BLACK BAG (/)

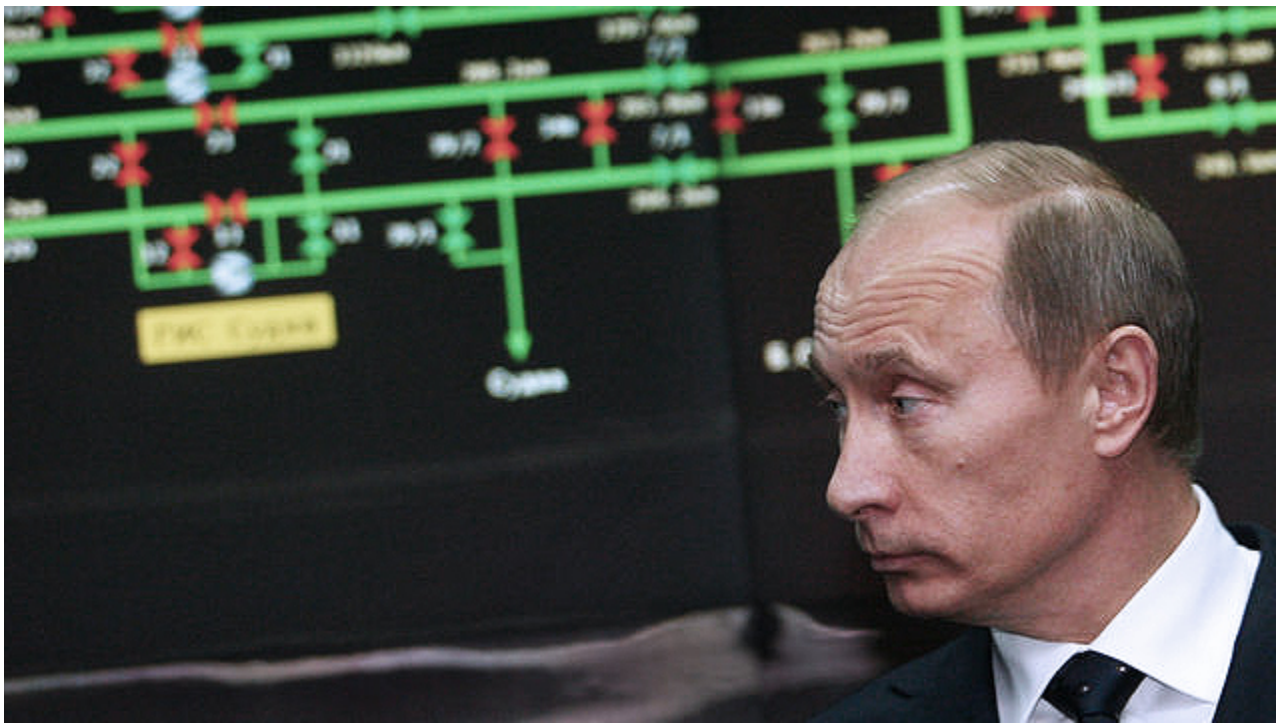
(/)

Putin Regime Offering 3.9 Million to Expose Tor's Anonymous Network (http://blackbag.gawker.com/putin-regime-offering-3-9-million-to-expose-tors-anonym-1612966385)

(http://matthew-phelan.kinja.com)

Matthew Phelan (http://matthew-phelan.kinja.com) 8,551 6

Filed to: MOTHER RUSSIA (/TAG/MOTHER-RUSSIA) Yesterday 3:45pm (http://blackbag.gaw



Russia is hoping that 3.9 million roubles (http://bit.ly/1nRU4Y0) will be sufficient to produce a feasibility study on cracking Tor (https://www.torproject.org/)—a nonprofit service that reroutes internet traffic to anonymize user's IP addresses. Turns out: They could have saved over 3.7 million roubles just by switching to whatever these guys at Carnegie Mellon did (http://www.theguardian.com/technology/2014/jul/22/is-tor-truly-anonymising-conference-cancelled)!

