

Forum:[Hack Forums](#)

Thread: [Do you use tor alone? or do you take extra security measures with tor?](#)

B E A S T - December 14, 2018, 11:40 pm

If you were to connect to a botnet would you use tor alone? if not what else do you use with tor to maximize anonymity?

SysAdmin - December 15, 2018, 6:37 am

Anything can be compromised, even Tor. Never use a single point of connection, always use a redundant connection to cover your Operational Security. Use a VPN, purchase it on a fake name with cryptocurrency, then buy a VPS, connect to the VPS and use another VPN on there.

I've read a while ago that a team of hackers used encrypted Virtual Machines as a Command & Control server, so they essentially connected to the C&C server from a VPN and fortified their OpSec with a highly encrypted Virtual Machine.

sh4moon - December 15, 2018, 8:38 am

(Dec 15, 2018 12:40 AM)hammered Wrote: [\[CITE\]](#) If you were to connect to a botnet would you use tor alone? if not what else do you use with tor to maximize anonymity?

I wouldn't. it makes a single point of failure, like sys said. use some proxies that aren't based in your home country. several of them preferably.

(Dec 15, 2018 07:37 AM)SysAdmin Wrote: [\[CITE\]](#) Anything can be compromised, even Tor. Never use a single point of connection, always use a redundant connection to cover your Operational Security. Use a VPN, purchase it on a fake name with cryptocurrency, then buy a VPS, connect to the VPS and use another VPN on there.

I've read a while ago that a team of hackers used encrypted Virtual Machines as a Command & Control server, so they essentially connected to the C&C server from a VPN and fortified their OpSec with a highly encrypted Virtual Machine.

do you have a link to that article or whatever it was? I want to read about that.

SysAdmin - December 15, 2018, 10:27 am

(Dec 15, 2018 09:38 AM)sh4moon Wrote: [\[CITE\]](#) I wouldn't. it makes a single point of failure, like sys said. use some proxies that aren't based in your home country. several of them preferably.

do you have a link to that article or whatever it was? I want to read about that.

I'll try and find it, cause it has been about a year. If I find it, I'll post the link.

SandboxEscaper - December 16, 2018, 7:03 pm

I wouldn't trust TOR at all.. and you really need to know what you're doing. If you make ONE mistake, they will catch you. Like others said.. it's best to use it as an extra layer.

To quote HackBack DIY guide..

"

3) (Optional) Don't connect directly to Tor

Tor isn't a panacea. They can correlate the times you're connected to Tor with the times your hacker handle is active. Also, there have been successful attacks against Tor [8]. You can connect to Tor using other peoples' wifi. Wifislax [9] is a linux distro with a lot of tools for cracking wifi. Another option is to connect to a VPN or a bridge node [10] before Tor, but that's less secure because they can still correlate the hacker's activity with your house's internet activity (this was used as evidence against Jeremy Hammond [11]).

The reality is that while Tor isn't perfect, it works quite well. When I was young and reckless, I did plenty of stuff without any protection (I'm referring to hacking) apart from Tor, that the police tried their hardest to investigate, and I've never had any problems.

..

BEAST - December 16, 2018, 7:07 pm

(Dec 16, 2018 08:03 PM)SandboxEscaper Wrote: [\[CITE\]](#) I wouldn't trust TOR at all.. and you really need to know what you're doing. If you make ONE mistake, they will catch you. Like others said.. it's best to use it as an extra layer.

To quote HackBack DIY guide..

..

3) (Optional) Don't connect directly to Tor

Tor isn't a panacea. They can correlate the times you're connected to Tor with the times your hacker handle is active. Also, there have been successful attacks against Tor [8]. You can connect to Tor using other peoples' wifi. Wifislax [9] is a linux distro with a lot of tools for cracking wifi. Another option is to connect to a VPN or a bridge node [10] before Tor, but that's less secure because they can still correlate the hacker's activity with your house's internet activity (this was used as evidence against Jeremy Hammond [11]).

The reality is that while Tor isn't perfect, it works quite well. When I was young and reckless, I did plenty of stuff without any protection (I'm referring to hacking) apart from Tor, that the police tried their hardest to investigate, and I've never had any problems.

..

Yep, tor alone isn't good at all.

indianboy - December 17, 2018, 5:23 am

(Dec 15, 2018 12:40 AM)hammered Wrote: [\[CITE\]](#) If you were to connect to a botnet would you use tor alone? if not what else do you use with tor to maximize anonymity?

Dear brother...

Don't use tor directly. Tor usage can be caught by your isp. it is also possible that your isp is tracking your tor usage. Always use socks, vpn, vps, vm, and also use vpn, vps and socks inside vm as sys and shamoon said.it will increase your anonimity perfectly.

Thanks for the wonderful question...)

osiris.sh - December 17, 2018, 7:00 am

i use it alone, no extra security

