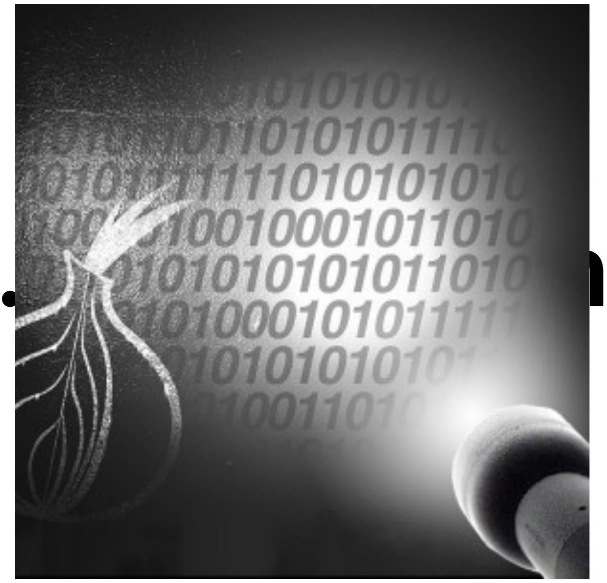
The Deep Web

Fear and loathing in the Tor network (http://kernelmag. /issue-sections /features-issue-sections/10386 /tor-network-

Trending



(http://kernelmag.dailydot.com/issue-sections /features-issue-sections/10376/how-to-search-deep-web-tor/)

The new search engines shining a light on the Deep Web

surveillance/)

By Patrick Howell O'Neill on September 28th, 2014

One strange encounter has been nagging Griffin Boyce for months.

He was eating lunch with a friend one afternoon late last March at an ornate Vietnamese restaurant in Washington, D.C. The place was practically empty, the final chill of an unbearably cold winter lingering outside. Curiously, a woman sidled up next to them, so near the two friends couldn't help but feel crowded.

"She picked the spot closest to us, two feet away, and ordered tea but didn't drink it," Boyce recalled. "She also seemed to be listening in. She left when we got the check, and watched us at the subway station."

Pho DC, the restaurant they were dining at, sits right around the corner from the International Spy Museum in the city's Penn Quarter neighborhood. One wonders if spies have a sense of humor about these sorts of things.

Boyce then returned home to find that his apartment had been broken into.

It wasn't obvious at first. There were plenty of valuable items—laptops, a flatscreen TV, and a PlayStation 4—that were not even touched. In fact, the only thing missing was a pair of microSD cards that had been on his desk.

Still, there was evidence of foul play. Boyce's routers had been pulled out of the cabinet and left dangling by their cables. His bedroom curtains were open where they hadn't been before, and most importantly, his laptop had been used and then turned off.

Boyce spoke to several lawyers following the incident. There wasn't enough damage to warrant the trouble it would cost to file a police report, they reasoned, and it probably wouldn't lead to anything. Even though he was sure a crime had taken place, Boyce decided that police involvement wasn't worth the effort.

(http://kernelmag.dailydot.com/issue-sections/features-issue-sections/10376/how-to-search-deep-web-tor/)

There's a whole other world out there. You just have to know where to look.

(http://kernelmag.dailydot.com/issue-sections/staff-editorials/10395/why-to-download-tor/)

Why we need Tor now more than ever (http://kernelmag.dailydot.com/issue-sections/staff-editorials/10395/why-to-download-tor/)

Despite its seedier affiliations, Tor is an essential tool for avoiding censorship and surveillance.

(http://kernelmag.dailydot.com/issue-sections/headline-story/10397/deep-web-size-

"My apartment was really obvious, but it could have been intentionally obvious," Boyce explained. "A security engineer [I spoke to] said either it was the worst contractor in the world or it was intentional. It seems like intimidation."

If the intruder didn't steal anything, what might he have been looking for?

Boyce writes code for Tor (http://www.dailydot.com/tags/tor/), the most popular anonymity network in existence. The software allows anyone to access the Internet anonymously or visit the Deep Web—the opaque abyss of the Internet that offers anonymity to anyone who wants it. It's essential for journalists, human rights activists, cops, and cybercriminals alike.

That means Boyce is also in close contact with many other people involved in the project, not to mention a few journalists who might be of keen interest to intelligence agencies.

If the burglar was after data on Boyce's laptop, tough break: Full-disk and home-directory encryption rendered it practically impenetrable. The machine housed lots of unreleased code for Boyce's personal projects, as well as a significant buddy list. That's more valuable than it sounds. A smart intelligence team can use a buddy list to nail down exactly who is talking to whom, helping them to build a social graph that maps both real and all potential communications.

The laptop was dropped in the quarantine bin, never to be trusted again.

"It created a lot of worry," said Boyce, who recalled sitting on his bed for half an hour in shock. "It made me withdraw from friends and family for quite a while."

Someone else might have dismissed the whole thing as an odd occurrence and an unfortunate coincidence. Boyce says he knows better.