Russia's Ministry of Internal Affairs, or MVD, posted (http://bit.ly/1nRU4Y0) their procurement specs (or "tender") (http://en.wikipedia.org/wiki/Government_procurement) earlier this month, calling for "research work on the possibility to obtain technical information about users (user equipment) of the anonymous network Tor." Very quickly, however, MVD rescinded those details as news outlets, like the *Moscow Times* (http://www.themoscowtimes.com/news/article/interior-ministry-seeks-ways-to-track-tor-user-data/504051.html) and (seriously (http://thefootballexaminer.com/technology-22/100-000-offered-by-russia-for-cracking-

tor-3548.html) everyone (http://bit.ly/1n13oTa) else (http://bit.ly/1rNLwIo), picked up the story:

> Russia's Interior Min has softened the description of its tender paying $100k to crack @torproject (https://twitter.com/torproject). h/t @josephfcox (https://twitter.com/josephfcox) pic.twitter.com/QJ52pBdMo0 (http://t.co/QJ52pBdMo0)
>
> — Kevin Rothrock (@KevinRothrock) July 25, 2014 (https://twitter.com/KevinRothrock/statuses/492647895993024512)

Or, maybe, Russia was just straight-up ashamed that researchers at Carnegie Mellon's Computer Emergency Response Team (http://www.cert.org/) had announced a cheaper $3000-method for exposing the identities of Tor users. (MVD's 3.9 million-rouble contract comes out to about $109,723-and-change USD.)

Carnegie Mellon researchers Alexander Volynkin and Michael McCord were scheduled to present a talk this August on the discovery, at the annual Black Hat hacker conference (https://www.blackhat.com/index.html)in Las Vegas. Entitled "You don't have to be the NSA to break Tor: de-anonymising users on a budget," it promised to show how any dedicated hacker-and-thousandaire could "de-anonymise hundreds of thousands of Tor clients and thousands of hidden services within a couple of months." Then, to the disappointment of many, the talk was removed from Black Hat's schedule (https://www.blackhat.com/us-14/schedule/), its synopsis replaced with (https://www.blackhat.com/latestintel/07212014-a-schedule-update.html) the following notice:

> *Late last week, we were informed by the legal counsel for the Software Engineering Institute (SEI) and Carnegie Mellon University that: "Unfortunately, Mr. Volynkin will not be able to speak at the conference since the materials that he would be speaking about have not yet [been] approved by CMU/SEI for public release." As a result, we have removed the Briefing from our schedule.*

What really happened, though?

Let's, just for a moment, speculate, shall we?

Carnegie Mellon's Software Engineering Institute is "a Federally Funded Research and Development Center (FFRDC) (http://www.sei.cmu.edu/about/organization/workingwithanFFRDC.cfm) sponsored by the U.S. Department of Defense (DoD)" according to

the Regime Offering (http://www.sei.cmu.edu/about/). As the *Guardian* reported yesterday (http://www.theguardian.com/technology/2014/jul/29/us-government-funding-tor-18m-onion-router), Tor received $1.8 million (https://www.torproject.org/about/findoc/2013-TorProject-FinancialStatements.pdf) from the U.S. government last year, the majority of it through "pass-through" grants via a third party, but $100,325 came directly from the National Science Foundation and $256,900 came the U.S. Department of State. That's roughly 65 percent of Tor's budget—and it has truly been money well spent, both for traditional espionage, and promoting freedom/regime change wherever American interests deem that freedom/regime change may ring. It would really suck to lose such an expensive asset—even just for the short period it would take to patch up whatever hole Volynkin and McCord discovered—yes?

A lot of journalists asked Carnegie Mellon and the Tor foundation itself (https://lists.torproject.org/pipermail/tor-talk/2014-July/033954.html), why the talk was pulled, with little in the way of new information emerging. Maybe they should have just asked Dad instead? The global hegemonic patriarchy that is the U.S. Military-Industrial complex, I mean.

