CRYPTOME

Question: Should You Trust Tor?

Answer: **Not If Your Life Is At Stake**

By Bill Blunden, July 16, 2014

In the ongoing drizzle of Snowden revelations the public has witnessed a litany of calls for the widespread adoption of online anonymity tools. One such technology is Tor, which employs a network of Internet relays to hinder the process of attribution. Though advocates at the Electronic Frontier Foundation openly claim that "Tor still works[1]" skepticism is warranted. In fact anyone risking incarceration (or worse) in the face of a highly leveraged intelligence outfit like the NSA would be ill-advised to put all of their eggs in the Tor basket. This is an unpleasant reality which certain privacy advocates have been soft-pedaling.

The NSA Wants You To Use Tor

Tor proponents often make a big deal of the fact that the NSA admits in its own internal documents that "Tor Stinks," as it makes surveillance more work-intensive[2]. What these proponents fail to acknowledge is that the spies at the NSA also worry that Internet users will abandon Tor:

> *"[A] Critical mass of targets use Tor. Scaring them away from Tor might be counterproductive"*

Go back and re-read that last sentence. Tor is a signal to spies, a big waving flag that gets their attention and literally draws them to your network traffic[3]. Certain aspects of Tor might "stink" but ultimately **the NSA wants people to keep using Tor**. This highlights the fact that security services, like the FBI[4], have developed sophisticated tools to remove the veil of anonymity that Tor aims to provide.

For example, the *Washington Post* reports[5]:

> *"One document provided by Snowden included an internal exchange among NSA hackers in which one of them said the agency's Remote Operations Center was capable of targeting anyone who visited an al-Qaeda Web site using Tor."*

It's well known that Tor is susceptible to what's called a *traffic confirmation attack* (AKA *end-to-end correlation*), where an entity monitoring the network traffic on both sides of a Tor session can wield statistical tools to identify a specific communication path. Keep in mind that roughly 90 percent of the world's internet communication flows through the United States[6], so it's easy for U.S. intelligence to deploying this approach by watching data flows around entry and exit points[7].

Another method involves "staining" data with watermarks. For example, the NSA has been known to mark network traffic by purchasing ad space from online companies like Google. The ads cause web browsers to create a cookie artifact on the user's computer which identifies the machine viewing the ad[8]. IP addresses may change but the cookie and its identifiers do not.

De-cloaking Tor users doesn't necessarily require a federal budget either. According to a couple of researchers slated to speak at Black Hat in a few weeks[9]:

> *"In our analysis, we've discovered that a persistent adversary with a handful of powerful servers and a couple gigabit links can de-anonymize hundreds of thousands Tor clients and thousands of hidden services within a couple of months. The total investment cost? Just under $3,000."*

Client Network Exploitation (CNE) Trumps Crypto

Back in 2009 security researcher Joanna Rutkowska implemented what she dubbed the "Evil Maid" attack to foil TrueCrypt's disk encryption scheme[10]. By compromising the Windows boot environment her team was able to capture the hard disk's encryption passphrase and circumvent TrueCrypt's protection. While users can [usually] defend against this sort of monkey business, by relying on a trusted boot process, the success of the Evil Maid attack underscores the capacity for subversion to trump encryption.

This type of client-side exploitation can be generalized for remote network-based operations. In a nutshell, it doesn't matter how strong your network encryption is if a spy can somehow hack your computer and steal your encryption passphrase (to decrypt your traffic) or perhaps just pilfer the data that they want outright.

Enter the NSAs QUANTUM and FOXACID tag team. QUANTUM servers have the ability to mimic web sites and subsequently re-direct user requests to a second set of FOXACID servers which infects the user's computer with malware[11]. Thanks to Ed Snowden it's now public knowledge that the NSA's goal is to industrialize this process of subversion (a system codenamed TURBINE[12]) so it can be executed on an industrial scale. Why go to the effort of decrypting Tor network traffic when spies can infect, infiltrate, and monitor millions of machine at a time?

Is it any wonder that the Kremlin has turned to old-school typewriters[13] and that German officials have actually considered a similar move[14]? In the absence of a faraday cage even tightly configured air-gapped systems can be breached using clever radio and cellular-based rootkits[15]. As one user shrewdly commented in an online post[16]:

> *"Ultimately, I believe in security. But what I believe about security leaves me far from the cutting edge; my security environment is more like bearskins and stone knives, because bearskins and stone knives are simple enough that I can *know* they won't do something I don't want them to do. Smartphones and computers simply cannot provide that guarantee. The parts of their security models that I do understand, *won't* prevent any of the things I don't want them to do."*

Software is hard to trust, there are literally thousands upon thousands of little nooks where a flaw can be "accidentally" inserted to provide a back door. Hardware is even worse.

