Fact Sheet: Cloud Flare and the Tor Project

What is the Tor Project?

The Tor Project (TorProject.org) is a non-profit organization that develops and distributes free software to help millions of people defend against online surveillance that threatens personal freedom and privacy. Tor's web browser and other privacy tools are used by human rights defenders, diplomats, government officials, and everyday people who value freedom from surveillance. The Tor browser also allows users to reach the free Internet in countries where the government restricts this access.

What is CloudFlare?

CloudFlare is a company that helps protect web sites from spam and other unwanted web traffic. However, as part of its services, it flags traffic from Tor users and sends CAPTCHAs to Tor users trying to reach its sites (for instance, Australia's office of Amnesty International http://www.amnesty.org.au/)–often multiple sets of CAPTCHAs *per website*—or an endless loop of them.

CloudFlare's Impact on Users

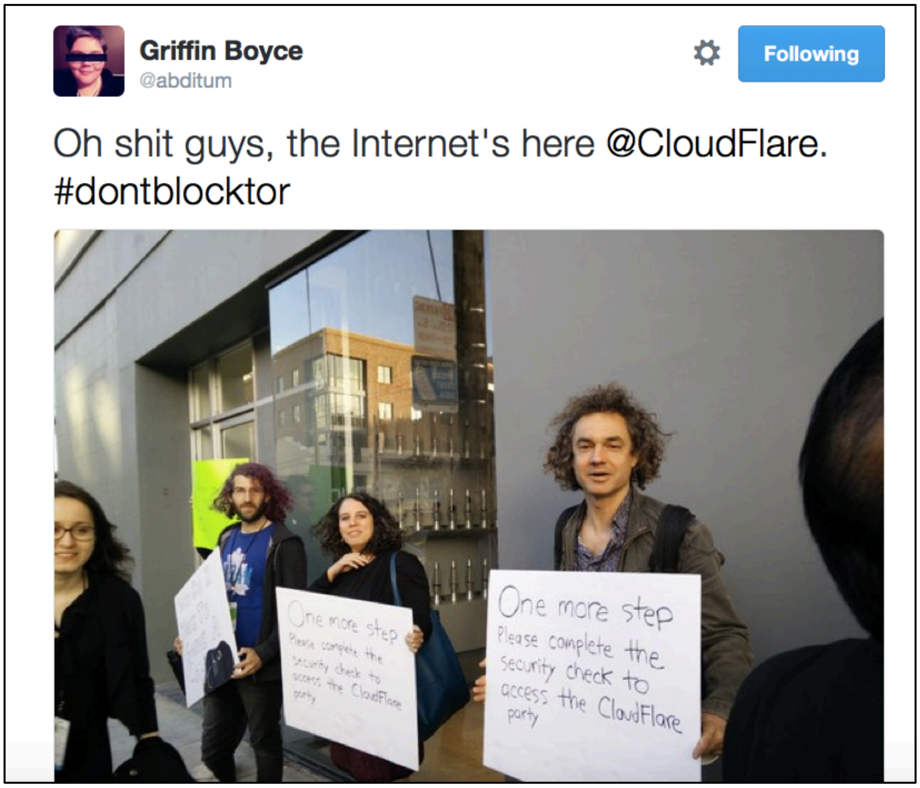
The goal of Tor is to provide secure access to the Internet, but CloudFlare prevents Tor users from reaching important websites. It blocks some web sites completely, while in other cases it presents users with a long series of slowly loading CAPTCHAs so that the user eventually gives up. When this happens, a user may be tempted to use an unsafe browser that reveals their location or other identifying information–encouraging them to take a serious risk if they are, for instance, human rights activists or domestic violence survivors. For these groups and others, Tor provides life-saving anonymity and masks their location.

Since CloudFlare makes so many websites inaccessible to Tor users, new users tend to blame themselves and believe that they are using Tor software improperly. They may then abandon using Tor altogether.

CloudFlare's impact is especially severe when Tor is being used in developing countries in which Internet speeds are slow and users pay by the minute. One at-risk human rights advocate from an East African country explains:

> *"You think the government is interfering or someone is playing around with it. You can't keep doing CAPTCHAs and they aren't working--you think something is broken here.*
>
> *Doing one CAPTCHA is enough to identify if I'm human or not. [With repeated CAPTCHAs] I will run away from Tor. I won't use it. If CloudFlare really cares for security, then they should let people use Tor. Treat Tor like any other browser traffic."*

There is a widespread backlash against CloudFlare and frequent flare-ups on social media:



