution.

because it is used heavier, also the bugs come to light faster.

splunk - August 10, 2014, 8:45 pm

NSA is learning way too much from deep web. It gives them cases to pursue :)

Coiner - August 11, 2014, 5:49 am

(Aug 10, 2014 08:45 PM)PARTYNEXTDOOR Wrote: [\[CITE\]](#) NSA is learning way too much from deep web. It gives them cases to pursue :)

<https://hackforums.net/showthread.php?tid=4382433>

You cant be deanonymized if you follow that thread.

?Criminal - August 11, 2014, 8:02 pm

if you want real anonymity, use a bi-quad wifi antenna, crack a bunch of WEP routers near you and if you wanna try your luck against doing a dictionary attack on WPA's be my guest. But anyways once you connect to a cracked WPA, set up a virtual machine and chain 2 vpns I recommend torguard and zorro (so basically 1 vpn on the virtual machine, 1 on the host machine) then chain a bunch of socks5's with proxifier preferably fresh ones from vip72 and spoof your mac address every day. You will be almost impossible to find, the only way law enforcement would find you is by opsec fails aka human fault which is usually posting info on your self without cleaning it up.

JaimeLannister - August 11, 2014, 9:07 pm

(Aug 11, 2014 08:02 PM)maybeBlue Wrote: [\[CITE\]](#) if you want real anonymity, use a bi-quad wifi antenna, crack a bunch of WEP routers near you and if you wanna try your luck against doing a dictionary attack on WPA's be my guest. But anyways once you connect to a cracked WPA, set up a virtual machine and chain 2 vpns I recommend torguard and zorro (so basically 1 vpn on the virtual machine, 1 on the host machine) then chain a bunch of socks5's with proxifier preferably fresh ones from vip72 and spoof your mac address every day. You will be almost impossible to find, the only way law enforcement would find you is by opsec fails aka human fault which is usually posting info on your self without cleaning it up.

Well, depending on what someone is doing I feel like there is the chance of them being caught by means other than directly tracing them back to their computer (this is why I wouldn't just go and committ crimes even if I had a very high level of privacy, aside from the ethical reasons of "who am I hurting, etc" (when it comes to the drug war I tend to feel like sane adults have a right to do what they want so long as they aren't directly (or intentionally or massively indirectly) hurting someone, and therefore ethically I wouldn't have an ethical issue with someone selling and/or buying drugs over Tor so long as they keep their word/end of the bargain and send what they are supposed to; but I feel like eventually you get caught and with mandatory minimums, etc. drug charges are not usually "mickey mouse" charges) when it comes to some types of fraud (where an innocent

individual gets screwed, I know they can usually eventually straighten things out but it can take a long time and cripple them financially for a while; when it comes to some of the big banks etc. that took bailouts then gave their CEO a 10 million dollar bonus I might feel a little different if someone went after them directly; but that would probably be much harder and have a much higher risk of getting caught and punishment).

For example, people that use stolen cc numbers or hack bank accounts: lets say there is no way they could trace back to the actual computer. If they carded somewhere they could use a sting possibly and catch them in person (x site checks to see if a transaction is valid and the real owner says it is not or maybe they aren't even sure but they decide to check it out) if they are buying goods and using a drop they could just wait and watch to see who picks it up (even if it is not the person who directly did it they could lean on that person and find out who they are bringing it to; honestly 90% of people, unless maybe they are hardened criminals (and even then you might be surprised), will spill and tell everything they know if it means not going to jail or maybe even just not getting probation. If they sent it to an account I feel like maybe they could follow the money (maybe they somehow secretly attach something somewhere etc.) and eventually find the person. If they are selling drugs they are probably sending with an envelope with a fake name and dropping it in a public mailbox somewhere, but if they are making a bunch of sales I doubt they drive 100 miles to do so; therefore they at least have a general area pinned down. Then there is someone who is receiving, and honestly many of these people are not going to be internet security experts, if they could even see info on where it is going they could bust them (that is aside from them catching random packages). Or an LEO could order if that somehow helps them trace back. Also, who knows, if someone ever does anything with anyone else physically around could they be looking over their shoulder? Did they ever tell ANYONE what they did/do?