Denouement

About a year ago John Young, the operator of the leaks site Cryptome, voiced serious concerns in a mailing list thread about the perception of security being conveyed by tools like Tor[17]:

> *"Security is deception. Comsec a trap. Natsec the mother of secfuckers"*

Jacob Appelbaum, who by the way is intimately involved with the Tor project, responded:

> *"Whatever you're smoking, I wish you'd share it with the group"*

Appelbaum's cavalier dismissal fails to appreciate the aforementioned countermeasures. What better way to harvest secrets from targets en mass than to undermine a ubiquitous technology that everyone thinks will keep them safe? Who's holding the shit-bag now? For activists engaged in work that could get them executed, relying on crypto as a universal remedy is akin to buying snake oil. John Young's stance may seem excessive to Tor promoters like Appelbaum but if Snowden's revelations have taught us anything it's that the cynical view has been spot on.

Bill Blunden is an independent investigator whose current areas of inquiry include information security, anti-forensics, and institutional analysis. He is the author of several books, including *The Rootkit Arsenal* and *Behold a Pale Farce: Cyberwar, Threat Inflation, and the Malware-Industrial Complex*. Bill is the lead investigator at Below Gotham Labs.

End Notes

[1] Cooper Quintin, "7 Things You Should Know About Tor," *Electronic Frontier Foundation*, July 1, 2014, https://www.eff.org/deeplinks/2014/07/7-things-you-should-know-about-tor

[2] 'Tor Stinks' presentation, *Guardian*, October 4, 2013, http://www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document

[3] J. Appelbaum, A. Gibson, J. Goetz, V. Kabisch, L. Kampf, L. Ryge, "NSA targets the privacy-conscious," http://daserste.ndr.de/panorama/aktuell/nsa230_page-1.html

[4]Kevin Poulsen, "FBI Admits It Controlled Tor Servers Behind Mass Malware Attack," *Wired*, September 13, 2013, http://www.wired.com/threatlevel/2013/09/freedom-hosting-fbi/

[5] Barton Gellman, Craig Timberg, and Steven Rich, "Secret NSA documents show campaign against Tor encrypted network," *Washington Post*, October 4, 2013

[6] James Ball, "NSA stores metadata of millions of web users for up to a year, secret files show," *Guardian*, September 30, 2013, http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents/print

[7] Maxim Kammerer, [tor-talk] End-to-end correlation for fun and profit, August 20, 2007, https://lists.torproject.org/pipermail/tor-talk/2012-August/025254.html

[8] Seth Rosenblatt, "NSA tracks Google ads to find Tor users," *CNET*, October 4, 2013, http://news.cnet.com/8301-1009_3-57606178-83/nsa-tracks-google-adsto-find-tor-users/

[9] Alexander Volynkin & Michael McCord, "You Don't Have to be the NSA to Break Tor: Deanonymizing Users on a Budget," *Black Hat USA 2014*, https://www.blackhat.com/us-14/briefings.html#you-dont-have-to-be-the-nsa-to-break-tor-deanonymizing-users-on-a-budget

[10] Joanna Rutkowska, "Evil Maid goes after TrueCrypt!" *Invisible Things Lab's Blog*, October 16, 2009, http://theinvisiblethings.blogspot.com/2009/10/evil-maid-goes-after-truecrypt.html

[11] Bruce Schneier, "Attacking Tor: how the NSA targets users' online anonymity," *Guardian*, October 4, 2013, http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity/print

[12] Ryan Gallagher and Glenn Greenwald, "How the NSA Plans to Infect 'Millions' of Computers with Malware," *Intercept*, March 12, 2014, https://firstlook.org/theintercept/article/2014/03/12/nsa-plans-infect-millions-computers-malware/

[13] Chris Irvine, "Kremlin returns to typewriters to avoid computer leaks," *Telegraph*, July 11, 2014, http://www.telegraph.co.uk/news/worldnews/europe/russia/10173645/Kremlin-returns-to-typewriters-to-avoid-computer-leaks.html

[14] Cyrus Farivar, "In the name of security, German NSA committee may turn to typewriters," *Ars Technica*, July 14, 2014, http://arstechnica.com/tech-policy/2014/07/in-the-name-of-security-german-nsa-committee-may-turn-to-typewriters/

[15] Jacob Appelbaum, "Shopping for Spy Gear: Catalog Advertises NSA Toolbox," *Der Spiegel*, December 29, 2013, http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html

[16] "Iron Box Security," *Cryptome*, June 6, 2014, http://cryptome.org/2014/06/iron-box-security.htm

[17] "Natsec the Mother of Secfuckers," *Cryptome*, June 9, 2013, http://cryptome.org/2013/06/nat-secfuckers.htm