Tor (anonymity network)

Tor is free software for enabling anonymous communication. The name is derived from an acronym for the original software project name "The Onion Router".[8][9] Tor directs Internet traffic through a free, worldwide, volunteer overlay network consisting of more than seven thousand relays[10] to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis. Using Tor makes it more difficult to trace Internet activity to the user: this includes "visits to Web sites, online posts, instant messages, and other communication forms".[11] The intent for Tor's use is to protect the personal privacy of its users, as well as their freedom and ability to conduct confidential communication by keeping their Internet activities from being monitored.

Tor does not prevent an online service from determining when it is being accessed through Tor. Tor protects a user's privacy, but does not hide the fact someone uses Tor. Some websites restrict allowances through Tor. For example, the MediaWiki TorBlock extension automatically restricts edits made through Tor, although Wikipedia allows some limited editing in exceptional circumstances.[12]

Onion routing is implemented by encryption in the application layer of a communication protocol stack, nested like the layers of an onion. Tor encrypts the data, including the next node destination IP address, multiple times and sends it through a virtual circuit comprising successive, random-selection Tor relays. Each relay decrypts a layer of encryption to reveal the next relay in the circuit to pass the remaining encrypted data on to it. The final relay decrypts the innermost layer of encryption and sends the original data to its destination without revealing or knowing the source IP address. Because the routing of the communication is partly concealed at every hop in the Tor circuit, this method eliminates any single point at which the communicating peers can be determined through network surveillance that relies upon knowing its source and destination.

An adversary may try to de-anonymize the user by some means. One way this may be achieved is by exploiting vulnerable software on the user's computer.[13] The NSA had a technique that targets a vulnerability – which they codenamed "EgotisticalGiraffe" – in an outdated Firefox browser version at one time bundled with the Tor package,[14] and in general, targets Tor users for close monitoring under its XKeyscore program.[15] Attacks against Tor are an active area of academic research,[16][17] and are welcomed by the Tor Project itself.[18] The bulk of the funding for Tor's development has come from the federal government of the United States,[19] initially through the Office of Naval Research and DARPA.[20]

Tor

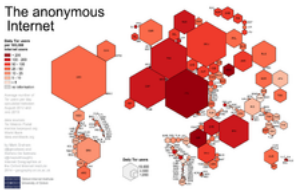
Developer(s)	The Tor Project, Inc
Initial release	20 September 2002[1]
Stable release	0.3.1.7 (18 September 2017[2]) [±] 0.3.0.11 (18 September 2017[3]) [±] 0.2.9.12 (LTS) (18 September 2017[3]) [±] 0.2.8.15 (18 September 2017[3]) [±] 0.2.5.14 (LTS) (8 June 2017[4]) [±]
Preview release	0.3.2.2-alpha (2 October 2017[5]) [±]
Repository	https://gitweb.torproject.org/tor.git
Development status	Active
Written in	C,[6] Python, Rust[7]
Operating system	Microsoft Windows · Unix-like (Android, Linux, macOS)
Size	2–4 MB
Type	Onion routing, anonymity
License	Original BSD
Website	torproject.org

Contents

History

The core principle of Tor, "onion routing", was developed in the mid-1990s by United States Naval Research Laboratory employees, mathematician Paul Syverson, and computer scientists Michael G. Reed and David Goldschlag with the purpose of protecting U.S intelligence communications online. Onion routing was further developed by DARPA in 1997.[21][22][23]

The alpha version of Tor, developed by Syverson and computer scientists Roger Dingledine and Nick Mathewson[19] and then called The Onion Routing project, or TOR project, launched on 20 September 2002.[1][24] The first public release occurred a year later.[25] On 13 August 2004, Syverson, Dingledine, and Mathewson presented "Tor: The Second-Generation Onion Router" at the 13th USENIX Security Symposium.[26] In 2004, the Naval Research Laboratory released the code for Tor under a free license, and the Electronic Frontier Foundation (EFF) began funding Dingledine and Mathewson to continue its development.[19]



A cartogram illustrating Tor usage

In December 2006, Dingledine, Mathewson, and five others founded The Tor Project, a Massachusetts-based 501(c)(3) research-education nonprofit organization responsible for maintaining Tor.[27] The EFF acted as The Tor Project's fiscal sponsor in its early years, and early financial supporters of The Tor Project included the U.S. International Broadcasting Bureau, Internews, Human Rights Watch, the University of Cambridge, Google, and Netherlands-based Stichting NLnet.[28][29][30][31][32]

From this period onward, the majority of funding sources came from the U.S. government.[19]

In November 2014 there was speculation in the aftermath of Operation Onymous that a Tor weakness had been exploited. A representative of Europol was secretive about the method used, saying: "*This is something we want to keep for ourselves. The way we do this, we can't share with the whole world, because we want to do it again and again and again.*"[33] A BBC source cited a "technical breakthrough"[34] that allowed the tracking of the physical location of servers, and the number of sites that police initially claimed to have infiltrated led to speculation that a weakness in the Tor network had been exploited. This possibility was downplayed by Andrew Lewman, a representative of the not-for-profit Tor project, suggesting that execution of more traditional police work was more likely.[35][36] However, in November 2015 court documents on the matter[37] generated serious ethical security research[38] as well as Fourth Amendment concerns.[39]

In December 2015, The Tor Project announced that it had hired Shari Steele as its new executive director.[40] Steele had previously led the Electronic Frontier Foundation for 15 years, and in 2004 spearheaded EFF's decision to fund Tor's early development. One of her key stated aims is to make Tor more user-friendly in order to bring wider access to anonymous web browsing.[41]

In July 2016 the complete board of the Tor Project resigned, and announced a new board, made up of Matt Blaze, Cindy Cohn, Gabriella Coleman, Linus Nordberg, Megan Price, and Bruce Schneier.[42][43]

Usage

Tor enables its users to surf the Internet, chat and send instant messages anonymously, and is used by a wide variety of people for both licit and illicit purposes.[47] Tor has, for example, been used by criminal enterprises, hacktivism groups, and law enforcement agencies at cross purposes, sometimes simultaneously;[48][49] likewise, agencies within the U.S. government variously fund Tor (the U.S. State Department, the National Science Foundation, and – through the Broadcasting Board of Governors, which itself partially funded Tor until October 2012 – Radio Free Asia) and seek to subvert it.[13][50]

Tor is not meant to completely solve the issue of anonymity on the web. Tor is not designed to completely erase tracks but instead to reduce the likelihood for sites to trace actions and data back to the user.[51]

Tor is also used for illegal activities, e.g., to gain access to censored information, to organize political activities,[52] or to circumvent laws against criticism of heads of state.