I could go on and on, but what I am saying is there seems to ALWAYS be some chance of getting caught even if just by shit luck. When I was younger I was arrested and convicted of a couple minor crimes (none of which had to do with computers; a simple assault on an LEO and some personal possession charges, nothing major but I did have to serve a 1-3; doesn't sound like a huge sentence but 15 or 16 months before being paroled can seem like quite a long time when you are sitting in the state penitentiary) I thought I would never be caught because I was simply a user and came from a good family, had a nice car with all the proper registration and insurance etc, and drove in a very legal manner.

But I learned the only 100% way not to get caught was to stop doing illegal things (and admittedly that is not a truly 100% way not to get arrested, just look at all the people that have been on death row and later cleared by DNA etc; as sucky as it is you also have to be a "normal" person in your appearance, mannerisms, political opinions etc. to reduce your risks further). Hell, even if you got away with all the crimes you committed what about the money made? If you live above your means the IRS etc. could get involved and get you for tax evasion, and if you set up a fake business or even put money through a real business that was made illegally that is a risk too. Unless you are going to be Robin Hood and just give that money away to the poor anonymously that is always a risk; what good is money you can't spend?

My biggest concerns are that I feel I have a right to say what I want (I am non-violent in my beliefs, unless it is self-defense, but I would probably be considered in the top 5% for how extreme I am in my political beliefs (where I fall on the 4 directional spectrum (it is not just left right like most people think of)) and I have family members that are probably in the top 1% when it comes to how extreme they are, but they are non-violent and are not trying to overthrow the government and therefore have a right to their beliefs as well (I would call myself a democratic socialist, like Bernie Sanders, and I am the conservative of my immediate family; some of them would say they are anarcho-communists who believe in a true "to each according to their needs, from each according to their abilities" and a very high level of voting, like most specific laws being voted on by the populace instead of simply electing representatives in most cases. I know our government and big corporations do not like

those types of beliefs. And I don't think I can ever be 100% untraceable either but at least I could make harder to be watched. Also, I feel political beliefs are the number 1 reason they would watch people.

I've already gone on too much for most people to read this whole post, but based even on the limited knowledge I have of computers I just in general feel like nothing is 100% safe; that just seems to be the way EVERYTHING is in life.

chrisman0091 - August 11, 2014, 9:36 pm

I do agree that Tor has it's flaws and yes it is possible to be tracked still, depends on the nodes you hit really. As said earlier(page 2/3?) even if the exit node is government as long as you don't have any personal information coming out of it you should be fine(if I'm thinking right), and then even if you do, that's where PGP and such comes into play.

But when it comes down to the average person wanting to use a .onion website, what better alternative can they use to stay anonymous?

Abdilo - August 11, 2014, 11:38 pm

(Aug 11, 2014 09:36 PM)chrisman0091 Wrote: [\[CITE\]](#) I do agree that Tor has it's flaws and yes it is possible to be tracked still, depends on the nodes you hit really. As said earlier(page 2/3?) even if the exit node is government as long as you don't have any personal information coming out of it you should be fine(if I'm thinking right), and then even if you do, that's where PGP and such comes into play.

But when it comes down to the average person wanting to use a .onion website, what better alternative can they use to stay anonymous?you need tor to access .onion domains lol or tor2web

splunk - August 11, 2014, 11:40 pm

I think of it as a whorehouse. You can go in a whorehouse, and people know you went into the house, but nobody can prove you bought a prostitute.

They can see your entry point, but not exactly the content.

Abdilo - August 11, 2014, 11:53 pm

(Aug 11, 2014 11:40 PM)PARTYNEXTDOOR Wrote: [\[CITE\]](#) I think of it as a whorehouse. You can go in a whorehouse, and people know you went into the house, but nobody can prove you bought a prostitute.

They can see your entry point, but not exactly the content.Best quote ever:

There is a cat in a box.

as long as you dont open it, the cat is both dead and alive.

when you open it, it is dead.

chrisman0091 - August 12, 2014, 6:49 am

(Aug 11, 2014 11:38 PM)Grey Hat Mafias Bitch Wrote: [\[CITE\]](#) you need tor to access .onion domains lol or tor2web

That was my point haha, there's no real alternative when you want to use that sort of stuff.