Anway: Tor is naturally very popular in Russia, where an ex-lieutenant colonel of the KGB named Vladimir Vladimirovich Putin has ruled—autocratically and without a shirt (http://shirtlessputindointhings.tumblr.com/post/36952890239/putin-is-kind-to-the-horse-he-doesnt-just-ride)—for going on 15 years.

Source: Tor metrics (https://metrics.torproject.org/users.html?graph=userstats-relay-country&start=2012-01-01&end=2014-07-25&country=ru&events=off#userstats-relay-country)

Russian citizens looking to duck censorship and political repression constitute the fifth largest block of Tor users, a figure that (as you can see in the chart above) has spiked recently due to the passage of a "bloggers law" that required any site with more than 3000 daily visitors to formally register with the government. Registering, as the *New York Times* clarifies

(http://www.nytimes.com/2014/05/07/world/europe/russia-quietly-tightens-reins-on-web-with-bloggers-law.html?_r=0), ultimately means that bloggers "will be considered a media outlet akin to a newspaper and be responsible for the accuracy of the information published." These bloggers will also no longer be permitted to post anonymously. High-traffic not-exactly-news agencies, like search engines and social networks, were required to keep a record of all activity on their sites for six months by the law—in stark contrast to the American method (http://www.wired.com/2012/03/ff_nsadatacenter/) wherein the government secretly stores it themselves outside Bluffdale, Utah (http://www.wired.com/tag/bluffdale/).

Still, unflattering comparisons notwithstanding, the suppression of public speech in Russia has been very severe lately, in response to a long string of well-attended opposition rallies since 2011. Three major opposition news sites were blocked by the Putin government (http://www.theguardian.com/world/2014/mar/14/russia-bans-alexei-navalny-blog-opposition-news-websites) in March, as was the blog of anti-corruption activist Alexei Navalny. (They all now, obviously, can only be accessed in Russia via Tor.) In April, state investigators searched (http://www.theguardian.com/world/2013/apr/18/russian-internet-social-media-network) the offices of the very popular Russian social networking site, VKontakte, as well as the home of its boy founder, Pavel Durov, ostensibly over allegations of some kind of traffic violation.

"A year ago, when the protests started, Durov showed he wasn't ready to close protest pages," a source told the *Guardian* (http://www.theguardian.com/world/2013/apr/18/russian-internet-social-media-network). "That's when his problems started."

That week, a fund belonging to Ilya Shcherbovich, a Russian oligarch and board member at the state-owned oil company Rosneft, unexpectedly bought 48 percent of VKontakte, meaning that "Putin is now the de facto owner" according to the *Guardian*'s source.

Worse still, Putin signed a law recently requiring that all internet companies (e.g. Facebook, Twitter) store Russian user data within the nation's borders, presumably so that it can be readily accessed by the government's intelligence agencies in collusion with the nation's communications providers, like Rostelecom. The law, which goes into effect in 2016, is clearly designed to stifle dissent, as is Rostelecom's recent investment in Deep Packet Inspection technology, which promises to filter internet traffic based on content rather than its point of origin.

Earlier this year, Putin very hilariously dismissed the whole internet (http://www.nytimes.com/2014/05/07/world/europe/russia-quietly-tightens-reins-on-web-with-bloggers-law.html?_r=0) as "a special C.I.A. project," which, while partially true, is not entirely fair to the Pentagon's APRANET and DARPA people (http://en.wikipedia.org/wiki/ARPANET), or Al Gore (http://www.snopes.com/quotes/internet.asp), or all the wizards who stayed up late at MIT and elsewhere to bring us the internet (http://www.powells.com/biblio/9780684832678). However, it does highlight that Tor, nonprofit though it may be, is caught along with Syria, and Ukraine, and the rest of us in some kind of post-Soviet Cold War right now.

So, in lieu of all this pertinent background, how should Russian MVD's desire for a Tor crackoff method be considered?

Andrei Soldatov, an expert on surveillance and security services, has told reporters that it is primarily a veiled threat from a government that, as opposed to China's wholesale blocking of websites, tends to focus more on intimidation.