Tor has been described by *The Economist*, in relation to Bitcoin and Silk Road, as being "a dark corner of the web".[53] It has been targeted by the American National Security Agency and the British GCHQ signals intelligence agencies, albeit with marginal success,[13] and more successfully by the British National Crime Agency in its Operation Notarise.[54] At the same time, GCHQ has been using a tool named "Shadowcat" for "end-to-end encrypted access to VPS over SSH using the TOR network".[55][56] Tor can be used for anonymous defamation, unauthorized news leaks of sensitive information, copyright infringement, distribution of illegal sexual content,[57][58][59] selling controlled substances,[60] weapons, and stolen credit card numbers,[61] money laundering,[62] bank fraud,[63] credit card fraud, identity theft and the exchange of counterfeit currency;[64] the black market utilizes the Tor infrastructure, at least in part, in conjunction with Bitcoin.[48] It has also been used to brick IoT devices.[65]

In its complaint against Ross William Ulbricht of Silk Road, the US Federal Bureau of Investigation acknowledged that Tor has "known legitimate uses".[66][67] According to CNET, Tor's anonymity function is "endorsed by the Electronic Frontier Foundation (EFF) and other civil liberties groups as a method for whistleblowers and human rights workers to communicate with journalists".[68] EFF's Surveillance Self-Defense guide includes a description of where Tor fits in a larger strategy for protecting privacy and anonymity.[69]

In 2014, the EFF's Eva Galperin told *Business Week* magazine that "Tor's biggest problem is press. No one hears about that time someone wasn't stalked by their abuser. They hear how somebody got away with downloading child porn."[70]

The Tor Project states that Tor users include "normal people" who wish to keep their Internet activities private from websites and advertisers, people concerned about cyber-spying, users who are evading censorship such as activists, journalists, and military professionals. As of November 2013, Tor had about four million users.[71] According to the *Wall Street Journal*, in 2012 about 14% of Tor's traffic connected from the United States, with people in "Internet-censoring countries" as its second-largest user base.[72] Tor is increasingly used by victims of domestic violence and the social workers and agencies that assist them, even though shelter workers may or may not have had professional training on cybersecurity matters.[73] Properly deployed, however, it precludes digital stalking, which has increased due to the prevalence of digital media in contemporary online life.[74] Along with SecureDrop, Tor is used by news organizations such as *The Guardian*, *The New Yorker*, ProPublica and *The Intercept* to protect the privacy of whistleblowers.[75]

In March 2015 the Parliamentary Office of Science and Technology released a briefing which stated that "There is widespread agreement that banning online anonymity systems altogether is not seen as an acceptable policy option in the U.K." and that "Even if it were, there would be technical challenges." The report further noted that Tor "plays only a minor role in the online viewing and distribution of indecent images of children" (due in part to its inherent latency); its usage by the Internet Watch Foundation, the utility of its hidden services for whistleblowers, and its circumvention of the Great Firewall of China were touted.[76]

Tor's executive director, Andrew Lewman, also said in August 2014 that agents of the NSA and the GCHQ have anonymously provided Tor with bug reports.[77]

The Tor Project's FAQ offers supporting reasons for the EFF's endorsement:

Web based Hidden Services in January 2015[44]

Category	Percentage
Gambling	0.4
Guns	1.4
Chat	2.2
New (Not yet indexed)	2.2
Abuse	2.2
Books	2.5
Directory	2.5
Blog	2.75
Porn	2.75
Hosting	3.5
Hacking	4.25
Search	4.25
Anonymity	4.5
Forum	4.75
Counterfeit	5.2
Whistleblower	5.2
Wiki	5.2
Mail	5.7
Bitcoin	6.2
Fraud	9
Market	9
Drugs	15.4

Web based Hidden Services in February 2016[45][46]

Category	Percentage
Violence	0.3
Arms	0.8
Social	1.2
Hacking	1.8
Illegitimate pornography	2.3
Nexus	2.3
Extremism	2.7
Unknown	3.0
Other illicit	3.8
Finance	6.3
Drugs	8.1
Other	19.6
None	47.7

> Criminals can already do bad things. Since they're willing to break laws, they already have lots of options available that provide better privacy than Tor provides....
>
> Tor aims to provide protection for ordinary people who want to follow the law. Only criminals have privacy right now, and we need to fix that....
>
> So yes, criminals could in theory use Tor, but they already have better options, and it seems unlikely that taking Tor away from the world will stop them from doing their bad things. At the same time, Tor and other privacy measures can fight identity theft, physical crimes like stalking, and so on.
>
> — Tor Project FAQ[78]

Operation

Tor aims to conceal its users' identities and their online activity from surveillance and traffic analysis by separating identification and routing. It is an implementation of onion routing, which encrypts and then randomly bounces communications through a network of relays run by volunteers around the globe. These onion routers employ encryption in a multi-layered manner (hence the onion metaphor) to ensure perfect forward secrecy between relays, thereby providing users with anonymity in network location. That anonymity extends to the hosting of censorship-resistant content by Tor's anonymous hidden service feature.[26] Furthermore, by keeping some of the entry relays (bridge relays) secret, users can evade Internet censorship that relies upon blocking public Tor relays.[79]

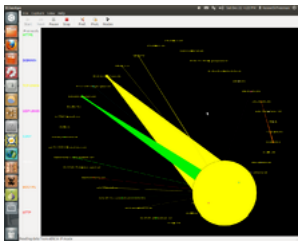
Infographic about how Tor works, by EFF

Because the IP address of the sender and the recipient are not *both* in cleartext at any hop along the way, anyone eavesdropping at any point along the communication channel cannot directly identify both ends. Furthermore, to the recipient it appears that the last Tor node (called the exit node), rather than the sender, is the originator of the communication.

Originating traffic

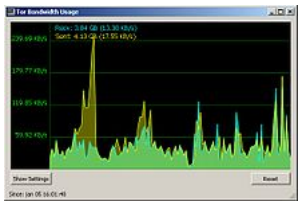
A Tor user's SOCKS-aware applications can be configured to direct their network traffic through a Tor instance's SOCKS interface. Tor periodically creates virtual circuits through the Tor network through which it can multiplex and onion-route that traffic to its destination. Once inside a Tor network, the traffic is sent from router to router along the circuit, ultimately reaching an exit node at which point the cleartext packet is available and is forwarded on to its original destination. Viewed from the destination, the traffic appears to originate at the Tor exit node.

Tor's application independence sets it apart from most other anonymity networks: it works at the Transmission Control Protocol (TCP) stream level. Applications whose traffic is commonly anonymized using Tor include Internet Relay Chat (IRC), instant messaging, and World Wide Web browsing.


A visual depiction of the traffic between some Tor relay nodes from the open-source packet sniffing program EtherApe

Hidden services

Tor can also provide anonymity to websites and other servers. Servers configured to receive inbound connections only through Tor are called hidden services. Rather than revealing a server's IP address (and thus its network location), a hidden service is accessed through its onion address, usually via the Tor Browser. The Tor network understands these addresses by looking up their corresponding public keys and *introduction points* from a distributed hash table within the network. It can route data to and from hidden services, even those hosted behind firewalls or network address translators (NAT), while preserving the anonymity of both parties. Tor is necessary to access hidden services.[80]


A Tor non-exit relay with a maximum output of 239.69 KB/s

Hidden services were first specified in 2003[81] and have been deployed on the Tor network since 2004.[82] Other than the database that stores the hidden-service descriptors,[83] Tor is decentralized by design; there is no direct readable list of all hidden services, although a number of hidden services catalog publicly known onion addresses.

Because hidden services do not use exit nodes, connection to a hidden service is encrypted end-to-end and not subject to eavesdropping. There are, however, security issues involving Tor hidden services. For example, services that are reachable through Tor hidden services *and* the public Internet are susceptible to correlation attacks and thus not perfectly hidden. Other pitfalls include misconfigured services (e.g. identifying information included by default in web server error responses), uptime and downtime statistics, intersection attacks, and user error.[83][84] The open source OnionScan program, written by independent security researcher Sarah Jamie Lewis, comprehensively examines hidden services for numerous flaws and vulnerabilities.[85]

Hidden services can also be accessed from a standard web browser without client-side connection to the Tor network, using services like Tor2web.[86] Popular sources of dark web .onion links include Pastebin, Twitter, Reddit, and other Internet forums.[87]

Arm status monitor

The anonymizing relay monitor (Arm) is a command-line status monitor written in Python for Tor.[88][89][90] This functions much like top does for system usage, providing real time statistics for:

- resource usage (bandwidth, cpu, and memory usage)
- general relaying information (nickname, fingerprint, flags, or/dir/controlports)
- event log with optional regex filtering and deduplication
- connections correlated against tor's consensus data (ip, connection types, relay details, etc.)
- torrc configuration file with syntax highlighting and validation

Most of arm's attributes are configurable through an optional armrc configuration file. It runs on any platform supported by curses including Linux, macOS, and other Unix-like variants.