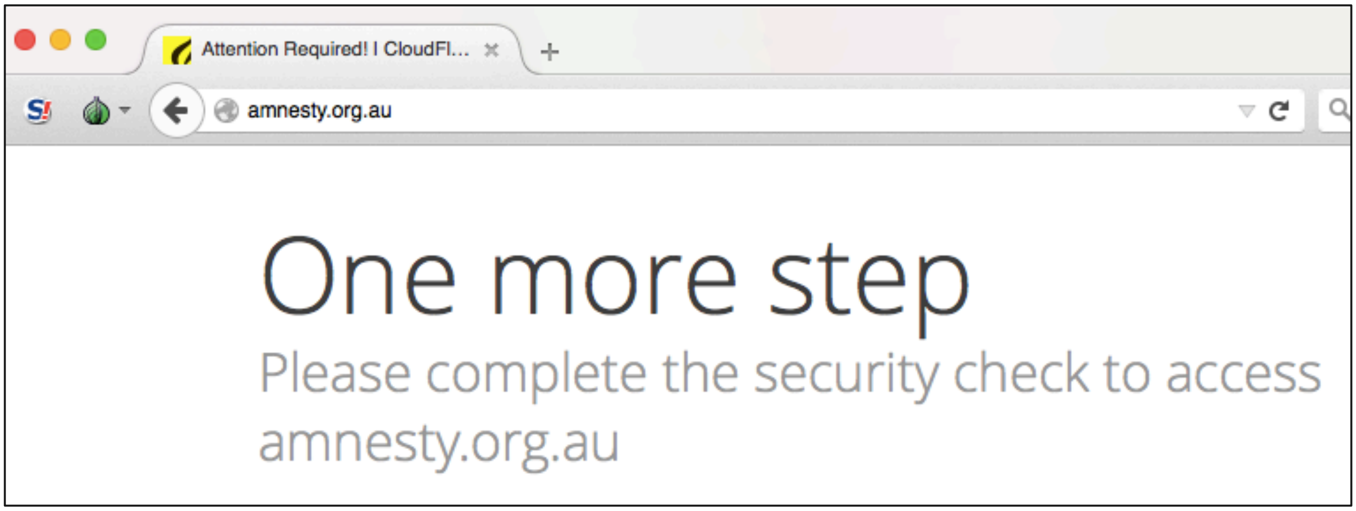
Griffin Boyce
@abditum

Oh shit guys, the Internet's here @CloudFlare. #dontblocktor

Following
One more step
Please complete the security check to access the CloudFlare party
One more step
Please complete the security check to access the CloudFlare party

CloudFlare's CAPTCHA system results in de facto censorship, since Tor users either cannot access a site or are deterred from using a site because of the obstacles presented by the CAPTCHAs. Tor users have complained that they can circumvent China's Great Fire Wall, but not CloudFlare. A 2015 report by UN Special Rapporteur David Kaye affirmed that Tor is an essential tool for freedom of expression online.

Security researchers described the problem in a recent paper: "A different kind of threat...involves websites providing Tor users with degraded service, resulting in them effectively being relegated to the role of second-class citizens on the Internet."[1]



Attention Required! | CloudFl...

amnesty.org.au

One more step

Please complete the security check to access amnesty.org.au

The Scale of the Problem

CloudFlare blocks Tor, and many other users, from accessing critical websites and seriously impedes access to websites for millions of others, including those for whom access to Tor is essential for their physical safety. Many Tor users are forced to deal with dozens of CAPTCHAs every day, and The Tor Project receives unsolicited complaints about the problem on a daily basis. CloudFlare has been aware of the problem since at least 2013.

Best Practices for Companies that Want to Support Tor User Access to their Websites (List Developing)

- Switch to a Content Delivery Provider that supports Tor users.
- Whitelist access over Tor: https://support.cloudflare.com/hc/en-us/articles/203306930

Mislabeling Tor Traffic

When a connection to a website travels over Tor, it will exit the network via one of the thousand exit relays set up by volunteers all over the world. The largest exit nodes transport more than 70,000 connections at a given moment. If a small number of these connections contains what CloudFlare qualifies as "malicious traffic" (spam, typically), CloudFlare will consider any subsequent connection as "malicious."

Because exit relays are picked (usually at random) by the Tor client, a single bad guy could have all relays qualified as transporting "malicious traffic."

While many Tor relays appear as "malicious" from CloudFlare's point of view, the abuse is likely coming from a tiny fraction of the millions of daily Tor users.

Impact on Tor Mobile (Orfox)

The same issue that Tor Browser users have had with CloudFlare CAPTCHAs is present on mobile devices as well.

In many developing countries, the overwhelming majority of users access the Internet via Android mobile phones. We have increasingly heard from users of Orfox, the Android version of Tor Browser, that while they find browsing the web through Tor mostly a great experience, the growing number of sites they cannot access due to CloudFlare is a deal breaker for them. They also largely blame the Orfox developers for not being able to solve the CAPTCHAs as a "bug that should be fixed."

Orfox has had nearly one million installs through Google Play since it launched in the Fall of 2015. There are over 10 million installations of Orbot, Tor for Android, which can be used with Orfox, or with any app through the proxy and VPN features. This includes Facebook for Android, which directly supports Orbot through a "use with Tor" option.

