SECURITY (/CATEGORY/SECURITY)

security (/tag/security/), privacy (/tag/privacy/), websites (/tag/websites/), encryption (/tag/encryption/)

Tor stands strong against the NSA, but your browser can bring you down

Brad Chacos
@BradChacos

Oct 4, 2013 10:27 AM

Another day, another revelation revealed by Edward Snowden's leaks. Friday, *The Guardian (http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption)* reported that the U.S. NSA and its British equivalent, the GCHQ (http://en.wikipedia.org/wiki/Government_Communications_Headquarters), have been actively trying to defeat the encrypted protection provided by the popular Tor anonymity software.

But amazingly, it appears the attempts have failed. The latest Snowden leak suggests that Tor has actually withstood the brunt of the NSA's efforts thus far.

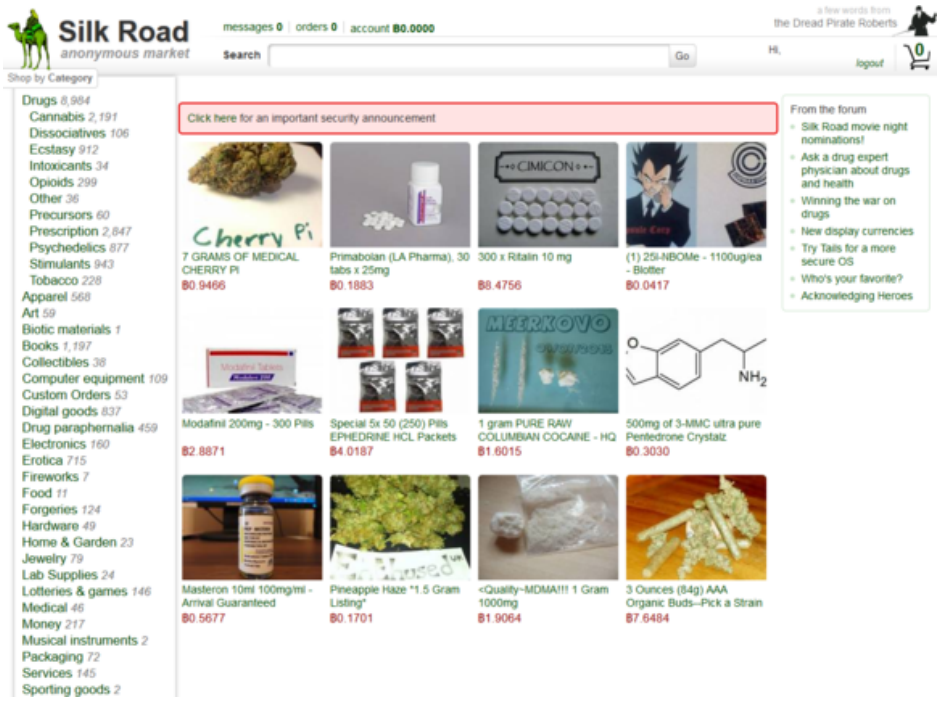
"We will never be able to de-anonymize all Tor users all the time," according to a leaked presentation titled 'Tor Stinks,' the Guardian reports. "With manual analysis, we can de-anonymize a very small fraction of Tor users."

That doesn't mean Tor is a magic bullet for cloaking your online steps, however.

Sneaking in through the side door

It's no surprise that the NSA is targeting Tor. Have you seen the depravity that goes on down there in the Tor-enabled Darknet, the hidden underbelly of the web? (http://www.pcworld.com/article/2046227/meet-darknet-the-hidden-anonymous-underbelly-of-the-searchable-web.html) The billion-dollar Silk Road drug bazaar

(http://www.pcworld.com/article/2051367/feds-seize-hefty-bitcoin-haul-during-silk-road-smackdown.html) was just the tip of the iceberg, and the anonymization software can also make communication easier for criminals.