The project began in the summer of 2009,[91][92] and since 18 July 2010 it has been an official part of the Tor Project. It is free software, available under the GNU General Public License


Arm's header panel and bandwidth graph.

Weaknesses

Like all current low-latency anonymity networks, Tor cannot and does not attempt to protect against monitoring of traffic at the boundaries of the Tor network (i.e., the traffic entering and exiting the network). While Tor does provide protection against traffic analysis, it cannot prevent traffic confirmation (also called *end-to-end correlation*).[93][94]

In spite of known weaknesses and attacks listed here, a 2009 study revealed that Tor and the alternative network system JonDonym (Java Anon Proxy, JAP) are considered more resilient to website fingerprinting techniques than other tunneling protocols

The reason for this is that conventional single-hop VPN protocols do not need to reconstruct packet data nearly as much as a multi-hop service like Tor or JonDonym. Website fingerprinting yielded greater than 90% accuracy for identifying HTTP packets on conventional VPN protocols versus Tor which yielded only 2.96% accuracy. However some protocols like OpenSSH and OpenVPN required a large amount of data before HTTP packets were identified.[95]

Researchers from the University of Michigan developed a network scanner allowing identification of 86% of live Tor "bridges" with a single scan.[96]

Eavesdropping

Autonomous system (AS) eavesdropping

If an autonomous system (AS) exists on both path segments from a client to entry relay and from exit relay to destination, such an AS can statistically correlate traffic on the entry and exit segments of the path and potentially infer the destination with which the client communicated. In 2012, LASTor proposed a method to predict a set of potential ASes on these two segments and then avoid choosing this path during path selection algorithm on client side. In this paper, they also improve latency by choosing shorter geographical paths between client and destination.[97]

Exit node eavesdropping

In September 2007, Dan Egerstad, a Swedish security consultant, revealed that he had intercepted usernames and passwords for e-mail accounts by operating and monitoring Tor exit nodes.[98] As Tor cannot encrypt the traffic between an exit node and the target server, any exit node is in a position to capture traffic passing through it that does not use end-to-end encryption such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS). While this may not inherently breach the anonymity of the source, traffic intercepted in this way by self-selected third parties can expose information about the source in either or both of payload and protocol data.[99] Furthermore, Egerstad is circumspect about the possible subversion of Tor by intelligence agencies:[100]

> "If you actually look in to where these Tor nodes are hosted and how big they are, some of these nodes cost thousands of dollars each month just to host because they're using lots of bandwidth, they're heavy-duty servers and so on. Who would pay for this and be anonymous?"

In October 2011, a research team from ESIEA claimed to have discovered a way to compromise the Tor network by decrypting communication passing over it.[101][102] The technique they describe requires creating a map of Tor network nodes, controlling one third of them, and then acquiring their encryption keys and algorithm seeds. Then, using these known keys and seeds, they claim the ability to decrypt two encryption layers out of three. They claim to break the third key by a statistical-based attack. In order to redirect Tor traffic to the nodes they controlled, they used a denial-of-service attack. A response to this claim has been published on the official Tor Blog stating that these rumours of Tor's compromise are greatly exaggerated.[103]

Traffic-analysis attack

Steven J. Murdoch and George Danezis from University of Cambridge presented an article at the 2005 IEEE Symposium on security and privacy on traffic-analysis techniques that allow adversaries with only a partial view of the network to infer which nodes are being used to relay the anonymous streams.[104] These techniques greatly reduce the anonymity provided by Tor. Murdoch and Danezis have also shown that otherwise unrelated streams can be linked back to the same initiator. This attack, however, fails to reveal the identity of the original user.[104] Murdoch has been working with and has been funded by Tor since 2006.

Tor exit node block

Operators of Internet sites have the ability to prevent traffic from Tor exit nodes or to offer reduced functionality to Tor users. For example, it is not generally possible to edit Wikipedia when using Tor or when using an IP address that also is used by a Tor exit node, due to the use of the TorBlock MediaWiki extension, unless an exemption is obtained. The BBC blocks the IP addresses of all known Tor guards and exit nodes from its iPlayer service - however relays and bridges are not blocked.[105]

Bad apple attack

In March 2011, researchers with the Rocquencourt French Institute for Research in Computer Science and Automation (Institut national de recherche en informatique et en automatique, INRIA), documented an attack that is capable of revealing the IP addresses of BitTorrent users on the Tor network. The "bad apple attack" exploits Tor's design and takes advantage of insecure application use to associate the simultaneous use of a secure application with the IP address of the Tor user in question. One method of attack depends on control of an exit node or hijacking tracker responses, while a secondary attack method is based in part on the statistical exploitation of distributed hash table tracking.[106] According to the study:[106]

> "This attack against Tor consists of two parts: (a) exploiting an insecure application to reveal the source IP address of, or trace, a Tor user and (b) exploiting Tor to associate the use of a secure application with the IP address of a user (revealed by the insecure application). As it is not a goal of Tor to protect against application-level attacks, Tor cannot be held responsible for the first part of this attack. However, because Tor's design makes it possible to associate streams originating from secure application with traced users, the second part of this attack is indeed an attack against Tor. We call the second part of this attack the bad apple attack. (The name of this attack refers to the saying "one bad apple spoils the bunch". We use this wording to illustrate that one insecure application on Tor may allow to trace other applications.)"

The results presented in the bad apple attack research paper are based on an attack in the wild launched against the Tor network by the authors of the study. The attack targeted six exit nodes, lasted for 23 days, and revealed a total of 10,000 IP addresses of active Tor users. This study is particularly significant because it is the first documented attack designed to target P2P file-sharing applications on Tor.[106] BitTorrent may generate as much as 40% of all traffic on Tor.[107] Furthermore, the bad apple attack is effective against insecure use of any application over Tor, not just BitTorrent.[106]

Some protocols expose IP addresses

Researchers from the French Institute for Research in Computer Science and Automation (INRIA) showed that the Tor dissimulation technique in BitTorrent can be bypassed by attackers controlling a Tor exit node. The study was conducted by monitoring six exit nodes for a period of 23 days. Researches used three attack vectors:[108]

Inspection of BitTorrent control messages
: Tracker announces and extension protocol handshakes may optionally contain client IP address. Analysis of collected data revealed that 35% and 33% of messages, respectively, contained addresses of clients.[108]:3

Hijacking trackers' responses
: Due to lack of encryption or authentication in communication between tracker and peer, typical man-in-the-middle attacks allow attackers to determine peer IP addresses and even verify the distribution of content. Such attacks work when Tor is used only for tracker communication.[108]:4

Exploiting distributed hash tables (DHT)
: This attack exploits the fact that distributed hash table (DHT) connections through Tor are impossible, so an attacker is able to reveal a target's IP address by looking it up in the DHT even if the target uses Tor to connect to other peers.[108]:4–5

With this technique, researchers were able to identify other streams initiated by users, whose IP addresses were revealed.[108]

Sniper attack

Jansen *et al.*, describe a DDoS attack targeted at the Tor node software, as well as defenses against that attack and its variants. The attack works using a colluding client and server, and filling the queues of the exit node until the node runs out of memory, and hence can serve no other (genuine) clients. By attacking a significant proportion of the exit nodes this way, an attacker can degrade the network and increase the chance of targets using nodes controlled by the attacker.[109]

