

THREAT LEVEL

With This Tiny Box, You Can Anonymize Everything You Do Online

BY ANDY GREENBERG 10.13.14 | 6:30 AM | PERMALINK

Share 2.1k Pin it 9



Anonabox

No tool in existence protects your anonymity on the Web better than the software Tor, which encrypts Internet traffic and bounces it through random computers around the world. But for guarding anything other than Web browsing, Tor has required a mixture of finicky technical setup and software tweaks. Now routing all your traffic through Tor may be as simple as putting a portable hardware condom on your ethernet cable.


Today a group of privacy-focused developers plans to launch a Kickstarter campaign for Anonabox. The \$45 open-source router automatically directs all data that connects to it by ethernet or Wifi through the Tor network, hiding the user's IP address and skirting censorship. It's also small enough to hide two in a pack of cigarettes. Anonabox's tiny size means users can carry the device with them anywhere, plugging it into an office ethernet cable to do sensitive work or in a cybercafe in China to evade the Great Firewall. The result, if Anonabox fulfills its security promises, is that it could become significantly easier to anonymize all your traffic with Tor—not just Web browsing, but email, instant messaging, filesharing and all the other miscellaneous digital exhaust that your computer leaves behind

SUBSCRIBE GIVE A GIFT RENEW INTERNATIONAL ORDERS

FOLLOW WIRED




MOST RECENT WIRED POSTS



These Are The Emails Snowden Sent to First Introduce His Epic NSA Leaks



The Bad Physics in The Amazing Spider-Man 2



The Strange and Radical New World of 3-D Printed Body Parts



Bizarre Gadget Makes Music by Scanning an Arm Tattoo



With This Tiny Box, You Can Anonymize Everything You Do Online



Next Big Trend: Robots That Follow You Around

TRENDING NOW ON WIRED

Finding a Video Poker Bug Made These Guys Rich—Then Vegas Made Them Pay

With This Tiny Box, You Can Anonymize Everything You Do Online

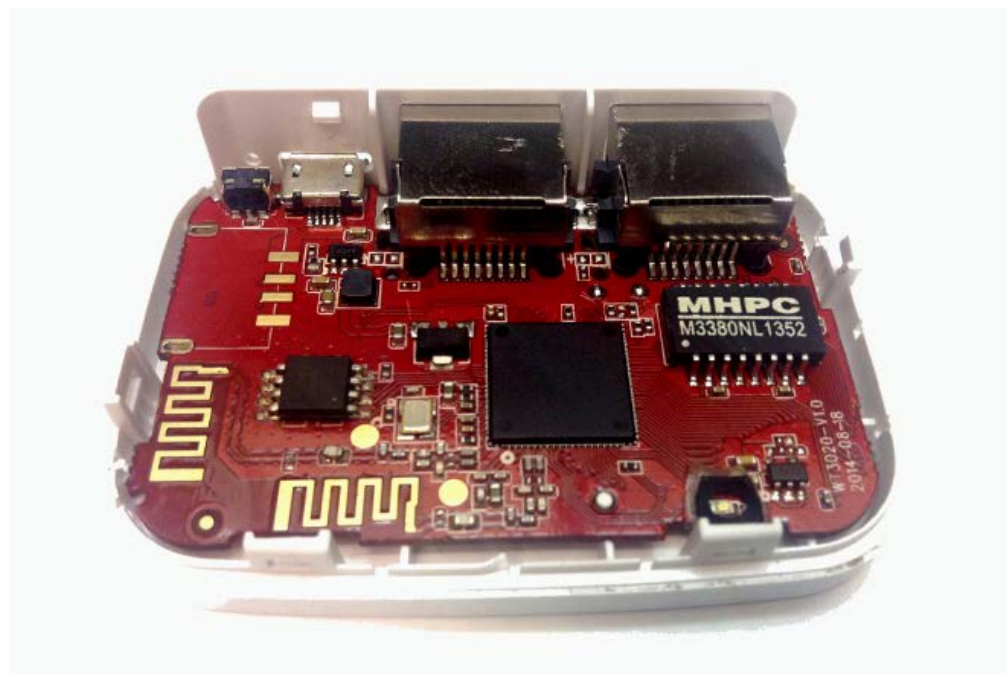
These Are The Emails Snowden Sent to First Introduce His Epic NSA Leaks

online.

“Now all your programs, no matter what you do on your computer, are routed over the Tor network,” says August Germar, one of the independent IT consultants who spent the last four years developing the Anonabox. He says it was built with the intention of making Tor easier to use not just for the software’s Western fans, but for those who really need it more in Internet-repressive regimes. “It was important to us that it be portable and small—something you can easily conceal or even throw away if you have to get rid of it.”

This has happened before

Anonabox is by no means the first project to attempt to integrate Tor directly into a router. But Germar argues it will strike the best balance yet of cheapness, easy setup, size and security. Tor-in-a-box projects like [Torouter](#) and [PORTAL](#), for instance, require the user to replace the software on a stock router. Another project called [OnionPi](#) is designed to be built one from a kit, and costs roughly twice as much as Anonabox.



