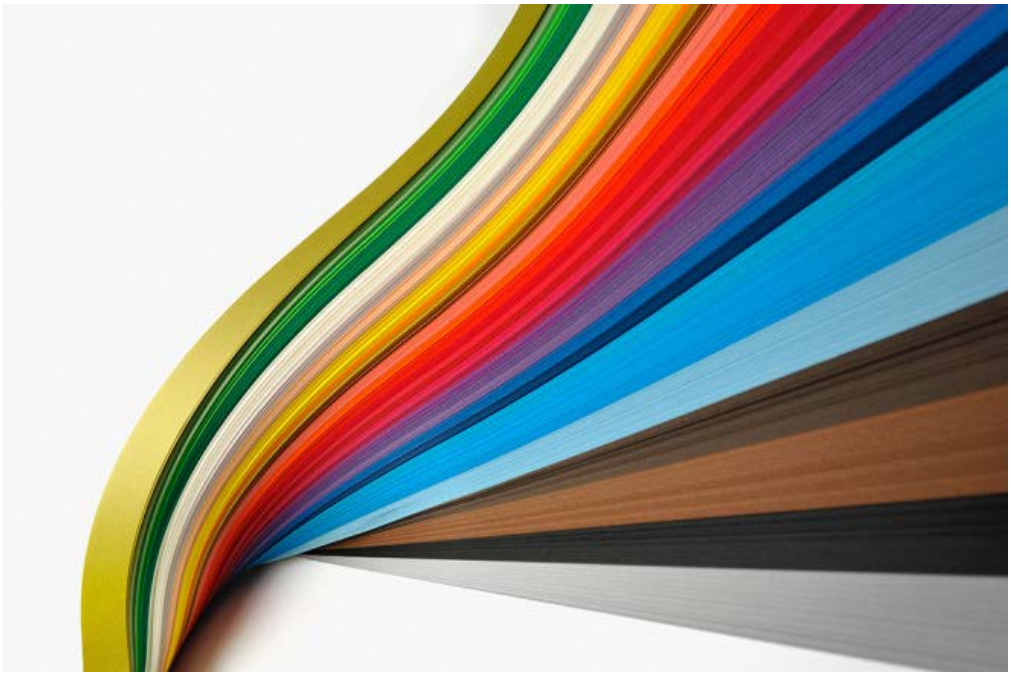
THREAT LEVEL

Now Everyone Wants to Sell You a Magical Anonymity Router. Choose Wisely

BY ANDY GREENBERG 10.24.14 | 6:30 AM | PERMALINK



Yagi Studio/Getty Images

Maintaining your privacy online, like investing in stocks or looking good naked, has become one of those nagging desires that leaves Americans with a surplus of stress and a deficit of facts. So it's no surprise that a cottage industry of privacy marketers now wants to sell them the solution in a $50 piece of hardware promising internet "anonymity" or "invisibility." And as with any panacea in a box, the quicker the fix, the more doubt it deserves.

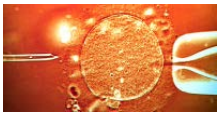
Last week saw the fast forward rise and fall of Anonabox, a tiny $45 router that promised to anonymize all of a user's traffic by routing it over the anonymity network Tor. That promise of plug-and-play privacy spurred Anonabox to raise $615,000 on the fundraising platform Kickstarter in four days, 82 times its modest $7,500 goal. Then on Thursday, Kickstarter froze those pledges, citing the project's misleading claims about its hardware sources. Other critics pointed to flaws in Anonabox's software's security, too.

But the Anonabox fiasco hasn't deterred other projects hoping to sell an anonymity router of their own. In fact, many of them see Anonabox's 9,000 disappointed backers as proof of the demand for their own privacy-in-a-box product. At least five new or soon-to-launch

MOST RECENT WIRED POSTS


Google's Search Czar Just Smashed Felix Baumgartner's Sky Dive Record


Stephen Hawking Joins Facebook, Urges Fans to 'Be Curious'


The Sobering Facts About Egg Freezing That Nobody's Talking About


A New Answers App Aims to Succeed Where Quora Failed


How to Earn the Right to Buy Ferrari's Most Exclusive Hypercar


Ebola Shows It Is Process--Not Technology--That Will Protect Us

TRENDING NOW ON WIRED

A Google Exec Just Skydived 136K Feet, Smashing the World Record

The Laborers Who Keep Dick Pics and Beheadings Out of Your Facebook Feed

Stephen Hawking Joins Facebook, Urges Fans to 'Be Curious'

Crowdfunding projects now claim to offer a consumer-focused anonymity router with names like Invizbox, Cloak, TorFi, and PORTAL, each with its own promises—and caveats.

Security Claims and Snake Oil

Some of those projects are already repeating Anonabox's mistakes, or making significant new ones. A project called TorFi, which offered a version of Tor installed on an off-the-shelf Wi-Fi router, has already had its Kickstarter campaign yanked, seemingly under the same prohibition that killed Anonabox (selling someone else's product). Another router initiative called Project Sierra doesn't use Tor's well-tested anonymity system that routes traffic through three random hops among thousands of computers; Instead, its creator Kerry Cox says it pushes data through VPN servers rented from a Texas hosting company, an option that likely means faster connections but not much real anonymity. Anything you do can be seen by that Texas company or any third party that can get access to its data, including law enforcement.