Heartbleed bug

The Heartbleed OpenSSL bug disrupted the Tor network for several days in April 2014 while private keys were renewed. The Tor Project recommended that Tor relay operators and hidden service operators revoke and generate fresh keys after patching OpenSSL, but noted that Tor relays use two sets of keys and that Tor's multi-hop design minimizes the impact of exploiting a single relay.[110] 586 relays later found to be susceptible to the Heartbleed bug were taken offline as a precautionary measure.[111][112][113][114]

Mouse fingerprinting

In March 2016 a security researcher based in Barcelona, demonstrated that laboratory techniques using time measurement via JavaScript at the 1-millisecond level[115] could potentially identify and correlate a user's unique mouse movements provided that the user has visited the same "fingerprinting" website with both the Tor browser and a regular browser.[116] This proof of concept exploits the "time measurement via JavaScript" issue which has been an open ticket on the Tor Project for ten months.[117]

Circuit fingerprinting attack

In 2015, the administrators of Agora, a darknet market, announced they were taking the site offline in response to a recently discovered security vulnerability in Tor. They did not say what the vulnerability was, but Wired speculated that it was the "Circuit Fingerprinting Attack" presented at the Usenix security conference.[118][119]

Volume information

A study showed that "anonymization solutions protect only partially against target selection that may lead to efficient surveillance" as they typically "do not hide the volume information necessary to do target selection".[120]

Implementations

The main implementation of Tor is written primarily in C, along with Python, JavaScript, and several other programming languages, and consists of 540,751 lines of code as of March 2016.[6]

Tor Browser

The Tor Browser, previously known as the Tor Browser Bundle (TBB),[124] is the flagship product of the Tor Project. It consists of a modified Mozilla Firefox ESR web browser, the TorButton, TorLauncher, NoScript, and HTTPS Everywhere Firefox extensions and the Tor proxy.[125][126] Users can run the Tor Browser from removable media. It can operate under Microsoft Windows, macOS, or Linux.[127]

The Tor Browser automatically starts Tor background processes and routes traffic through the Tor network. Upon termination of a session the browser deletes privacy-sensitive data such as HTTP cookies and the browsing history.[126]

Following a series of disclosures on global surveillance, Stuart Dredge (writing in *The Guardian* in November 2013) recommended using the Tor Browser to avoid eavesdropping and retain privacy on the Internet.[128]

Firefox / JavaScript anonymity attack

In August 2013 it was discovered that the Firefox browsers in many older versions of the Tor Browser Bundle were vulnerable to a JavaScript attack, as NoScript was not enabled by default.[14] Attackers used this vulnerability to extract users' MAC and IP addresses and Windows computer names.[129][130][131] News reports linked this to a United States Federal Bureau of Investigation (FBI) operation targeting Freedom Hosting's owner, Eric Eoin Marques, who was arrested on a provisional extradition warrant issued by a United States court on 29 July. The FBI is seeking to extradite Marques out of Ireland to Maryland on four charges — distributing, conspiring to distribute, and advertising child pornography — as well as aiding and abetting advertising of child pornography. The warrant alleges that Marques is "the largest facilitator of child porn on the planet".[132][133] The FBI acknowledged the attack in a 12 September 2013 court filing in Dublin;[134] further technical details from a training presentation leaked by Edward Snowden revealed the codename for the exploit as "EgotisticalGiraffe".[135]

The FBI, in Operation Torpedo, has targeted Tor hidden servers since 2012, such as in the case of Aaron McGrath, who was sentenced to 20 years for running three hidden Tor servers containing child pornography.[136]

Tor Messenger

On 29 October 2015, the Tor Project released Tor Messenger Beta, an instant messaging program based on Instantbird with Tor and OTR built in and used by default.[137] Like Pidgin and Adium, Tor Messenger supports multiple different instant messaging protocols; however, it accomplishes this without relying on *libpurple*, implementing all chat protocols in the memory-safe language JavaScript instead.[139]

Third-party applications

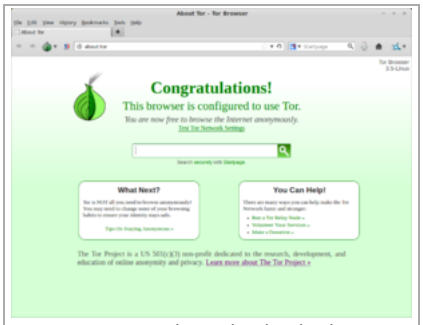
Vuze (formerly Azureus) BitTorrent client,[140] Bitmessage anonymous messaging system,[141] and TorChat instant messenger include Tor support.

The Guardian Project is actively developing a free and open-source suite of applications and firmware for the Android operating system to improve the security of mobile communications.[142] The applications include ChatSecure instant messaging client,[143] Orbot Tor implementation,[144] Orweb (discontinued) privacy-enhanced mobile browser,[145][146] Orfox, the mobile counterpart of the Tor Browser, ProxyMob Firefox add-on,[147] and ObscuraCam.[148]

Security-focused operating systems

Several security-focused operating systems like GNU/Linux distributions including Hardened Linux From Scratch, Incognito, Liberté Linux, Qubes OS, Subgraph, Tails, Tor-ramdisk, and Whonix, make extensive use of Tor.[149]

Tor Browser



Tor Browser on Linux Mint showing its start page – about:tor

Developer(s)	Tor Project
Stable release	7.0.6[121] (28 September 2017) [±]
Preview release	7.5-alpha-5[122] (28 September 2017) [±]
Development status	Active
Operating system	Windows XP and later · Unix-like (inc. macOS)
Engine	Gecko
Size	32–41 MB
Available in	16 languages[123]
Type	Onion routing, anonymity, web browser, feed reader
License	GPL
Website	www.torproject.org /projects/torbrowser.html

Tor Messenger

Developer(s)	The Tor Project

Reception, impact, and legislation

Initial release	29 October 2015[137]
Preview release	0.5.0-beta-1[138] / 28 September 2017
Repository	https://gitweb.torproject.org/tor-messenger-build.git
Development status	Active
Written in	C/C++, JavaScript, CSS, XUL
Operating system	Windows XP and later · Unix-like (inc. macOS)
Available in	English
Website	trac.torproject.org/projects/tor/wiki/doc/TorMessenger

Tor has been praised for providing privacy and anonymity to vulnerable Internet users such as political activists fearing surveillance and arrest, ordinary web users seeking to circumvent censorship, and people who have been threatened with violence or abuse by stalkers.[151][152] The U.S. National Security Agency (NSA) has called Tor "the king of high-secure, low-latency Internet anonymity",[13] and *BusinessWeek* magazine has described it as "perhaps the most effective means of defeating the online surveillance efforts of intelligence agencies around the world".[153] Other media have described Tor as "a sophisticated privacy tool",[154] "easy to use"[155] and "so secure that even the world's most sophisticated electronic spies haven't figured out how to crack it".[70]

Advocates for Tor say it supports freedom of expression, including in countries where the Internet is censored, by protecting the privacy and anonymity of users. The mathematical underpinnings of Tor lead it to be characterized as acting "like a piece of infrastructure, and governments naturally fall into paying for infrastructure they want to use".[156]

The project was originally developed on behalf of the U.S. intelligence community and continues to receive U.S. government funding, and has been criticized as "more resembl[ing] a spook project than a tool designed by a culture that values accountability or transparency".[19] As of 2012, 80% of The Tor Project's $2M annual budget came from the United States government, with the U.S. State Department, the Broadcasting Board of Governors, and the National Science Foundation as major contributors,[157] aiming "to aid democracy advocates in authoritarian states".[15] Other public sources of funding include DARPA, the U.S. Naval Research Laboratory and the Government of Sweden.[31][158] Some have proposed that the government values Tor's commitment to free speech, and uses the darknet to gather intelligence.[159] Tor also receives funding from NGOs including Human Rights Watch, and private sponsors including Reddit and Google.[160] Dingledine said that the United States Department of Defense funds are more similar to a research grant than a procurement contract. Tor executive director Andrew Lewman said that even though it accepts funds from the U.S. federal government, the Tor service did not collaborate with the NSA to reveal identities of users.[161]

Play media

A very brief animated primer on Tor pluggable transports[150] a method of accessing the anonymity network.