For those involved in Tor, his encounter is merely the latest in a string of incidents that have led them to one inevitable conclusion:

infographic/)

The unstoppable rise of the Deep Web (http://kernelmag.dailydot.com/issue-sections/headline-story/10397/deep-web-size-infographic/)

The fall of Silk Road didn't kill the Deep Web. It made it stronger.

They're nearly all being watched all over the world.

Threat level

First launched in 2002 and boasting 150 million downloads in the last year alone, Tor plays an instrumental role in political activism all over the world.

When Turkey censored the Internet earlier this year amid profound civil unrest, the population turned to Tor as a workaround, with more than 10,000 new users (http://www.dailydot.com/technology/turkey-10000-per-day-tor/) signing up daily. It's a staple in more oppressive countries like Iran, China, as well as across nations in Africa. Julian Assange (http://www.dailydot.com/tags/julian-assange/) relied on it to kickstart and sustain WikiLeaks. Its most famous user is Edward Snowden (http://www.dailydot.com/tags/edward-snowden/), who used it to leak tens of thousands of National Security Agency (http://www.dailydot.com/tags/nsa/) documents.

> Governments are engaged in an arms race with liberation technologists like Tor developers—a fight that has no end in sight.

The team behind Tor also does extensive outreach work with activists around the globe—from Iran's liberal Green Party to democrats in Zimbabwe— that put them in direct conflict with numerous powerful ruling regimes. When Iran blacklisted (http://www.dailydot.com/politics/iran-censors-tor-75-percent/)Tor and knocked 75 percent of users in the country offline earlier this year, developers worked overtime to identify the problem and work with Iranians to circumvent the newest roadblock thrown in front of them.

For that reason, governments are engaged in an arms race with liberation technologists like Tor developers—a fight that has no end in sight.

Tor developers are working to expand the software's capability and accessibility, no matter what level of tech literacy a person possesses.

Boyce, for instance, is involved in a project called Stormy that is meant to make launching (http://www.dailydot.com/technology/tor-stormy-launch-september-2014/)hidden services—anonymous websites on the Tor network—a much easier task. Other projects aim to make the network even faster (http://www.dailydot.com/technology/toroken-tor-bitcoin-anonymity/), to build an anonymous Instant messenger (http://www.dailydot.com/technology/tor-instant-messaging-bundle/), and a Tor-powered mobile operating system (http://www.dailydot.com/technology/tor-anonymous-mobile-os-tails/).

In short, everything Tor is doing is meant to give more people easy access to powerful anonymity, and the developers behind the project are almost all prominent liberation technology activists with their hands in projects all over the Internet and the world.

Given Tor's proven ability to challenge authority and resist power, it's easy to see why governments around the world might be interested in keeping close tabs on those involved.

Person of interest

It's impossible to say when and where exactly the alleged surveillance began, but there's one catalyst that gets much of the blame for why it started.

"Jake's WikiLeaks work got all of Tor targeted, frankly," Andrew Lewman, Tor's executive director, said.

He’s referring to Jacob Appelbaum (http://www.dailydot.com/tags/jacob-appelbaum/), an American developer, activist, and journalist living in Berlin. His substantial résumé only begins with representing and working with Julian Assange (http://www.dailydot.com/tags/julian-assange/) and WikiLeaks (http://www.dailydot.com/tags/wikileaks/). He’s an ongoing advocate for Edward Snowden (http://www.dailydot.com/tags/edward-snowden/), the whistleblower who revealed the extent of the National Security Agency (http://www.dailydot.com/tags/nsa/)’s spying apparatus, and has done extensive journalistic work on Snowden’s leaks.

He’s also a prominent software developer and spokesperson for Tor, which was used by both Snowden and Assange to leak many thousands of documents to the world—to say nothing of his work on a host of other anti-censorship tools through the years.

Appelbaum was also the first member of the Tor Project to speak publicly about being followed in the streets of Berlin. He’s livetweeted (https://twitter.com/ioerror/status/216671818528989184)incidents when he believed he was being followed, taunting his surveiller about how easy it was to spot him and his conspicuous colleagues. After Snowden’s leaks began, he let the world know that the increased surveillance he endured was both a point of pride—the world must really be paying attention, after all—and an extreme annoyance.

“When I flew away for an appointment, I installed four alarm systems in my apartment,” he told the German daily newspaper *Berliner Zeitung* in December 2013. “When I returned, three of them had been turned off. The fourth, however, had registered that somebody was in my flat—although I’m the only one with a key. And some of my effects, whose positions I carefully note, were indeed askew. My computers had been turned on and off.”

> "If you work with people who are under surveillance on a regular basis, eventually you will be surveilled."
> —Griffin Boyce

As stressful as his situation has been in Berlin, things were even worse for him in the United States.

"In the U.S., I'm fairly certain I've had a black bag job"—a covert and often illegal intelligence-gathering operation—"on my apartment," Appelbaum told (http://motherboard.vice.com/blog/jacob-appelbaum-utopia-interview) *Vice* last year.