"It's not important if the Russian government is able to block Tor or not," Soldatov says (http://www.theguardian.com/world/2014/jul/25/russia-research-identify-users-tor). "The importance is that they're sending signals that they are watching this. People will start to be more cautious."

However, Russian Pirate Party (http://en.wikipedia.org/wiki/Pirate_Party_of_Russia) leader Stanislav Sharikov told *Global Voices (http://globalvoicesonline.org/2014/07/24/russia-tor-privacy-nsa/)* that the $100,000 contract (http://zakupki.gov.ru/epz/order/notice/zkk44/view/common-info.html?regNumber=0373100088714000008), which is frankly small by tech company standards, and the contract's origin in the Interior Ministry, suggests that this may have been a true public relations goof-up. MVD, Sharikov suggests, is more interested in conducting genuine police work, ferreting out child pornographers in the Deep Web, and so forth, and should not really be confused with the hardcore spooks at Russia's intelligence agency, the FSB.

For what it's worth, this is exactly the perspective that the Tor Project's board appears to have taken. Engaging in a charming bit of trash talk, Tor's executive director Andrew Lewman told Vice's *Motherboard* (http://motherboard.vice.com/read/russia-has-put-a-bounty-on-tor), "What the Russian's have really done is effectively offer a bug bounty program for Tor. We assume many other national police forces are doing the same thing, just not publicly. We have a good track record of reverse engineering attacks and fixing the attack, even when we're not told the details."

Pretty baller, right? Lewman continues, "There are some talented people in Russia who will likely try to get some funding for finding bugs. It will be interesting to see if they find anything; and if they do, if the bugs are around design or more standard software vulnerabilities."

"The bug is a nice bug," Tor Project Leader Roger Dingledine reassured (https://lists.torproject.org/pipermail/tor-talk/2014-July/033956.html) subscribers to Tor Talk group, "but it isn't the end of the world."

Reassuring as this all may sound, the reality is of course simply that Tor is vulnerable *right now*, to anyone who has been surveilling CERT researchers at Carnegie Mellon, like their DoD paymasters or (Oh, wow!) sexy, college-aged Russian spies at Carnegie Mellon. Are you a researcher at Carnegie Mellon's Software Engineering Institute? You might be having sex right now with someone who does not really love you, but is instead a Russian spy. Or a Chinese spy. Who told you that you were really worthy of love? They might also be a spy.

As for the rest of you, this global drama should not directly impact you, no doubt, because you purchased a junk ThinkPad on Craigslist, anonymously, in cash, and have been pirating Internet access from a mile away with a PREMIERTEK Outdoor 2.4GHz 24dBi Directional High-Gain N-Type Female Aluminum Die Cast Grid Parabolic Antenna (http://www.premiertek.net/products/networking/ANT-GRID-24dBi.html), like I told you to, right?

Right?

[*photo of Putin visiting Gazprom HQ via (http://www.gettyimages.com/detail/news-photo/russian-prime-minister-vladimir-putin-inspects-the-inside-news-photo/84267250) Alexander Nemenov/AFP /Getty Images*]

To contact the author (https://twitter.com/CBMDP), email matthew.phelan@gawker.com (mailto:matthew.phelan@gawker.com), pgp public key (http://pgp.mit.edu/pks/lookup?op=get&search=0x11E842642C4B4E99).

6 ★ 33 Reply

Matthew Phelan's Discussions (http://blackbag.gawker.com/putin-regime-offering-3-9-million-to-expose-tors-anonym-1612966385)

All replies (http://blackbag.gawker.com/putin-regime-offering-3-9-million-to-expose-tors-anonym-1612966385/all)

Paul_D (http://stahvinahtist002.kinja.com) ▸ Matthew Phelan
Yesterday 4:42pm (http://blackbag.gawker.com/tor-accept-challenge-1613564470)
(http://stahvinahtist002.kinja.com)

TOR ACCEPT CHALLENGE

9 ★ 1 Reply

Dolemite (http://dolemite.kinja.com) ▸ Paul_D
Yesterday 4:44pm (http://blackbag.gawker.com/tor-expose-self-unbuckles-pants-1613565904)
(http://dolemite.kinja.com)

3 ★ Reply

(http://terpsnation.kinja.com)

Terpsnation (http://terpsnation.kinja.com) ▸ Matthew Phelan
Yesterday 5:47pm (http://blackbag.gawker.com/give-it-a-month-3-9-million-roubles-will-be-worth-299-1613608420)

Give it a month, 3.9 million roubles will be worth $2999, and who'll be laughing then!