Critics say that Tor is not as secure as it claims,[162] pointing to U.S. law enforcement's investigations and shutdowns of Tor-using sites such as web-hosting company Freedom Hosting and online marketplace Silk Road.[19] In October 2013, after analyzing documents leaked by Edward Snowden, *The Guardian* reported that the NSA had repeatedly tried to crack Tor and had failed to break its core security, although it had had some success attacking the computers of individual Tor users.[13] *The Guardian* also published a 2012 NSA classified slide deck, entitled "Tor Stinks", which said: "We will never be able to de-anonymize all Tor users all the time", but "with manual analysis we can de-anonymize a very small fraction of Tor users".[163] When Tor users are arrested, it is typically due to human error, not to the core technology being hacked or cracked.[164] On 7 November 2014, for example, a joint operation by the FBI, ICE Homeland Security investigations and European Law enforcement agencies led to 17 arrests and the seizure of 27 sites containing 400 pages.[165] A late 2014 report by *Der Spiegel* using a new cache of Snowden leaks revealed, however, that as of 2012 the NSA deemed Tor on its own as a "major threat" to its mission, and when used in conjunction with other privacy tools such as OTR, Cspace, ZRTP, RedPhone, Tails, and TrueCrypt was ranked as "catastrophic," leading to a "near-total loss/lack of insight to target communications, presence..."[166][167]

In March 2011, The Tor Project received the Free Software Foundation's 2010 Award for Projects of Social Benefit. The citation read, "Using free software, Tor has enabled roughly 36 million people around the world to experience freedom of access and expression on the Internet while keeping them in control of their privacy and anonymity. Its network has proved pivotal in dissident movements in both Iran and more recently Egypt."[168]

In 2012, *Foreign Policy* magazine named Dingledine, Mathewson, and Syverson among its Top 100 Global Thinkers "for making the web safe for whistleblowers".[169]

In 2013, Jacob Appelbaum described Tor as a "part of an ecosystem of software that helps people regain and reclaim their autonomy. It helps to enable people to have agency of all kinds; it helps others to help each other and it helps you to help yourself. It runs, it is open and it is supported by a large community spread across all walks of life."[170]

In June 2013, whistleblower Edward Snowden used Tor to send information about PRISM to *The Washington Post* and *The Guardian*.[171]

In 2014, the Russian government offered a $111,000 contract to "study the possibility of obtaining technical information about users and users' equipment on the Tor anonymous network".[172][173]

In October 2014, The Tor Project hired the public relations firm Thomson Communications to improve its public image (particularly regarding the terms "Dark Net" and "hidden services," which are widely viewed as being problematic) and to educate journalists about the technical aspects of Tor.[174]

In June 2015, the special rapporteur from the United Nations' Office of the High Commissioner for Human Rights specifically mentioned Tor in the context of the debate in the U.S. about allowing so-called backdoors in encryption programs for law enforcement purposes[175] in an interview for *The Washington Post*.

In July 2015, the Tor Project announced an alliance with the Library Freedom Project to establish exit nodes in public libraries.[176][177] The pilot program, which established a middle relay running on the excess bandwidth afforded by the Kilton Library in Lebanon, New Hampshire, making it the first library in the U.S. to host a Tor node, was briefly put on hold when the local city manager and deputy sheriff voiced concerns over the cost of defending search warrants for information passed through the Tor exit node. Although the DHS had alerted New Hampshire authorities to the fact that Tor is sometimes used by criminals, the Lebanon Deputy Police Chief and the Deputy City Manager averred that no pressure to strong arm the library was applied, and the service was re-established on 15 September 2015.[178] U.S. Rep. Zoe Lofgren (D-Calif) released a letter on 10 December 2015, in which she asked the DHS to clarify its procedures, stating that "While the Kilton Public Library's board ultimately voted to restore their Tor relay, I am no less disturbed by the possibility that DHS employees are pressuring or persuading public and private entities to discontinue or degrade services that protect the privacy and anonymity of U.S. citizens."[179][180][181] In a 2016 interview, Kilton Library IT Manager Chuck McAndrew stressed the importance of getting libraries involved with Tor: "Librarians have always cared deeply about protecting privacy, intellectual freedom, and access to information (the freedom to read). Surveillance has a very well-documented chilling effect on intellectual freedom. It is the job of librarians to remove barriers to information."[182] The second library to host a Tor node was the Las Naves Public Library in Valencia, Spain, implemented in the first months of 2016.[183]

In August 2015, an IBM security research group, called "X-Force", put out a quarterly report that advised companies to block Tor on security grounds, citing a "steady increase" in attacks from Tor exit nodes as well as botnet traffic.[184]

In September 2015, Luke Millanta developed and released OnionView, a web service that plots the location of active Tor relay nodes onto an interactive map of the world. The project's purpose was to detail the network's size and escalating growth rate.[185][186]

In December 2015, Daniel Ellsberg (of the Pentagon Papers),[187] Cory Doctorow (of Boing Boing),[188] Snowden,[189] and artist-activist Molly Crabapple,[190] amongst others, announced their support of Tor.

In March 2016, New Hampshire state representative Keith Ammon introduced a bill[191] allowing public libraries to run privacy software. The bill specifically referenced Tor. The text was crafted with extensive input from Alison Macrina, the director of the Library Freedom Project.[192] The bill was passed by the House 268–62.[193]

Also in March 2016, the first Tor node, specifically a middle relay, was established at a library in Canada, the Graduate Resource Centre (GRC) in the Faculty of Information and Media Studies (FIMS) at the University of Western Ontario.[194] Given that the running of a Tor exit node is an unsettled area of Canadian law,[195] and that in general institutions are more capable than individuals to cope with legal pressures, Alison Macrina of the Library Freedom Project has opined that in some ways she would like to see intelligence agencies and law enforcement attempt to intervene in the event that an exit node were established.[196]

On May 16, 2016, CNN reported on the case of core Tor developer Isis Agora Lovecruft, who had fled to Germany under the threat of a subpoena by the FBI during the Thanksgiving break of the previous year. Lovecruft has legal representation from the Electronic Frontier Foundation.[197]

On December 2, 2016, *The New Yorker* reported on burgeoning digital privacy and security workshops in the San Francisco Bay Area, particularly at the hackerspace Noisebridge, in the wake of the 2016 United States presidential election; downloading the Tor browser was mentioned.[198] Also, on December 2016, Turkey has blocked the usage of Tor, together with ten of the most used VPN services in Turkey, which were popular ways of accessing banned social media sites and services.[199]

Tor (and Bitcoin) was fundamental to the operation of the darkweb marketplace AlphaBay, which was taken down in an international law enforcement operation in July 2017.[200] Despite federal claims that Tor would not shield you, however,[201] elementary operational security errors outside of the ambit of the Tor network led to the site's downfall.[202]