August Germar

In terms of consumer friendliness, the closest device yet to a plug-and-play Tor router has been [Safeplug](#), a \$49 variant on a Pogoplug router modified to route all traffic over Tor. But at more than twice the size, the Safeplug isn’t nearly as portable as the Anonabox. And it’s also been criticized for security flaws; Researchers at Princeton found in September that it didn’t have any authentication on its settings page. That means a hacker could use a technique called a Cross-Site Request Forgery to trick a user into clicking on a link that would change the router’s functions or turn off its Tor routing altogether. It also uses an outdated version of Tor, one that had been updated even before the device shipped last year.

Anonabox’s security hasn’t yet been audited for those sorts of flaws. But its creators point out that it will be entirely open source, so its code can be more easily scrutinized for errors

...reatest Maps in History,
...ected in One Fantastic Book

The Mustang Finally Grows Up,
But It’s Still a Hoodlum at Heart

RED *threat*
level

WRITERS

erg

ip

SUBSCRIBE TO WIRED MAGAZINE

SUBSCRIBE

Get Our Newsletter

WIRED’s best stories in your inbox,
delivered weekly.

Enter your email address

Submit

Will be used in accordance with our [Privacy Policy](#)

ADVERTISEMENT

SERVICES

SUBSCRIBE

Quick Links: [Contact Us](#) | [Login/Register](#) | [Newsletter](#) | [RSS Feeds](#) | [WIRED Jobs](#) | [WIRED Mobile](#) | [FAQ](#) | [Sitemap](#)

and fixed if necessary.

The community is watching

The non-profit Tor project itself is reserving judgment for now. But its executive director Andrew Lewman tells WIRED he's keeping an eye on the project, and that it "looks promising so far." Micah Lee, lead technologist for Glenn Greenwald's [The Intercept](#) and a frequent developer on Tor-related projects, says he's mostly encouraged by the idea. One of the potential vulnerabilities for Tor users, after all, is that a website they visit could run an exploit on their computer, installing malware that "phones home" to a server across a non-Tor connection to reveal their real IP address. "If you're using something like this, everything goes over Tor, so that can't happen," Lee says. "A Tor router can definitely have a big benefit in that there's physical isolation."

He nonetheless cautions that Anonabox alone won't fully protect a user's privacy. If you use the same browser for your anonymous and normal Internet activities, for instance, websites can use "browser fingerprinting" techniques like cookies to identify you. Lee suggests that even when routing traffic over Tor with Anonabox, users should use the Tor Browser, a hardened browser that avoids those fingerprinting techniques. (To avoid running their traffic through Tor twice and reducing bandwidth speeds to a crawl, he points to a setting in the Tor Browser called "transparent torification," which turns off the browser's own Tor routing.)

The Anonabox has been in the works since 2010, long enough that its developers have been able to evolve their own custom board as well as an injection-molded case. That customization, Germar says, means the tiny device still packs in 64 megabytes of storage and a 580 megahertz processor, easily enough to fit the Tor software and run it without any slowdowns.

Built for civil disobedience

Germar says he and his friends began thinking about the possibility for the device around the time of the Arab Spring in late 2010 and early 2011. The Anonabox is ultimately intended for users in other countries where Tor's anti-censorship and privacy properties can help shield activists and journalists. It can be used in a cybercafe, for instance, where users can't easily install new software on computers. And it's capable of so-called "pluggable transports"—extensions to Tor that often allow its traffic to better impersonate normal encrypted data.

The hardware design of the Anonabox is also intended to work in the most sensitive international situations: It uses a micro-USB as a power source, a common standard around the world, and its small size is meant to allow easy concealment. Germar points out that its rounded corners means it can even be stowed in a bodily orifice. And it can be destroyed more easily than a larger router. "Maybe it's too late and the police are already downstairs, so you smash the box with a brick and throw the pieces out the window," he says. "Or maybe you just crush it by stepping on it with your shoe and flush the pieces down the toilet."

Germar's ultimate goal, he says, is to bring Tor to a new audience that has never before had access to its protections. "This isn't just about making things easier for people who use Tor

now, but also those who would like to use Tor but can't for whatever reason," he says.

"Those are the people we want to help."

 Share 2.1k 



[24 Comments](#) | [Permalink](#)

[FAQ](#) | [CONTACT US](#) | [WIRED STAFF](#) | [ADVERTISING](#) | [PRESS CENTER](#) | [SUBSCRIPTION SERVICES](#) | [NEWSLETTER](#) | [RSS FEEDS](#) 

Condé Nast Web Sites: [Webmonkey](#) | [Reddit](#) | [ArsTechnica](#) | [Details](#) | [Golf Digest](#) | [GQ](#) | [New Yorker](#)

WIRED.com © 2014 Condé Nast. All rights reserved. Use of this Site constitutes acceptance of our [User Agreement](#) (effective 01/02/2014) and [Privacy Policy](#) (effective 01/02/2014). [Your California Privacy Rights](#).

The material on this site may not be reproduced, distributed, transmitted, cached or otherwise used, except with the prior written [permission of Condé Nast](#).

[Ad Choices](#) 