```
Audience: General, people who stumble upon gnu.org
          1924+/-395 words english
          1028+/-395 words instead?
          755 words        rahisibhasha
          stab at          french
Version: 2019-05-29
```

###

大云墙 (Dà Yún qiáng)
大きな雲壁 (Ookina Kumo kabe)
The Great Cloudwall

by Jeff Cliff

essistensa una reason you go to

###

There is a reason that none of your favourite work has appeared on Tor since early 2016[15].
That reason has lead to the discovery of a threat to the operation of the World Wide Web.

Prerequisites:
- The JavaScript Trap[47]
- Understanding that Google is not to be trusted[45][46]
- Nick Szabo: "Trusted Third Parties are Security Holes"[44][48]

Cloudflare is a network service for turing tests its users use against visitors, which means that it frustrates attempts
by users of its users to develop software to interact with their websites[3].
This might seem strange at first - why would you need a program to access a web resource?
But there's many things that work on the web like this, including RSS, streaming, chat, podcasts, and anti-virus definitions[57][58] which
are completely broken by a CAPTCHA appearing mid stream[11].
"We humans don't make HTTP requests, our machines to do it for us."
This makes clear what is really being tested here - whether or not you have the right software stack in between you and
Cloudflare.

This is not hypothetical: Cloudflare is currently attempting to dictate which browsers users of their "protected"
websites may use[60].

{{expand}}

Your right to use Free Software in this stack is at risk and could disappear at any moment.

It also is extracting free labor from website users[35], in effect tricking humans into acting like robots in order to
pass a test designed to see whether or not they are a robot. Worse, this labor is being used to train[62] Google's artificial intelligence, a very
poor candidate for "friendly AI"[36]. Given unfriendly AI is an existential[43]

risk[42] to mankind, avoiding this
should be among the highest of priorities.

This software stack includes human language: the CAPTCHAs are in English, leaving non-English speakers around the world
at a disadvantage[13]. Attempts to fix this are bound by the fact that they also leak language information to
Cloudflare[21].

Furthermore, they use Google's reCaptcha for their turing test/"proof you are a human" challenge and Google is known as a part of NSA's PRISM surveillance project so they expose their website visitor's data to PRISM data collection.

On its own, this is terrible bad but it's also worth pointing out how the reCAPTCHAs work. It isn't by whether or not you
click on the correct icon (though that is a factor too) but also collect:

> mouse movement, its slightness and straightness
> page scrolls
> time intervals between browser events
> keystrokes
> click location history tied to user fingerprint
> device information
> All these criteria are stored in the browser’s cookie and are processed by Google’s servers
> It should be emphasized that there is DARPA technology to identify people by mouse movements and typing
[23]

This collection of data is likely illegal in regions where privacy is taken seriously (like the EU)[24].

It is frustrating even when it works because you have to fill out 20 captchas on the off-chance that you succeed one time in
twenty. So this is 95% censorship and 5% wasting users' time[5].

More important, though, is that it starts to form a ratchet for web browser technology; the captchas are upgraded all the
time and if you use an older browser, you risk being left behind even when it works.

How Cloudflare Threatens You

"When you fetch a page from a website that is served from Cloudflare, JavaScript has been injected on-the-fly into that
page by Cloudflare. And they also plant a cookie that brands your browser with a globally-unique ID. This happens even if
the website is using SSL and shows a cute little padlock in your browser" [10]

- Cloudflare tracks you
Even if your traffic is protected from onlookers, Cloudflare itself can see your traffic[6] because they are a MITM[14][31].
In addition, if Cloudflare[53] has intercepted your traffic(MITM), so has the NSA[33].
"If a site uses Cloudflare, then the browser lock icon is a false promise."[14]
"The short version, a rhetorical question: Would you trust a key escrow regime, in which an “authorized” entity was
entrusted with the potential to decrypt all communications at will? If not, why

would you trust a de facto mass decryption chokepoint at which many communications are actually decrypted?"[34]

In other words,

- They are in a position to track, tap, and link Internet activity across a wide range of sites. [14]

- Cloudflare frustrates accessibility efforts[25][27][36]: "CAPTCHA remains the most problematic item indicated by respondents" Cloudflare is one of the largest, if not the largest source of unconsensual CAPTCHAS, making them quite possibly the biggest impediment in accessibility efforts worldwide.