In August 2017 according to reportage cybersecurity firms which specialize in monitoring and researching the dark web (which rely on Tor as its infrastructure) on behalf of banks and retailers routinely share their findings with the FBI and with other law enforcement agencies "when possible and necessary" regarding illegal content. The Russian-speaking underground offering a crime-as-a-service model is regarded as being particularly robust.[203]

Improved security

Tor responded to earlier vulnerabilities listed above by patching them and improving security. In one way or another, human (user) errors can lead to detection. The Tor Project website provides best practices (instructions) on how to properly use the Tor browser. When improperly used, Tor is not secure. For example, Tor warns its users that not all traffic is protected; only the traffic routed through the Tor browser is protected. Users are also warned to use https versions of websites, not to use Tor over Tor, not to torrent with Tor, not to enable browser plugins, not to open documents downloaded through Tor while online, and to use safe bridges.[204] Users are also warned that they cannot provide their name or other revealing information in web forums over Tor and stay anonymous at the same time.[205]

Despite intelligence agencies' claims that 80% of Tor users would be de-anonymized within 6 months in the year 2013,[206] that has still not happened. In fact, as late as September 2016, FBI could not locate, de-anonymize and identify the Tor user who hacked into the email account of a staffer on Hillary Clinton's email server.[207]

The best tactic of law enforcement agencies to de-anonymize users appears to remain with Tor-relay adversaries running poisoned nodes, as well as counting on the users themselves using Tor browser improperly. E.g., downloading video through Tor browser and then opening the same file on an unprotected hard drive while online can make the users' real IP addresses available to authorities.[208]

Odds of detection

When properly used, odds of being de-anonymized through Tor are said to be extremely low. Tor project's cofounder Nick Mathewson recently explained that the problem of "Tor-relay adversaries" running poisoned nodes means that a theoretical adversary of this kind is not the network's greatest threat:

> "No adversary is truly global, but no adversary needs to be truly global," he says. "Eavesdropping on the entire Internet is a several-billion-dollar problem. Running a few computers to eavesdrop on a lot of traffic, a selective denial of service attack to drive traffic to your computers, that's like a tens-of-thousands-of-dollars problem." At the most basic level, an attacker who runs two poisoned Tor nodes—one entry, one exit—is able to analyse traffic and thereby identify the tiny, unlucky percentage of users whose circuit happened to cross both of those nodes. At present the Tor network offers, out of a total of around 7,000 relays, around 2,000 guard (entry) nodes and around 1,000 exit nodes. So the odds of such an event happening are one in two million (1/2000 x 1/1000), give or take.[206]

Tor does not provide protection against end-to-end timing attacks: if an attacker can watch the traffic coming out of the target computer, and also the traffic arriving at the target's chosen destination (e.g. a server hosting a .onion site), he can use statistical analysis to discover that they are part of the same circuit.[205]

Levels of security

Depending on individual user needs, Tor browser offers Three levels of security located under Onion tab > Security Settings. In addition to encrypting the data, including constantly changing IP address through a virtual circuit comprising successive, randomly selected Tor relays, several other layers of security are at user's disposal:

1. Low (default) – at this security level, all browser features are enabled.

– This level provides the most usable experience, and the lowest level of security

2. Medium – at this security level, the following changes apply:

– HTML5 video and audio media become click-to-play via NoScript.

– On sites where JavaScript is enabled, performance optimizations are disabled. Scripts on some sites may run slower

– Some mechanisms of displaying math equations are disabled.

– Some font rendering features are disabled.

– JavaScript is disabled by default on all non-HTTPS sites.

3. High – at this security level, the following changes apply:

– HTML5 video and audio media become click-to-play via NoScript.

– On sites where JavaScript is enabled, performance optimizations are disabled. Scripts on some sites may run slower

– Some mechanisms of displaying math equations are disabled.

– Some font rendering features are disabled.

– JavaScript is disabled by default on all sites.

– Some types of images are disabled.

– Some fonts and icons may display incorrectly

See also

- .onion
- Anonymous P2P
- Anonymous web browsing

- Crypto-anarchism
- Darknet
- Dark web
- Deep web (search indexing)
- Freedom of information
- Freenet
- GNUnet
- I2P
- Internet censorship
- Internet censorship circumvention
- Internet privacy
- Privoxy
- Proxy server
- Psiphon
- Sandbox (computer security)
- Tor2web