2 ★ Reply

(http://mcpoyle.kinja.com)

McPoyle (http://mcpoyle.kinja.com) ▸ Matthew Phelan
Yesterday 4:36pm (http://blackbag.gawker.com/wow-roubles-are-super-lame-1613560140)

Wow, roubles are super lame.

2 ★ 1 💬 Reply

(http://matthew-phelan.kinja.com)

Matthew Phelan (http://matthew-phelan.kinja.com), Host ▸ McPoyle
Yesterday 4:41pm (http://blackbag.gawker.com/lol-its-true-1613564086)

LOL. It's true.

1 ★ Reply

(http://mazalya.kinja.com)

Mazalya (http://mazalya.kinja.com) ▸ Matthew Phelan
Yesterday 4:45pm (http://blackbag.gawker.com/regime-the-putin-regime-the-russian-government-too-1613566686)

Regime? The Putin *Regime*? The Russian government too many letters for you?

5 ★ 4 💬 Reply

(http://matthew-phelan.kinja.com)

Matthew Phelan (http://matthew-phelan.kinja.com), Host ▸ Mazalya
Yesterday 4:50pm (http://blackbag.gawker.com/i-did-not-make-the-70-character-count-rule-mazalya-go-161356

I did not make the 70 character count rule, Mazalya! (http://www.theawl.com/2013/04/half-a-tweet-gawker-headlines-max-out-at-70-characters-tomorrow) Google News(?) and Facebook(?) and this guy did:

EXPAND

(Also, this article is pretty fair, you will find, I hope. I am weirdly agnostic on Putin.)

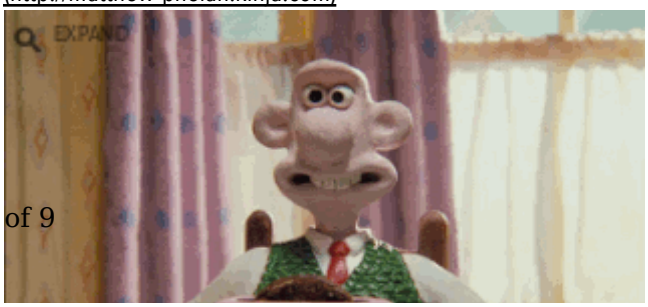
5 ★ Reply

MrTripps (http://mrtripps.kinja.com) ▸ Matthew Phelan
Yesterday 5:11pm (http://blackbag.gawker.com/i-was-hanging-out-with-a-bunch-of-pen-test-geeks-about-1613584719)
(http://mrtripps.kinja.com)

I was hanging out with a bunch of pen test geeks about a month ago and asked if Tor really is secure. They just laughed and laughed. Short answer: no.

1 ★ Reply

Matthew Phelan (http://matthew-phelan.kinja.com), Host ▸ MrTripps
Yesterday 5:18pm (http://blackbag.gawker.com/this-wasnt-in-the-new-york-metro-area-was-it-perchanc-161358
(http://matthew-phelan.kinja.com)



This wasn't in the New York Metro Area, was it, perchance?

[*matthew.phelan@gawker.com (mailto:matthew.phelan@gawker.com)*]

1 Reply


(http://mrtripps.kinja.com)

MrTripps (http://mrtripps.kinja.com) ▸ Matthew Phelan
Yesterday 8:03pm (http://blackbag.gawker.com/nah-texas-1613686462)

Nah. Texas.

Reply

View all 33 replies (http://blackbag.gawker.com/putin-regime-offering-3-9-million-to-expose-tors-anonym-1612966385/all)