There's no doubting that Appelbaum has been targeted in various capacities. For instance, in 2010, as part of a wider sweep against WikiLeaks, the U.S. Department of Justice obtained a secret court order (http://www.dailydot.com/news/wikileaks-court-order-twitter-records-fight/) directing Twitter (http://www.dailydot.com/communities/twitter/) to turn over "all records" relating to Appelbaum's account, including all correspondence both public and private, records of activity, and connection data.

"My mother was arrested and jailed supposedly for unrelated charges," Appelbaum told (http://motherboard.vice.com/blog/jacob-appelbaum-utopia-interview)*Vice*, "and—at at least two points—interrogated about my role in WikiLeaks. I'm fairly certain that my partner woke up with night vision goggles pointed at her by unknown parties outside her house."

Not everyone believes Appelbaum's claims. They are, after all, anecdotes that are mostly difficult or impossible to prove.

"I've talk to those in charge of following," Robert Graham, a prominent security researcher, said last year. “They don’t find your claims of being followed credible.”

However, in the Internet freedom community and at Tor in particular, there’s little doubt that physical surveillance is taking place.

“If you work with people who are under surveillance on a regular basis, eventually you will be surveilled,” Boyce said.

By that logic, everyone at Tor is under the microscope. Many anti-censorship and privacy activists—a scene in which Tor plays a starring role—believe that countries all over the world are actively watching them and attempting to infiltrate their circles, their groups, and even their parties.

“I’ve been followed in foreign countries,” Lewman said. “I’ve had interactions with people who seem to know way too much about me, stuff that I haven’t told anyone for 20 years so then you don’t know who you’re talking to.”

“I’ve been followed,” Karen Reilly, Tor’s development director, added. “As a woman, being followed and not knowing whether it’s somebody who works for the government or a random person who may wish me harm, makes me incredibly angry.”

Boyce specifically claims to have had surveillance run-ins since 2011. As he’s become more involved in Tor, the experiences have become stranger.

“The day before leaving [the country last], me and another [Tor] researcher were followed in D.C.,” he said. “As we were going up an escalator, someone took our photo as they were going down. Then they ran onto the train.”

On a recent work trip, a laptop Boyce was carrying was held and pried open at landing, he claimed. “The [laptop] bag was ‘lost’ for several hours, then found, then ‘lost’ again, then delivered to the hotel.”

Some people understandably take incidents like these as a cue to exit the world of Internet activism. When allegedly targeted, Boyce said a friend of his abruptly left the country, moved his family abroad, and backed off of activism in general—ironically, to a country that rumored to be engaged in some aggressive spying of its own.

If the goal of the alleged surveillance is intimidation, results are mixed.

“We’re in no way the only people this happens to,” Boyce said. “Only a handful of people talk [publicly] about it.”

Every developer at Tor who spoke with The Kernel believed that they had personally experienced physical surveillance either at home or in public, though not everyone was comfortable explaining the incidents on the record.

That doesn’t mean that every single person working at Tor is necessarily being followed, but it does paint a vivid portrait of the vigilance and suspicions permeating through the most prominent privacy project of this era.

“I deal every day with people that are incredibly, outlandishly paranoid for a variety of completely legitimate reasons,” Boyce said earlier this year. He called paranoia a fixed “feature of the landscape” of the censorship-circumvention world.

For Reilly, the prospect of widespread surveillance touches a more personal nerve.

“One of the reasons I’m so passionate about it is that part of my family was behind the Iron Curtain. I’m half-German,” she explained. “State surveillance is part of my family’s history.

“It’s same playbook in authoritarian regimes as it is at home—it’s just a different language.”

If the goal of the alleged surveillance is intimidation, results are mixed. There have been contractors and volunteers reportedly visited by security services who have stopped working with Tor as a direct result. But for those who stick around, it only strengthens their resolve.

“There have probably been an equal number who have had this happen and said, ‘Fuck them,’ only to have their dedication become stronger,” Lewman explained.

“I’m willing to continue to work,” Reilly continued. “That doesn’t make me special; there’s no room for victim-blaming or shaming people into accepting risk, but I feel angry on behalf of people trying to make the world a better place.”

Photos via waferboard (https://www.flickr.com/photos/waferboard/5624753564/)*/Flickr (CC BY 2.0), Jim Pennucci* (https://www.flickr.com/photos/pennuja/9526683684/)*/Flickr (CC BY 2.0), and Wikimedia* (http://upload.wikimedia.org/wikipedia/commons/thumb/1/15/Tor-logo-2011-flat.svg/1280px-Tor-logo-2011-flat.svg.png) | *Remix by Max Fleishman*

More from THE KERNEL

<

(http://kernelmag.dailydot.com/issue-sections/features-issue-sections/10393

(http://kernelmag.dailydot.coı/issue-sections/features-issue-sections/10407
>