Footnotes

1. Dingledine, Roger (20 September 2002). "Pre-alpha: run an onion proxy now!" (http://archives.seul.org/or/dev/Sep-2002/msg00019.html). *or-dev* (Mailing list). Retrieved 17 July 2008.
2. { {cite web |url=https://blog.torproject.org/tor-0317-now-released |title=Tor 0.3.1.7 is now released! |first=Nick |last=Mathewson |website=nickm's blog |publisher=The Tor Project |date=18 September 2017 |accessdate=18 September 2017}}
3. Mathewson, Nick (18 September 2017). "New Tor stable releases (0.2.8.15, 0.2.9.12, 0.3.0.11) with fix for onion service security issue" (https://blog.torproject.org/new-tor-stable-releases-02815-02912-03011-fix-onion-service-security-issue). *nickm's blog*. The Tor Project. Retrieved 18 September 2017.
4. Mathewson, Nick (8 June 2017). "Tor 0.3.0.8 is released, with security fixes for hidden services. (As are 0.2.4.29, 0.2.5.14, 0.2.6.12, 0.2.7.8, 0.2.8.14, and 0.2.9.11)" (https://lists.torproject.org/pipermail/tor-announce/2017-June/000131.html). *tor-announce* (Mailing list). Retrieved 10 June 2017.
5. Lovecruft, Isis Agora (2 October 2017). "Tor 0.3.2.2-alpha is released!" (https://blog.torproject.org/tor-0322-alpha-released). *isis's blog*. The Tor Project. Retrieved 6 October 2017.
6. "Tor" (https://www.openhub.net/p/tor). *Open HUB*. Retrieved 20 September 2014.
7. Hahn, Sebastian (2017-03-31). "[tor-dev] Tor in a safer language: Network team update from Amsterdam" (https://lists.torproject.org/pipermail/tor-dev/2017-March/012088.html). Retrieved 2017-04-01.
8. Li, Bingdong; Erdin, Esra; Güneş, Mehmet Hadi; Bebis, George; Shipley, Todd (14 June 2011). "An Analysis of Anonymity Usage". In Domingo-Pascual, Jordi; Shavitt, Yuval; Uhlig, Steve. *Traffic Monitoring and Analysis: Third International Workshop, TMA 2011, Vienna, Austria, April 27, 2011, Proceedings* (https://books.google.com/books?id=f7CPGTclfc8C&pg=PA113). Berlin: Springer-Verlag. pp. 113–116. ISBN 978-3-642-20304-6. Retrieved 6 August 2012.
9. "Tor Project: FAQ" (https://www.torproject.org/docs/faq#WhyCalledTor). *www.torproject.org*. Retrieved 18 January 2016.
10. "Tor Network Status" (http://torstatus.blutmagie.de/) Retrieved 14 January 2016.
11. Glater, Jonathan D. (25 January 2006). "Privacy for People Who Don't Show Their Navels" (https://www.nytimes.com/2006/01/25/technology/techspecial2/25privacy.html?_r=1). *The New York Times*. Retrieved 13 May 2011.
12. PATRICK KINGSLEY (June 10, 2017). "Turks Click Away, but Wikipedia Is Gone" (https://www.nytimes.com/2017/06/10/world/europe/turkey-wikipedia-ban-recep-tayyip-erdogan.html). The New York Times. Retrieved June 11, 2017.
13. Ball, James; Schneier, Bruce; Greenwald, Glenn (4 October 2013). "NSA and GCHQ target Tor network that protects anonymity of web users" (https://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption) *The Guardian*. Retrieved 5 October 2013.
14. "Peeling back the layers of Tor with Egotistical Giraffe" (https://www.theguardian.com/world/interactive/2013/oct/04/egotistical-giraffe-nsa-tor-document) *The Guardian*. 4 October 2013. Retrieved 5 October 2013.
15. J. Appelbaum, A. Gibson, J. Goetz, V. Kabisch, L. Kampf, L. Ryge (3 July 2014). "NSA targets the privacy-conscious" (http://daserste.ndr.de/panorama/aktuell/nsa230_page-1.html). *Panorama*. Norddeutscher Rundfunk Retrieved 4 July 2014.
16. Goodin, Dan (22 July 2014). "Tor developers vow to fix bug that can unclak users" (https://arstechnica.com/security/2014/07/tor-developers-vow-to-fix-bug-that-can-uncloak-users/). *Ars Technica*.
17. "Selected Papers in Anonymity" (http://freehaven.net/anonbib/#2014) *Free Haven*.
18. "Tor Research Home" (https://research.torproject.org/) *torproject.org*.
19. Levine, Yasha (16 July 2014). "Almost everyone involved in developing Tor was (or is) funded by the US government" (http://pando.com/2014/07/16/tor-spooks/) *Pando Daily*. Retrieved 21 April 2016.
20. "Onion Routing: Our Sponsors" (https://www.onion-router.net/Sponsors.html) *www.onion-router.net*. Retrieved 17 August 2017.
21. Fagoyinbo, Joseph Babatunde (28 May 2013). *The Armed Forces: Instrument of Peace, Strength, Development and Prosperity* (https://books.google.com/books?id=qM0uxPH8RasC&printsec=frontcover&dq=The+Armed+Forces:+Instrument+of+Peace,+Strength,+Development+and+Prosperity&hl=en&sa=X&ei=_-oVKD1J8uMyAS41IGYCA&ved=0CCoQ6AEwAA#v=onepage&q=The%20Armed%20Forces%3A%20Instrument%20of%20Peace%2C%20Strength%2C%20Development%20and%20Prosperity&f=false). AuthorHouse. ISBN 978-1-4772-2647-6. Retrieved 29 August 2014.
22. Leigh, David; Harding, Luke (8 February 2011). *WikiLeaks: Inside Julian Assange's War on Secrecy* (https://books.google.com/books?id=qGLjvFNuaM4C&printsec=frontcover&dq=WikiLeaks:+Inside+Julian+Assange%27s+War+on+Secrecy&hl=en&sa=X&ei=gesAVP36NNGPyATnhYLoCQ&ved=0CB8Q6AEwAA#v=onepage&q=WikiLeaks%3A%20Inside%20Julian%20Assange%27s%20War%20on%20Secrecy&f=false) PublicAffairs. ISBN 978-1-61039-062-0. Retrieved 29 August 2014.
23. Ligh, Michael; Adair, Steven; Hartstein, Blake; Richard, Matthew (29 September 2010). *Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code* (https://books.google.com/books?id=PFGeIEx41T4C&lpg=PP1&dq=Malware%20Analyst%27s%20Cookbook%20and%20DVD%3A%20Tools%20and%20Techniques&pg=PP1#v=onepage&q=Malware%20Analyst%27s%20Cookbook%20and%20DVD:%20Tools%20and%20Techniques&f=false) John Wiley & Sons. ISBN 978-1-118-00336-7. Retrieved 29 August 2014.
24. "Tor FAQ: Why is it called Tor?" (https://www.torproject.org/docs/faq#WhyCalledTor). *Tor Project*. Retrieved 1 July 2011.
25. Dingledine, Rogert. "Tor is free" (https://lists.torproject.org/pipermail/tor-dev/2003-October/002185.html) *Tor-dev Mail List*. Tor Project. Retrieved 23 September 2016.
26. Dingledine, Roger; Mathewson, Nick; Syverson, Paul (13 August 2004). "Tor: The Second-Generation Onion Router" (http://www.usenix.org/events/sec04/tech/dingledine.html). *Proc. 13th USENIX Security Symposium*. San Diego, California Retrieved 17 November 2008.
27. "Tor Project: Core People" (https://www.torproject.org/about/corepeople). *Tor Project*. Retrieved 17 July 2008.
28. "Tor Project Form 990 2008" (https://www.torproject.org/about/findoc/2008TorProject-Form990.pdf) (PDF). *Tor Project*. 2009. Retrieved 30 August 2014.
29. "Tor Project Form 990 2007" (https://www.torproject.org/about/findoc/2007TorProject-Form990.pdf) (PDF). *Tor Project*. 2008. Retrieved 30 August 2014.
30. "Tor Project Form 990 2009" (https://www.torproject.org/about/findoc/2009TorProject-Form990andPC.pdf) (PDF). *Tor Project*. 2010. Retrieved 30 August 2014.
31. "Tor: Sponsors" (https://www.torproject.org/about/sponsors.html.en). *Tor Project*. Retrieved 11 December 2010.
32. Krebs, Brian (8 August 2007). "Attacks Prompt Update for 'Tor' Anonymity Network" (http://voices.washingtonpost.com/securityfix/2007/08/attacks_prompt_update_for_tor.html). *Washington Post*. Retrieved 27 October 2007.
33. Greenberg, Andy (7 November 2014). "Global Web Crackdown Arrests 17, Seizes Hundreds Of Dark Net Domains" (https://www.wired.com/2014/11/operation-onymous-dark-web-arrests) *Wired*. Retrieved 9 August 2015.
34. Wakefield, Jane (7 November 2014). "Huge raid to shut down 400-plus dark net sites –" (http://www.bbc.co.uk/news/technology-29950946). *BBC News*. Retrieved 9 August 2015.
35. O'Neill, Patrick Howell (7 November 2014). "The truth behind Tor's confidence crisis" (http://www.dailydot.com/politics/tor-crisis-of-confidence/). *The Daily Dot*. Retrieved 10 November 2014.
36. Knight, Shawn (7 November 2014). "Operation Onymous seizes hundreds of darknet sites, 17 arrested globally" (http://www.techspot.com/news/58751-operation-onymous-seizes-hundreds-darknet-sites-17-arrested.html) *Techspot*. Retrieved 8 November 2014.
37. "Court Docs Show a University Helped FBI Bust Silk Road 2, Child Porn Suspects" (http://motherboard.vice.com/read/court-docs-show-a-university-helped-fbi-bust-silk-road-2-child-porn-suspects) *Motherboard*. 11 November 2015. Retrieved 20 November 2015.
38. "Did the FBI Pay a University to Attack Tor Users?" (https://blog.torproject.org/blog/did-fbi-pay-university-attack-tor-users) *torproject.org*. 11 November 2015. Retrieved 20 November 2015.
39. Zorz, Zeljka (12 November 2015). "Tor Project claims FBI paid university researchers $1m to unmask Tor users" (http://www.net-security.org/secworld.php?id=19097) *Help Net Security*. Retrieved 20 November 2015.
40. "Announcing Shari Steele as our new executive director" (https://blog.torproject.org/blog/announcing-shari-steele-our-new-executive-director) *torproject.org*. 11 November 2015. Retrieved 12 December 2015.
41. Detsch, Jack (8 April 2016). "Tor aims to grow amid national debate over digital privacy: The Tor Project's new executive director Shari Steele is on a mission to change the image of the group's anonymous browser and make its 'clunky and hard to use' technology more user-friendly" (http://www.csmonitor.com/World/Passcode/2016/0408/Tor-aims-to-grow-amid-national-debate-over-digital-privacy) *The Christian Science Monitor*. Retrieved 9 May 2016.
42. "Tor Project installs new board of directors after Jacob Appelbaum controversy" (https://www.theverge.com/2016/7/13/12176262/tor-project-new-board-members-announced), Colin Lecher, July 13, 2016, The Verge
43. "The Tor Project Elects New Board of Directors" (https://blog.torproject.org/blog/tor-project-elects-new-board%C2%A0-directors) July 13th, 2016, Tor.org
44. Owen, Gareth. "Dr Gareth Owen: Tor: Hidden Services and Deanonymisation" (https://www.youtube.com/watch?v=-oTEoLB-ses&t=1998). Retrieved 20 June 2015.
45. Moore, Daniel. "Cryptopolitik and the Darknet" (http://www.tandfonline.com/doi/abs/10.1080/00396338.2016.1142085) *Survival: Global Politics and Strategy* Retrieved 20 March 2016.