Monetization of Tor Users Versus non-Tor Users

A recent survey by CloudFlare competitor Akamai found that Tor users buy as much online as non-Tor users https://www.stateoftheinternet.com/resources-cloud-security-2015-q2-web-security-report.html

CloudFlare + Tor Discussions

CloudFlare has been aware of this problem for at least 3 years and Tor Project developers have engaged online and in person with CloudFlare developers for at least 18 months, but the problem of blocking Tor users has not been resolved and our users continue to suffer.

Examples of Affected Websites:

amnesty.org.au
arabnews.com
avaaz.org
dailymail.co.uk
plannedparenthood.org
stackexchange.com
medium.com

Notes on CloudFlare's Blocking by IP Address
(Fact: One IP Address Does Not Equal One User)

Any country, ISP, or region that has a limited number of public IPv4 addresses suffers from similar issues to Tor exit nodes.

Unwanted traffic going through a single IP address can potentially block thousands or even millions of users from using CloudFlare sites.

The underlying issue is CloudFlare's design assumption that an IP address represents a single user. *Yet there may be millions of users behind a handful of IP addresses.*

CloudFlare's design discriminates against:

- Regions with high populations and low IPv4 address allocations.
- Poorer users, because recent, more secure versions of many operating systems won't run on old hardware.
- Less technically savvy users, who might not know how to secure their computers or run a virus scan (or solve a CAPTCHA–the required action can be difficult to decipher).
- Users who are visually or physically impaired.

This discrimination might be unintentional, but it is very real.

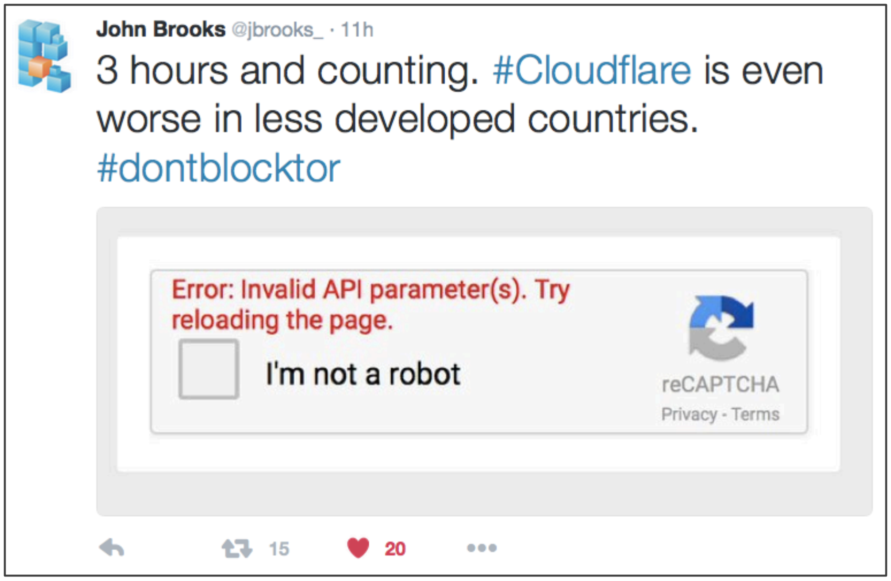
CloudFlare itself alludes to this on their CAPTCHA page:
"If you are on a personal connection, like at home, you can run an anti-virus scan on your device to make sure it is not infected with malware.
If you are at an office or shared network, you can ask the network administrator to run a scan across the network looking for misconfigured or infected devices."

This isn't practical for someone at an ISP with a large number of users.

CloudFlare's design assumption only works for communities that are allocated one or more IP addresses per person. As there are 7.5 billion people in the world, and only 3.5 billion usable IPv4 addresses, some regions lose out.

The US & Canada still have IPv4 addresses to give out. The Asia-Pacific ran out of IPv4 addresses in mid-2011, as did Europe in late 2013.[2] It also seems likely that African countries have very few IPv4 addresses compared with their population.

Here is a tweet from a developer testing Tor in Vietnam. He answered more than 30 sets of CAPTCHAs over three hours before accessing a website:



John Brooks @jbrooks_ · 11h

3 hours and counting. #Cloudflare is even worse in less developed countries. #dontblocktor

Error: Invalid API parameter(s). Try reloading the page.

□ I'm not a robot

Conclusion: CloudFlare's CAPTCHA system, which considers each IP address to be a single user, blocks access to information and hinders the right to privacy and free expression for millions of people. It puts Tor users, including human rights activists, domestic violence survivors, and others, at risk by forcing them to use unsafe computer software to reach essential websites.

The Tor Project's Mission Statement: "To advance human rights and freedoms by creating and deploying free and open anonymity and privacy technologies, supporting their unrestricted availability and use, and furthering their scientific and popular understanding."

—

1. Khattak, Sheharbano, et al. "Do You See What I See? Differential Treatment of Anonymous Users." *Network and Distributed System Security Symposium*. 2016.

2. https://en.wikipedia.org/wiki/IPv4_address_exhaustion#Regional_exhaustion