- Cloudflare makes using Tor frustrating by making efforts to become anonymous more difficult and making it more likely that people will use non-Tor connections for some or all of their web browsing. The problem is getting worse with time. [13]

- It's not just Tor[19] but Tor users are the biggest group of people who've noticed it and are organizing against it so far.

- In particular, the model of Project Honeypot depends on one IPv4 address, meaning one person. As IPv4 addresses become scarce, more and more ISPs (and whole countries[22]) are forced to use higher and higher levels of NAT. The result is that the kinds of treatment of Tor users by Cloudflare starts to be not just for Tor, but for all web users. "Tor is just being slightly ahead of what the IPv4 Internet is going to look like pretty soon." The next time a large group wakes up, millions of websites might be down (including critical ones) across a whole continent. This has actually happened already. [49]

"It was made clear in the Snowden leaks that GCHQ, the NSA, etc. would like people to stop using Tor so I am sure they are very happy to see CF make general web browsing difficult and frustrating for ordinary users." [12]

- Worse, Cloudflare makes using Tor *dangerous* because enabling JavaScript and images to deal with their system makes it likely that some people will enable JavaScript and images on other websites, which, even if Cloudflare wasn't threatening them, would. [9]

- Cloudflare is capable of tracking users of its websites, and initial looks into its JavaScript/CAPTCHA seems to bear out that they are doing so.

- Cloudflare can target individual users with JavaScript malware; since you typically wind up enabling their JavaScript to use websites, you fall into their trap. Because they track users, are giving, individualised code, and work directly with the US government/DHS, there's no reason why they can't tailor attacks to specific users.

- Even if they aren't doing it yet, they are at any point one US government administration, one vulture capital funding purchase[26], or one internally rogue element away from executing JavaScript code on hundreds of millions of people's computers a "highly attractive" target[7] with no oversight. The code CAPTCHA itself protects attempts to detect such things from happening.

- The way that Cloudflare is constructed means that even by accident, billions of people can be analyzed by their government[51] and have their access limited or completely cut off at the government's whim.

Background : How Cloudflare threatens the web

- Cloudflare is a MITM for the whole web

- As of 3 years ago 10% of the top 25,000 websites used Cloudflare[2]
- A billion people in china are restricted by the Great Firewall[8]. Anyone who goes so far as to circumvent that must then deal with the "Great Cloudwall" for accessing the open internet.

- This is not just an individual problem, but fundamentally threatens the ecosystem of the web.
Cloudflare is breaking the open internet one site at a time. The web is massively resilient - we can do without Stack Overflow, GNU.org or even Google but when a significant enough portion of websites use a single provider, there starts to be a systematic risk that if that single provider goes down, all of the websites behind it will be inaccessible. Worse, you won't be allowed to access it unless you have the right kind of US government approved credential, contingent, perhaps, on running software only they approve of.

It is becoming a single point of failure for the internet. [39]

Right now, there are alternative sources for, for example, the US constitution[17]. It is not unthinkable that Cloudflare is getting big enough to threaten even that.

{FIX ME - make section clearer}
"A.1 sometimes there are necessary websites for some degree of necessary. Government websites, public service, etc. How long until those are behind the "Great Cloudwall"?
B: Not long. Our service is competitive and convenient. If public service websites choose to use our service for awesome DDoS protection, it's their choice."[36]

- Cloudflare has already started down the slippery slope[52] of censoring websites. If they didn't have a stranglehold on people accessing the internet, it would not be a problem. They are big enough that censorship from Cloudflare is starting to be a systematic exclusion from the political process.

"Cloudflare is perfect: it can implement censorship on the fly without anyone getting wise to it!"[40]

- DNS[39]: given that they have become so systematically powerful, the next step to cementing their power is to attack DNS. Their 1.1.1.1 DNS server, like Google's 8.8.8.8, is marketed to people so that Cloudflare will still be able to see you're going to them even if you don't interact with websites "protected" by them.

It gives them even more data to track you with.

Background : Where does Cloudflare come from?

Cloudflare comes from a project called "Project Honey Pot"[61], originally intended to track online fraud and abuse.

