the grugq Follow

Information Security Researcher :: PGP 0xDB60C7B9BD531054 :: https://www.patreon.com/grugq

Dec 19, 2016 · 5 min read

Tor and its Discontents

Problems with Tor usage as panacea

This post deals with problems related to Tor usage that are not technical. I try to look at the human side of things, and I'm quite concerned by the meme of Tor as "panacea solution to arbitrary infosec problems." I don't particularly want to fight the privacy activist cult that has developed around Tor, but I feel compelled to state my concerns. (Also, I got triggered by Dan Guido who is writing on the same topic.)

Counterintelligence and security professionals will tell you that you need to adhere to disciplined rules of operation to maintain a strong security posture. That you need to develop a threat model, figure out what you're trying to protect, and then develop and execute a plan that will provide that protection. This sequence has even been codified in the five step OPSEC process. It is self evident if you think about security (and/or privacy) that you have to follow this sequence.

The "tools first" brigade love to advance "use *${this}*" as if whatever *${this}* is will implement all sequences of the process for you. Then any tool which fails to address a real threat, or provide the appropriate protection, can be blamed for not addressing arbitrary threat models. This entire approach is backwards.

Fallacy: Tor protects people in oppressive regimes

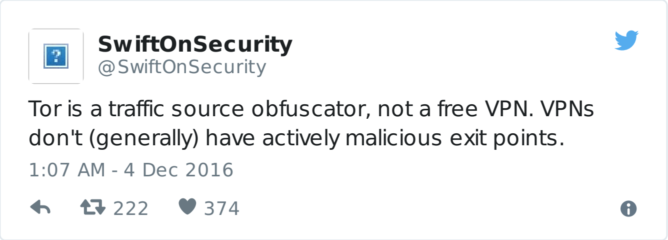
It doesn't work well for them. In almost all cases a good VPN is safer (e.g. won't cooperate with Vietnamese legal authorities); and provides the same protections:

- geographic shifting
- IP masking, and
- "on the wire" data encryption

In addition, most really repressive places actually look for Tor and target those ppl. VPNs are used to watch Netflix and Hulu, but Tor has only one use case – to evade the authorities. There is no cover. (This is assuming it is being used to evade even in a country incapable of breaking Tor anonymity.)

In many ways Tor can be riskier than a VPN:

1. VPNs are (typically) not actively malicious
2. VPNs provide good cover that Tor simply cannot – "I was using it to watch Hulu videos" is much better than – "I was just trying to buy illegal drugs online"



SwiftOnSecurity
@SwiftOnSecurity

Tor is a traffic source obfuscator, not a free VPN. VPNs don't (generally) have actively malicious exit points.

1:07 AM - 4 Dec 2016

222 374

As someone who works with ppl that do actual investigative journalism (among other at risk groups) and need to protect themselves, basically the only thing Tor has going for it is that it is free and essentially frictionless to setup and use. These ppl tend not to be extremely technical, so “download and run this free tool and you’re magically safe” resonates well with them.

“*Download and run this and you get a free proxy / VPN; oh, yeah, but you’ll stand out like a fucking glow stick and you have no good reason to use it except as an evasion tool against state authorities. Good luck explaining that when they ask uncomfortable questions.*”

Tor is not a new problem for states, they have been working on solutions for years, that includes injecting malicious nodes. We’ve seen this numerous times. It is a reasonable conjecture to assume a significant percentage of Tor nodes are controlled by Mallory.

Tor Browser Bundle is high risk

> *[Tor Browser Bundle] collapses state-level targeting of browsers to a small set of Firefox versions; TBB is the most risky browser you can possibly run*
>
> *— Thomas Ptacek (paraphrasing Bruce Leidl)*

Tor Browser Bundle is the worst browser possible. This is truth. To follow the reasoning why, there are a few main key issues:

- Monoculture
- Firefox lacks critical security features
- Firefox “Rapid Release” schedule

Anonymity Needs Homogeny—Security Doesn’t

Anonymity is essentially a property of a system that ensures any user is equally likely to be the source of an event (communication, transaction, whatever.) This is one of the reasons that Tor Browser Bundle is pushed so heavily—it creates a large pool of homogeneous users. That is good for anonymity.

Homogeneous users is bad for security because it creates a monoculture, which means the same bugs are present across the entire population. That is generally considered bad in security (although not as a first principle, just as a good rule of thumb.)

Security through diversity is a thing. It provides natural segmentation – smaller clusters of populations have vulnerable traits that are not widely shared by everyone. Diversity is thus a desirable state for security (sometimes.) Diversity is obviously less good for anonymity because the larger the pool of homogeneous users the safer everyone is (risk is distributed across the group and becomes diffuse.) The more potential people that could be suspects, the harder it is to figure out who is actually responsible. That's the theory anyway…

How Tor Browser Bundle achieves this homogeny is by using a modified version of the Firefox "extended support release" browser. Now, why that is not ideal.

How the Sausage is Made

Mozilla, the company that makes Firefox, formalized a release schedule for handling their development. It is based on fixed windows (6 weeks) where builds cascade down a series of different channels (Nightly, Aurora, etc.), each time with more bug fixes and stability. This is transparent and a perfectly acceptable way to manage a software project (Chrome has a similar series of channels, although they move much faster and not on a fixed schedule.)

1. Mozilla releases **Nightly** builds every day (basically)
2. **Aurora** builds are released every 6 weeks
3. **Beta** builds are bug fix releases of **Aurora**, every 6 weeks
4. **Release** builds are final bug fix releases of **Beta**, every 6 weeks
5. **Extended Support Release** builds are **Release** builds with all the *Critical* and *High* security bugs patched, about every 6 weeks.

TBB is a modification of Firefox's **Extended Support Release** (ESR) build.

Some say Window of Vulnerability, some say Window of Opportunity

The conclusion is obvious—Tor Browser Bundle is based on a code base that may have publicly patched *Critical* or *High* bugs that are months old. And all the *Medium* and *Low* bugs are simply never patched (forever days, as they're sometimes called.)

An adversary can do any number of things to attack the TBB, for example:

1. Monitor for *Critical* / *High* patched vulnerabilities in the less stable channels (Nightly, Aurora, Beta) and then check whether the vulnerability exists and is exploitable in TBB. They have a window of exposure that might last weeks or months.
2. Chain a series of *Medium* / *Low* vulnerabilities together until they get the level of access they require, e.g. remote code execution. They have a permanent window of exposure.
3. Find an unknown and unpatched vulnerability in Firefox (or the dozens of libraries it uses) that is exploitable in Tor

> Browser Bundle. The window of exposure might be years or merely days.

What the Tor Browser Bundle does is essentially focus all of the vulnerability research on a single slow moving, poorly defended target. The monoculture that provides protective anonymity – hiding in the herd – exposes the herd to the same vulnerabilities. And everyone is looking for those vulnerabilities.

> *[Tor Browser Bundle] is the only reason that FireFox is a valuable target— [redacted]*

If the only thing between you and your negative outcome is a bug in Tor Browser Bundle, prepare to see your negative outcome.

Concluding Remarks

Firefox is one of the weakest browsers in terms of anti exploitation mitigations, making it less safe to use than alternatives. Tor Browser Bundle is at the tail end of the pipeline of patching (of which it receives only a minimal patch set), making it a risky choice to defeat state level adversaries.

Threat models that include a Global Passive Adversary, or a capable nation state level adversary, or an adversary that doesn’t require an IP address to conduct an investigation, are not well protected by Tor.