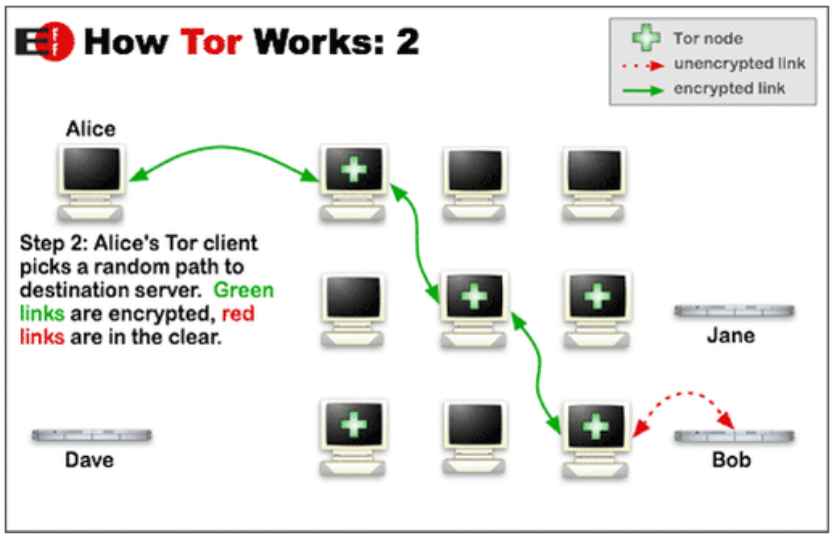
(http://images.techhive.com/images/article/2013/08/silk-road-mainpage-100049468-orig.png)

You could buy anything at the Silk Road before its recent shutdown—crack, meth, forged IDs, assassins, computer-hacking services, you name it.

Yes, Tor is also a haven for whistleblowers and political dissidents, but it's the government's job to stop bad guys from doing bad things, remember—and cracking Tor can help them do that.

Along those lines, the NSA *has* managed to identify some Tor traffic, but doing so involved taking advantages of vulnerabilities in the Firefox browser included with the Tor Browser Bundle (http://www.pcworld.com/article/2026362/review-tor-browser-bundle-lets-you-browse-in-anonymity.html), rather than compromising the Tor network itself. The NSA infected browsers with rogue code via a "honey pot" website designed to only attack people using the Tor network, though *The Guardian* says Firefox 17 plugged the particular hole the authorities were using.

Earlier this year, the FBI seized control of the servers of the largest Darknet website-hosting service, and infected them with malware that "phoned home" (http://www.wired.com/threatlevel/2013/09/freedom-hosting-fbi/) with the distinct MAC address of users who visited the hosting service's sites. Again, the identification method relied on software vulnerabilities (http://www.pcworld.com/article/2046013/tor-project-stop-using-windows-disable-javascript.html). Tor quickly updated the Tor Browser Bundle to a more recent version of Firefox, and disabled JavaScript by default to squash the exploit.



While the NSA and GCHQ haven't breached the Tor network directly, they're trying. *The Guardian* reports that the duo is dabbling in proof-of-concept attacks that entail mass surveillance of the Tor network, or a mixture of tapping core Internet cables while simultaneously controlling a large number of Tor's "exit nodes," which deliver unencrypted requests to website servers.

The government agencies have also discussed "shaping" future Tor development to increase crackability—as the NSA did with NIST encryption standards and backdoors in other software (http://www.pcworld.com/article/2048268/schneier-on-nsas-encryption-defeating-efforts-trust-no-one.html) —or actively disrupting Tor to drive users off the network.

Security expert Bruce Schneier has a mind bogglingly deep technical discussion of the NSA's Tor-skirting attempts in another *Guardian* article (http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity) if you're interested in nitty-gritty details.

Protecting yourself

Even so, Snowden's documents seem to indicate that Tor's core security is intact, at least for now.

“The good news is that they went for a browser exploit, meaning there’s no indication they can break the Tor protocol or do traffic analysis on the Tor network,” Tor president Roger Dingledine told *The Guardian*. “Infecting the laptop, phone, or desktop is still the easiest way to learn about the human behind the keyboard.”

Indeed, endpoint protection was one of the four important security lessons learned (http://www.pcworld.com/article/2051673/4-important-lessons-learned-from-the-silk-road-smackdown.html) in the wake of the Silk Road’s smackdown. Keep your software up-to-date! The federal case against Snowden’s email provider also drove home the point that email can never be truly secure (http://www.pcworld.com/article/2046962/nsa-dodging-mail-service-explains-why-email-can-never-truly-be-private-and-secure.html)—a minor concern for most folks, but a major concern for people seeking sanctity in Tor’s anonymous network.

Tor also can’t help you stay anonymous if you’re running around the Net and filling out web forms willy-nilly, or if you’re using certain browser plugins. Our tutorial to how (and why) to surf the web in secret (http://www.pcworld.com/article/2013534/how-and-why-to-surf-the-web-in-secret.html) has all the details.

Finally, regardless of whether or not you’re using Tor, check out PCWorld’s guides to NSA-proofing your data (http://www.pcworld.com/article/2048248/heres-how-to-best-secure-your-data-now-that-the-nsa-can-crack-almost-any-encryption.html) and protecting your PC from Prism surveillance (http://www.pcworld.com/article/2041044/how-to-protect-your-pc-from-prism.html). Even if you’ve got nothing to hide from the government, adopting strong security practices is always a smart idea.