Master Antrax - August 13, 2014, 5:42 pm

if you use it right then its fine. It puts you behind a proxy, they cant tell if you use it or not.

Osiris1717 - November 18, 2014, 10:54 pm

They host exit node's to try and capture you also.

-Elusive- - November 19, 2014, 9:46 am

You people actually disgust me. I am genuinely sick

HIGH PAID FELLA - November 19, 2014, 9:54 am

You can use your botnet as relay, just use many in like country's where they don't care about online crime.

SyntaxTheGod - November 19, 2014, 12:39 pm

Im sorry to do this but i have to correct something here, 90% of the world's internet connections do not flow threw the us.

IceColdVirus - November 20, 2014, 12:36 pm

tor is monitored by the NSA each and everyday but they don't target hackers for the most part

ÇdnîS Lu?i? - November 20, 2014, 6:00 pm

We live in a world which revolves around Duality. Information/disinformation is at your hands on all levels. It is truly your knowledge and experience that allows you to base and form your own opinion intellectually. Who funds Tor?

Quote:Tor: Sponsors

The Tor Project's diversity of users means we have a diversity of funding sources too — and we're eager to diversify even further!

Thank you to all the people and groups who have made Tor possible so far, and thank you especially to the individual volunteers who have made non-financial contributions: coding, testing, documenting, educating, researching, and running the relays that make up the Tor network.

Active Sponsors in 2014:

SRI International (2011-2014)

US Department of State Bureau of Democracy, Human Rights, and Labor (2013-2015)

National Science Foundation joint with Georgia Tech and Princeton University (2012-2016)

Radio Free Asia (2012-2014)

An anonymous North American ISP (2009-present)

The Ford Foundation (2013-2014)

Google Summer of Code (2007-present)

More than 4,300 personal donations from individuals like you (2006-present)

[Source](#)

If it is too good to be true, then it is most likely a sham.

DeplorSocio - November 20, 2014, 6:03 pm

Not to mention the fact that the US government donates a couple million every year to TOR.

wewlad - December 24, 2014, 3:23 pm

Anybody who thinks TOR is compromised is truly an idiot who doesn't read. Any of you who say "but muh end-to-end attacks" don't realize the likelihood of one happening. The NSA would have to have tor end nodes and relays up the ass to perform an end-to-end attack. The only people who get caught while using tor are caught from user error like using javascript or using a screenname they use on a clearnet website.

stackoverflowin - December 24, 2014, 5:55 pm

In a sense of things that's actually a smart move from the NSA, driving people to use TOR automatically puts a red flag on their head.

Interesting.

crazyycast13 - December 24, 2014, 9:38 pm

Oh boy this thread is still up?

(Dec 24, 2014 06:55 PM)StackOverlowin Wrote: [\[CITE\]](#) In a sense of things that's actually a smart move from the NSA, driving people to use TOR automatically puts a red flag on their head.

Interesting.

It's a very smart move, which is why just using TOR will get you caught sooner or later.

This thread has an amazing amount of tactics to gain anonymity, so if you are interested in keeping yourself hidden, read through this thread and search anything you don't know.

Better yet, just ask how to implement it. I'd rather answer a question about that than someone saying "hey man how do you crypt".

Bucked - December 25, 2014, 4:03 am

Tor is still safe, but not 100% anonymous

Yamakasinge - December 25, 2014, 4:05 am

I was actually trusting TOR Thank you man

w34k - December 25, 2014, 2:21 pm

<http://thestack.com/chakravarty-tor-traffic-analysis-141114>

Betty Blue - December 26, 2014, 9:50 pm

(Dec 24, 2014 04:23 PM)Ziplt Wrote: [\[CITE\]](#) Anybody who thinks TOR is compromised is truly an idiot who doesn't read. Any of you who say "but muh end-to-end attacks" don't realize the likelihood of one happening. The NSA would have to have tor end nodes and relays up the ass to perform an end-to-end attack. The only people who get caught while using tor are caught from user error like using javascript or using a screenname they use on a clearnet website.