"What was Project Honey Pot?
'A service that positions itself as some kind of a grassroot-y anti-spam registry, but in reality seems to be a pro-corporate law enforcement tool with the specific aim of entrapping and prosecuting spammers/phishing scammers in a way that’s friendly to the marketing industry.'"

The US Department of Homeland Security approached the developers in 2007-8[1][36] for access to their data and they have been working with the US government[54] and law enforcement ever since[1].

On HTTP GET requests:

Cloudflare has a history of shutting down open DNS and open NTP servers.

"It would be great if they allowed GET requests - for example - such requests should not and generally do not modify server side content. They do not do this - this breaks the web in so many ways, it is incredible. Using wget with Tor on a website hosted by CF is... a disaster. Using Tor Browser with it - much the same. These requests should be idempotent according to spec, I believe."

{FIX ME - "critical of it"?}
Cloudflare has a history of closing tickets that are critical of it without actually resolving the issue[29][30][32]

"Cloudflare is based in a country with secret courts, secret police, and secret prisons that are above the law - and this secret government has characterized Cloudflare's data as extremely valuable"[28]
"The CEO says, "Cloudflare's strength lies in the DATA it collects -- not in its CODE.'"[28]
"The U.S. federal government is a Cloudflare customer."[28]
"Cloudflare has never stated that a government agency did not install wiretapping equipment or software on the same premises as a Cloudflare server."[28]
"Cloudflare has never indicated that the architecture of its content distribution network is resistant to warrantless mass surveillance."[28]
"Cloudflare has given the Chinese government unprecedented censorship capability."[28]
"Cloudflare has no intention to shut down as Lavabit did in order to protect the user from unlawful surveillance."[28]
"Some Cloudflare customers are paying over 1 million dollars per year for an undisclosed service."[28]

"But Cloudflare is really necessary, the web is a nasty place"

- The more of the web is held within Cloudflare, the more pressure will be on websites not behind Cloudflare
- As of 2016, by Cloudflare's own data, Tor was not as bad as normal internet

connections.

- People: "But we need Cloudflare to protect us from DDoS.”
  Cloudflare: "That’s a nice site you have there. It would be a shame, such a shame, if anything happened to it. Why don’t you let us decrypt all your TLS sessions[59] so we can protect you?"[14]

I heard Cloudflare is working with Tor and all is good now?

- Just because you can't see the problem doesn't mean it's not there.

- This is not true. Their websites still CAPTCHA their users, same as ever, and news agencies across the political spectrum screwed up stories about how the 'problem is fixed'. [18]

- It's actually worse, though[17], if we couldn't see it[60] - it was easy to get a lot of riled up Tor users to understand that Cloudflare was their adversary. It's a lot harder to convince people who are not blocked from their websites, today, why giving systematic control over the world wide web might be a bad thing tomorrow.

"Right now, Cloudflare says it monitors nearly 1/5 of all Internet visits. An astounding claim for a company most people haven’t even heard of"[40]

- But they are now doing more to track users and threaten the anonymity of Tor users.

- Cloudflare is one of a couple of large network providers that are capturing the vast majority of digital communications, effectively creating private networks the size of the modern internet that are competitive with and not subject to the same kinds of scrutiny and regulation as the internet[58].

What if we shut down Cloudflare and migrate all websites out of them?

We're probably going to have the same problem with another company very soon. Just as when suddenly Microsoft no longer had a monopoly on software, we didn't get rid of the problem of proprietary software, there's a couple of problems that, if we don't solve them, something like Cloudflare is roughly inevitable as a consequence:

Cloudflare DNS

"DNS[50] is around, servers are insecure, proper end-to-end crypto isn't the norm hence MITM goes unnoticed, anonymity is an edge case, routing lacks built-in resiliency to disruption, we're always going to have actors building a business model around cobbling together superficial, overapproximating mitigations."[20]

Mozilla and Cloudflare

"At least for browsing with Firefox, because Mozilla has partnered up with Cloudflare and will resolve the domain names from the application itself via a DNS server from Cloudflare based in the United States. Cloudflare will then be able to read everyone's DNS requests."
Sharing DNS requests with Cloudflare represents mozilla having a security hole, straight to the Cloudflare (and probably: the NSA).

What can you do?