A third option called Wemagin has filled its Kickstarter page with brash claims of a "military grade" USB drive that offers untraceability (without using Tor) and a "private browser...so simple your Grandmother can use it." It doesn't offer details about how any of those features actually work. "I'm surprised these guys aren't telling you it'll also help you lose weight and is powered by antioxidants," says Steve Lord, a British penetration tester and one of the critics who poked holes in Anonabox's security claims.

A humbler project called Invizbox, which launched last week on Indiegogo, is more straightforward about its protections and imperfections. Invizbox uses the same hardware as Anonabox, and similarly integrates Tor with the open source wireless software OpenWRT. It promises, however, to fix its predecessor's configuration flaws—Anonabox was criticized for shipping with no password protection for its Wi-fi network by default, and hardcoded root and SSH passwords that could let a hacker compromise the device. But Invizbox still uses stock hardware that its creators admit may have vulnerabilities it can't control, and the project has yet to release its software for outside scrutiny.

More promising, perhaps, are projects like Cloak and PORTAL. Cloak is a $56, open-source Tor router set to launch with a Kickstarter campaign early next week. Cloak's creators, a group of developers spread across Britain, Malaysia, and China, are developing their device's hardware from scratch. One member of the team, a founder of the Shenzhen, China-based hardware maker Dragino, is leading the creation of Cloak's board and injection molded case, which isn't yet finished. And Cloak's open-source code has already been published for public appraisal. "This is the right attitude," says Lord. "They're doing it the way that Anonabox should have done it."

PORTAL, by contrast, focuses more on software than hardware: The project, whose name is an acronym for "Personal Onion Router To Assure Liberty" uses a "hardened" version of OpenWRT combined with Tor that's designed to be installed on any stock router. Marc Rogers, a security consultant and one of PORTAL's creators, says they've carefully pruned features out of OpenWRT to minimize attack points for any hacker trying to compromise the router. And unlike other projects, he says PORTAL's developers have taken pains to integrate Tor so that it's guaranteed to "fail closed"—Even if the router somehow can't connect to Tor, no data will ever be sent over the unprotected Internet. "If Tor isn't working, it's a brick," Rogers says.

Big Challenges Ahead

But even the most reputable of these Tor router projects like PORTAL and Cloak face serious challenges. Because the official Tor Project doesn't support OpenWRT, they'll be responsible for their own firmware updates. If a vulnerability is found in Tor—not too uncommon an event—it will have to be patched by the Cloak or PORTAL teams themselves, and then users will have to be warned to install the update or be left vulnerable. When the Tor Project was working on creating its own Tor router in 2012, that necessity of separate security updates for OpenWRT was one of the stumbling blocks that kept the router from coming to fruition, says Runa Sandvik, a former Tor developer. "Getting a new version of Tor on OpenWRT out to people was a bit of a process, and not one that the Tor Project itself could easily own and control at that point," she says. "You'd have to take it on yourself to keep it updated to keep your users safe."

More fundamentally, routing all the data that goes through your home router over the Tor network may not even be such a smart idea. As soon as a users log into just one of their online accounts over that connection, they've likely identified themselves, and their traffic can be correlated with any other browsing that they had hoped to keep anonymous. To prevent browser fingerprinting techniques like cookies, careful users will still need to use the Tor browser, with its "transparent torification" setting on to avoid routing their traffic through Tor twice and slowing it to a crawl. And even involuntary data leakage like the location data uploaded by desktop searches in Apple's OSX Yosemite could be enough to pierce the veil.

Andrew Lewman, executive director of the Tor project, says he's supportive of the idea of building a Tor hardware router, but cautions that simply funneling all your traffic through Tor isn't a simple privacy cure. "We don't do any analysis or cleaning of your data in transit over Tor; nor do we want to do so," Lewman writes. "Plugging in an operating system that wants to share all your data behind a Tor router will just share all of your data over Tor"—including all the data that could accidentally finger you as its source.

Better Yet…

In many cases, users would be better off segmenting their online activities into sensitive communications that need to be Torified, and the normal non-sensitive browsing that could actually pollute their untraceable traffic. That means carefully plugging into and out of a Tor router depending on the situation; Or privacy activist and developer Micah Lee suggests keeping one computer connected into a Tor router and using that machine only for anonymous activities. "Just using a Tor router won't necessarily make you anonymous...A lot of what you do on the internet is intrinsically not anonymous." Lee says. "These projects are really good, but you need to be cautious. Don't think you're anonymous when you're not."

As with all privacy technology, no single tool provides complete security or anonymity. Instead, fully protecting yourself requires a change in behavior to consider the privacy consequences of every action online—what hackers and spies call "operational security" or "opsec." And that can't be bought in a box. "There's not much point in having an opsec tool," says PORTAL's Rogers, "if you don't have an opsec frame of mind."

49 Comments | Permalink