Somewhere in Russia an eavesdropper is operating a network of wiretapped nodes at the edge of the Tor anonymity network. And he's particularly interested in what you're doing on Facebook.

Russian Spy Nodes Caught Snooping on Facebook Users

By Kevin Poulsen
01.21.14
5:52 PM

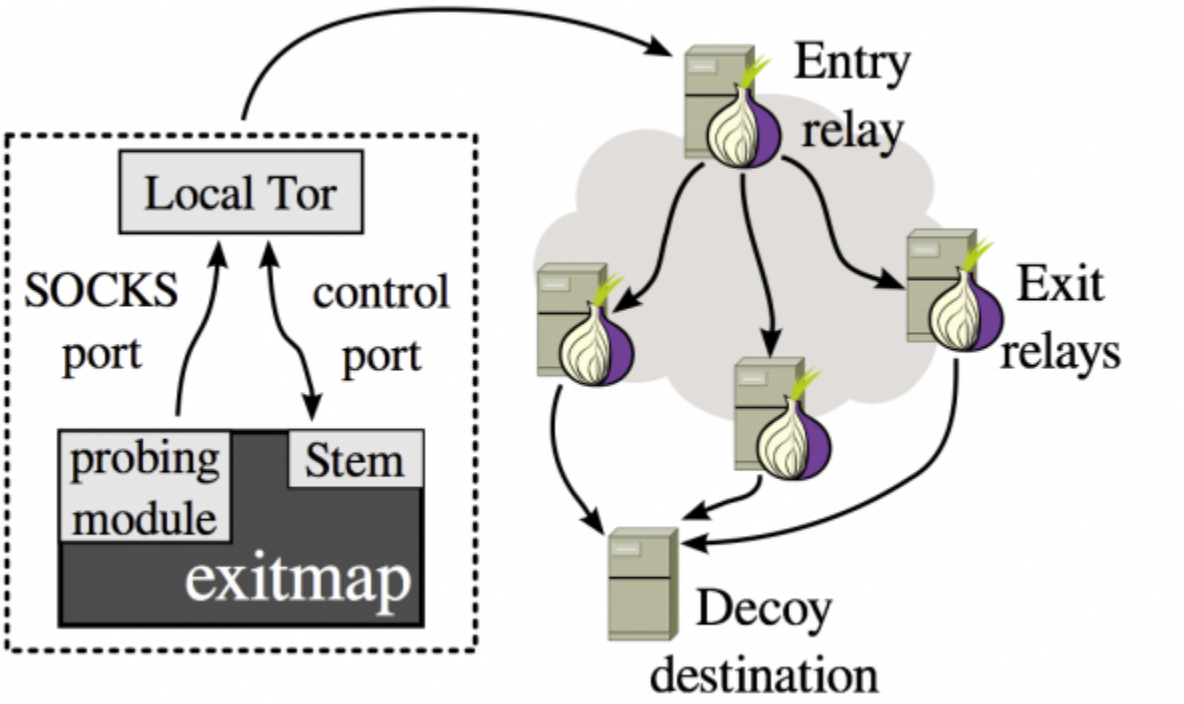

Image courtesy of Philipp Winter and Stefan Lindskog

Somewhere in Russia an eavesdropper is operating a network of wiretapped nodes at the edge of the Tor anonymity network. And he's particularly interested in what you're doing on Facebook.

That's the conclusion of two researchers who used custom software to test Tor exit nodes for sneaky behavior, in a four-month study published yesterday.

Philipp Winter and Stefan Lindskog of Karlstad University in Sweden identified 25 nodes that tampered with web traffic, stripped out encryption, or censored sites. Some of the faulty nodes likely resulted from configuration mistakes or ISP issues. But 19 of the nodes were caught using the same bogus crypto certificate to perform man-in-the-middle attacks on users, decrypting and re-encrypting traffic on the fly.

At times the evil nodes were programmed to intercept only traffic to particular sites, like Facebook, perhaps to reduce the chances of detection.

"These are the ones that we actually found," says Winter. "But there might be some more that we didn't find."

Tor is free software that lets you surf the web anonymously. It achieves that by accepting connections from the public internet – the "clearnet" — encrypting the traffic and bouncing it through a winding series of computers before dumping it back on the web through any of over 1,000 "exit nodes."

Traffic is safe from interception in the middle of that tangle of routing. But when it hits the exit node it's unavoidably vulnerable to spying, the same way a postcard is intrinsically vulnerable to a snooping mailroom clerk.

Since Tor nodes are run by volunteers, half of them anonymous, and they can be easily set up and taken down again at will, it's accepted that unencrypted web traffic will sometimes fall into the hands of a corrupt exit node operator. WikiLeaks, for example, famously got its start by eavesdropping on Chinese hackers through a bugged exit node.

The new study looked at exit nodes that were going beyond passive eavesdropping on unencrypted web traffic and were taking steps to actively spy on SSL-encrypted traffic. By checking the digital certificates used over Tor connections against the certificates used in direct clearnet sessions, researchers found several exit nodes in Russia that were clearly staging man-in-the-middle attacks. The Russian nodes were re-encrypting the traffic with their own self-signed digital certificate issued to the made-up entity "Main Authority."

Unlike other anomalous exit nodes, when the researchers had the "Main Authority" nodes blacklisted in Tor, new ones using the same certificate would pop up again in short order. In all, they saw 19 different Main Authority nodes in their four months of testing. Eighteen were in Russia, and one was in the U.S.

It's not clear who's behind Main Authority, but the researchers think it's more likely to be an individual snoop with a weird, voyeuristic hobby than a government agency. For one thing, receiving a self-signed certificate triggers a conspicuous browser warning to Tor users. "It was actually done pretty stupidly," says Winter.

But the study is a reminder that the NSA and the FBI aren't the only adversaries targeting Tor users. Tor's *raison d'etre* — keeping users anonymous – is not undermined by the corrupt exit nodes. Tor remains the best way to protect your anonymity online.

"We think it's a good paper and its great that someone is doing the research," says Andrew Lewman, executive director of the nonprofit Tor Project. "Plaintext over Tor is still plaintext. We've been saying this since 2010."

Kevin Poulsen is the investigations editor at Wired and author of Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground (Crown, 2011). His PGP fingerprint is A4BB A435

2FE1 B4A8 46E1 7AF6 DA4B 5DFA FF09 4870
Read more by Kevin Poulsen
Follow @kpoulsen on Twitter.

Tags: anonymity, russia, Tor
Post Comment | 3 Comments | Permalink
Back to top

3 comments

0

Join the discussion…

Best Community Share Login

Disturbed12 • 5 hours ago
What makes TOR better than I2P?
2 • Reply • Share ›

Muddy Road • 2 hours ago
Why would anyone in their right mind want to hack the drivel on Facebook?

I would think at a certain point one would become irreversibly bonkers.

And, the roll your own certificate generates an ominous warning....hmmmm
1 • Reply • Share ›

Carbon-12 • an hour ago
Wait... does the Tor Browser not use HTTPS by default? If the page is encrypted with Facebook's public key, then no amount of bad nodes should be able to snoop on it.
• Reply • Share ›

Subscribe Add Disqus to your site DISQUS