Learn more about Cloudflare and make sure the people around you know about Cloudflare. Use Tor by default to be more
exposed to the blocks. Go to the anti-Cloudflare collaboration repository[41] and make sure websites you use aren't
"protected", and if they are, contact the people who run the website requesting that they no longer use Cloudflare. Get
involved!

References

[1] crimeflare. Is CloudFlare a honey pot?
https://web.archive.org/web/20170721161127/http://www.crimeflare.us/honeypot.html
[2] ioerror. Issues with corporate censorship and mass surveillance.
https://trac.torproject.org/projects/tor/ticket/18361#comment:15
[3] ioerror. Issues with corporate censorship and mass surveillance.
https://trac.torproject.org/projects/tor/ticket/18361#comment:21
[5] ioerror. Issues with corporate censorship and mass surveillance.
https://trac.torproject.org/projects/tor/ticket/18361#comment:28
[6] ioerror. Issues with corporate censorship and mass surveillance.
https://trac.torproject.org/projects/tor/ticket/18361#comment:30
[7] ioerror. Issues with corporate censorship and mass surveillance.
https://trac.torproject.org/projects/tor/ticket/18361#comment:32
[8] ioerror. Issues with corporate censorship and mass surveillance.
https://www.bloomberg.com/quicktake/great-firewall-of-china
[9] ioerror. Issues with corporate censorship and mass surveillance.
https://trac.torproject.org/projects/tor/ticket/18361#comment:51
[10] crimeflare. Is CloudFlare a honey pot?
https://web.archive.org/web/20170721161127/http://www.crimeflare.us/honeypot.html
[11] ioerror. Issues with corporate censorship and mass surveillance.
https://trac.torproject.org/projects/tor/ticket/18361#comment:59
[12] ioerror. Issues with corporate censorship and mass surveillance.
https://trac.torproject.org/projects/tor/ticket/18361#comment:66
[13] mikeperry. The Trouble with CloudFlare. https://blog.torproject.org/trouble-cloudflare
[14] nullius. Block Global Active Adversary Cloudflare.
https://trac.torproject.org/projects/tor/ticket/24351#comment:8
[15] Unknown. Google+
https://plus.google.com/105395547687614433866/posts/G9nnQBnLtjp
[16] Unknown. Google+
https://plus.google.com/105395547687614433866/posts/XnQryQ7hR9G
[17] msmach. Cloudflare Ends CAPTCHAs For Tor Users
https://it.slashdot.org/comments.pl?sid=12641622&cid=57348584
[18] msmach. Cloudflare Ends CAPTCHAs For Tor Users
https://it.slashdot.org/comments.pl?sid=12641622&cid=57388544
[19] ioerror. Issues with corporate censorship and mass surveillance.
https://trac.torproject.org/projects/tor/ticket/18361#comment:90
[20] ioerror. Issues with corporate censorship and mass surveillance.
https://trac.torproject.org/projects/tor/ticket/18361#comment:112
[21] ioerror. Issues with corporate censorship and mass surveillance.
https://trac.torproject.org/projects/tor/ticket/18361#comment:132
[22] ioerror. Issues with corporate censorship and mass surveillance.
https://trac.torproject.org/projects/tor/ticket/18361#comment:141
[23] ioerror. Issues with corporate censorship and mass surveillance.
https://trac.torproject.org/projects/tor/ticket/18361#comment:147
[24] ioerror. Issues with corporate censorship and mass surveillance.

https://trac.torproject.org/projects/tor/ticket/18361#comment:160

[25] ioerror. Issues with corporate censorship and mass surveillance. https://trac.torproject.org/projects/tor/ticket/18361#comment:175

[26] ioerror. Issues with corporate censorship and mass surveillance. https://trac.torproject.org/projects/tor/ticket/18361#comment:183

[27] ioerror. Issues with corporate censorship and mass surveillance. https://trac.torproject.org/projects/tor/ticket/18361#comment:231

[28] ioerror. Issues with corporate censorship and mass surveillance. https://trac.torproject.org/projects/tor/ticket/18361#comment:236

[29] ioerror. Issues with corporate censorship and mass surveillance. https://trac.torproject.org/projects/tor/ticket/18361#comment:255

[30] gk. Cloudflare breaks loading the chat. https://trac.torproject.org/projects/tor/ticket/23141