<http://thestack.com/chakravarty-tor-traffic-analysis-141114>

Take a read.

EDIT: Didn't even see you posted the link above w34k.

JaimeLannister - December 26, 2014, 11:06 pm

I actually had the contents of my BTC wallet stolen, most likely through a compromised Tor node during the blockchain security update, just recently (I just actually made a post about it a couple hours ago to learn more about what that means- but at the very least it says SOMETHING about Tor (even if it was blockchain's fault due to their security update that would show some of your info can be leaked out to compromised nodes in some circumstances)).

Honestly, I wouldn't put financial info and would probably connect to Tor through a VPS now for a further layer of protection- or simply use other anonymity methods (like VPN or VPS to a socks 5 server) at this point

Intugro - December 26, 2014, 11:33 pm

Everybody thought the Tor hitman page was legit, turns out it was an trap by the FBI. Anyone who tried to purchase it was caught, including the owner of The Silk Road, he attempted to buy an assassination from there and got fucked up. lol

B4tman - December 27, 2014, 1:22 am

This was a good insight, and makes perfect sense.

bren1337 - December 27, 2014, 2:11 am

Shouldn't be doing illegal things, anyways. I only use tor so idiots can't DDoS me.

JaimeLannister - December 27, 2014, 2:29 am

(Dec 27, 2014 12:33 AM)Intugro Wrote: [\[CITE\]](#) Everybody thought the Tor hitman page was legit, turns out it was an trap by the FBI. Anyone who tried to purchase it was caught, including the owner of The Silk Road, he attempted to buy an assassination from there and got fucked up. lol

Anyone who thinks one could actually buy a hitman on Tor is pretty foolish. Not saying you couldn't run into some idiot that wants to be one, but when you look at it rationally it would be very unlikely a real hitman would ever sell their services in such a manner- I won't really get further into (like specifics) but just think about it....

B?ue - December 27, 2014, 2:33 am

Everyone's yelling left right and center about how TOR is compromised and shit,
Can someone please explain how should someone wanting to use TOR maintain anonymity?

Takaii - December 27, 2014, 6:39 pm

Its a lot of great information post on this post ?

crazyycast13 - December 28, 2014, 7:36 am

(Dec 27, 2014 03:33 AM)BlueLights Wrote: [\[CITE\]](#) Everyone's yelling left right and center about how TOR is compromised and shit,

Can someone please explain how should someone wanting to use TOR maintain anonymity?
Don't use it from your house, or anywhere near your house.

As nakamoto said, try to remain at least 30+ miles from your house when using tor for questionable activities. Connect either through free WiFi or wardriving.

You can't just rely on one thing, that's what it comes down to.

detaerC - May 20, 2015, 9:44 am

(Aug 4, 2014 05:53 PM)Omniscient Wrote: [\[CITE\]](#) IMHO if you need TOR to hide your activity then you're likely doing something maybe you shouldn't be in which case you're not safe. You're only truly safe when you're not doing things you shouldn't be.

But to speak directly about TOR being unsafe for use because of the NSA. I don't believe TOR can be trusted simply because anyone can setup a node. For all anyone knows the NSA might control dozens or even hundreds of nodes.

You're such a fatty, theres always a way to be safe.

-NBA - May 20, 2015, 1:41 pm

I get nervous just thinking about Tor. If you're gonna do something that bad then just do it in person.

NoScript - May 20, 2015, 5:51 pm

(Aug 4, 2014 05:53 PM)Omniscient Wrote: [\[CITE\]](#) IMHO if you need TOR to hide your activity then you're likely doing something maybe you shouldn't be in which case you're not safe. You're only truly safe when you're not doing things you shouldn't be.

But to speak directly about TOR being unsafe for use because of the NSA. I don't believe TOR can be trusted simply because anyone can setup a node. For all anyone knows the NSA might control

dozens or even hundreds of nodes.

Or.. Just maybe.. We could be using Tor to protect our anonymity and fight back against the government?

And anyway as Omniscient has said, they possibly control thousands of Nodes which they can be owned by anyone so more or less the service itself is internally flawed.