[31] nullius. Block Global Active Adversary Cloudflare. https://trac.torproject.org/projects/tor/ticket/24351#comment:20

[32] nullius. Block Global Active Adversary Cloudflare. https://trac.torproject.org/projects/tor/ticket/24351#comment:44

[33] nullius. Block Global Active Adversary Cloudflare. https://trac.torproject.org/projects/tor/ticket/24351#comment:52

[34] nullius. Block Global Active Adversary Cloudflare. https://trac.torproject.org/projects/tor/ticket/24351#comment:60

[35] nullius. Block Global Active Adversary Cloudflare. https://trac.torproject.org/projects/tor/ticket/24321#comment:13

[36] Anonymous. Cloudflare philosophy. https://codeberg.org/crimeflare/cloudflare-tor/src/master/cloudflare-philosophy.md

[37] Peter O'Shaughnessy. Screen Reader User Survey Results #7. https://toot.cafe/@peter/99398584471715976

[39] ungeich. A new feature in Firefox https://blog.ungleich.ch/en-us/cms/blog/2018/08/04/mozillas-new-dns-resolution-is-dangerous/

[40] Yasha Levine. iSucker: Big Brother Internet Culture http://exiledonline.com/isucker-big-brother-internet-culture/

[41] Anonymous. The Great Cloudwall. http://codeberg.org/crimeflare/cloudflare-tor

[42] lesswrong wiki. Unfriendly artificial intelligence https://wiki.lesswrong.com/wiki/Unfriendly_artificial_intelligence

[43] Ben Harack. What is an existential risk? https://www.visionofearth.org/future-of-humanity/existential-risks/what-is-an-existential-risk/

[44] Nick Szabo. Twitter http://twitter.com/nickszabo4

[45] FSF. Google's Software is Malware https://www.gnu.org/proprietary/malware-google.en.html

[46] Richard Stallman. Reasons not to use Google https://stallman.org/google.html

[47] Richard Stallman. The JavaScript Trap https://www.gnu.org/philosophy/javascript-trap.html

[48] Nick Szabo. Trusted Third Parties are Security Holes. 2001. https://nakamotoinstitute.org/trusted-third-parties

[49] slashgeek. CloudFlare is ruining the internet (for me) https://www.slashgeek.net/2016/05/17/cloudflare-is-ruining-the-internet-for-me/

[50] Hamid Sarfraz. How likely is it that CloudFlare is an NSA operation? https://www.quora.com/How-likely-is-it-that-CloudFlare-is-an-NSA-operation/answer/Hamid-Sarfraz

[51] Karthik Balakrishnan. Airtel is sniffing and censoring CloudFlare’s traffic in India and CloudFlare doesn’t even know it. https://medium.com/@karthikb351/airtel-is-sniffing-and-censoring-cloudflares-traffic-in-india-and-they-don-t-even-know-it-90935f7f6d98

[52] http://pleroma.oniichanylo2tsi4.onion/notice/1563

[53] StopMITMInt. Add an option to stop trusting Cloudflare certificate https://github.com/mozilla-mobile/focus-android/issues/1743#issuecomment-351555735

[54] goody2shoes. Block Global Active Adversary Cloudflare

https://lists.torproject.org/pipermail/tor-talk/2018-January/043889.html
[55] EFF. The Crypto Wars https://www.eff.org/document/crypto-wars
[56] http://forums.clamwin.com/viewtopic.php?t=4915
[57] November 2018 Archives by thread http://lists.clamav.net/pipermail/clamav-users/2018-November/thread.html
[58] https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20181218/Documents/Geoff_Huston_Presentation.pdf
[59] Thorin-Oakenpants. let's talk about our little buddy cloudflare. https://github.com/ghacksuserjs/ghacks-user.js/issues/310#issuecomment-351913412
[60] ghost. What do you think about Cloudflare? https://github.com/privacytoolsIO/privacytools.io/issues/374#issuecomment-460413259
[61] Unspam Technologies, Inc. https://projecthoneypot.org/
[62] TechRader. Captcha if you can: how you’ve been training AI for years without realising it https://www.techradar.com/news/captcha-if-you-can-how-youve-been-training-ai-for-years-without-realising-it