46. Cox, Joseph (1 February 2016). "Study Claims Dark Web Sites Are Most Commonly Used for Crime" (https://motherboard.vice.com/read/study-claims-dark-web-sites-are-most-commonly-used-for-crime) Retrieved 20 March 2016.
47. Zetter, Kim (17 May 2005). "Tor Torches Online Tracking" (http://archive.wired.com/politics/security/news/2005/05/67542?currentPage=all) *Wired*. Retrieved 30 August 2014.
48. Gregg, Brandon (30 April 2012). "How online black markets work" (http://www.csoonline.com/article/705316/how-online-black-markets-work) *CSO Online*. Retrieved 6 August 2012.
49. Morisy, Michael (8 June 2012). "Hunting for child porn, FBI stymied by Tor undernet" (http://www.muckrock.com/news/archives/2012/jun/08/hunting-child-porn-fbi-stymied-tor-undernet/). *Muckrock*. Retrieved 6 August 2012.
50. Lawrence, Dune (23 January 2014). "The Inside Story of Tor, the Best Internet Anonymity Tool the Government Ever Built" (http://www.businessweek.com/articles/2014-01-23/tor-anonymity-software-vs-dot-the-national-security-agency) *Bloomberg Businessweek*. Retrieved 28 April 2014.
51. "Tor: Overview" (https://www.torproject.org/about/overview.html.en). *The Tor Project*.
52. Cochrane, Nate (2 February 2011). "Egyptians turn to Tor to organise dissent online" (http://www.scmagazine.com.au/News/246707,egyptians-turn-to-tor-to-organise-dissent-online.aspx). *SC Magazine*. Retrieved 10 December 2011.
53. "Bitcoin: Monetarists Anonymous" (http://www.economist.com/node/21563752) *The Economist*. 29 September 2012 Retrieved 19 May 2013.
54. Boiten, Eerke; Hernandez-Castro, Julio (28 July 2014). "Can you really be identified on Tor or is that just what the cops want you to believe?" (http://phys.org/news/2014-07-tor-cops.html). *Phys.org*.
55. "JTRIG Tools and Techniques" (https://firstlook.org/theintercept/document/2014/07/14/jtrig-tools-techniques/) *The Intercept*. 14 July 2014.
56. "Document from an internal GCHQ wiki lists tools and techniques developed by the Joint Threat Research Intelligence Group" (https://www.documentcloud.org/documents/1217406-jtrigall.html#document/p4gz) *documentcoud.org*. 5 July 2012. Retrieved 30 July 2014.
57. Bode, Karl (12 March 2007). "Cleaning up Tor" (http://www.broadbandreports.com/shownews/Cleaning-Up-Tor-82218). *Broadband.com*. Retrieved 28 April 2014.
58. Jones, Robert (2005). *Internet forensics*. O'Reilly. p. 133. ISBN 0-596-10006-X.
59. Chen, Adrian (11 June 2012). "'Dark Net' Kiddie Porn Website Stymies FBI Investigation" (http://gawker.com/5916994/dark-net-kiddie-porn-website-stymies-fbi-investigation). *Gawker*. Retrieved 6 August 2012.
60. Chen, Adrian (1 June 2011). "The Underground Website Where You Can Buy Any Drug Imaginable" (https://web.archive.org/web/20110603015735/http://gawker.com/5805928/the-underground-website-where-you-can-buy-any-drug-imaginable) *Gawker*. Archived from the original (http://gawker.com/5805928/the-underground-website-where-you-can-buy-any-drug-imaginable) on 3 June 2011. Retrieved 20 April 2012.
61. Steinberg, Joseph (8 January 2015). "How Your Teenage Son or Daughter May Be Buying Heroin Online" (https://www.forbes.com/sites/josephsteinberg/2015/01/08/how-your-children-can-buy-illegal-drugs-online/) *Forbes*. Retrieved 6 February 2015.
62. Goodin, Dan (16 April 2012). "Feds shutter online narcotics store that used TOR to hide its tracks" (https://arstechnica.com/tech-policy/news/2012/04/feds-shutter-online-narcotics-store-that-used-tor-to-hide-its-tracks.ars?src=fbk) *Ars Technica*. Retrieved 20 April 2012.
63. "Treasury Dept: Tor a Big Source of Bank Fraud" (http://krebsonsecurity.com/2014/12/treasury-dept-tor-a-big-source-of-bank-fraud/) *Krebs on Security*. 5 December 2014.
64. Farivar, Cyrus (3 April 2015). "How a $3.85 latte paid for with a fake $100 bill led to counterfeit kingpin's downfall" (https://arstechnica.com/tech-policy/2015/04/how-a-3-85-latte-paid-for-with-a-fake-100-bill-lead-to-counterfeit-kingpins-downfall/) *Ars Technica*. Retrieved 19 April 2015.
65. Cimpanu, Catalin (2017-04-06). "New Malware Intentionall Bricks IoT Devices" (https://www.bleepingcomputer.com/news/security/new-malware-intentionally-bricks-iot-devices/). *BleepingComputer*.
66. Turner, Serrin (27 September 2013). "Sealed compaint" (https://web.archive.org/web/20131002221530/http://www1.icsi.berkeley.edu/~nweaver/UlbrichtCriminalComplaint.pdf) (PDF). *United States of America v Ross William Ulbricht*. Archived from the original (http://www1.icsi.berkeley.edu/~nweaver/UlbrichtCriminalComplaint.pdf) (PDF) on 2 October 2013.
67. Higgins, Parker (3 October 2013). "In the Silk Road Case, Don't Blame the Technology" (https://www.eff.org/deeplinks/2013/10/silk-road-case-dont-blame-technology). *Electronic Frontier Foundation* Retrieved 22 December 2013.
68. Soghoian, Chris (16 September 2007). "Tor anonymity server admin arrested" (http://news.cnet.com/8301-13739_3-9779225-46.html) *CNET News*. Retrieved 17 January 2011.
69. "Surveillance Self-Defense: Tor" (https://ssd.eff.org/tech/tor). *Electronic Frontier Foundation*. Retrieved 28 April 2014.
70. Harris, Shane; Hudson, John (4 October 2014). "Not Even the NSA Can Crack the State Department's Favorite Anonymous Service" (http://thecable.foreignpolicy.com/posts/2013/10/04/not_even_the_nsa_can_crack_the_state_departments_online_anonymity_tool). *Foreign Policy*. Retrieved 30 August 2014.
71. Dredge, Stuart (5 November 2013). "What is Tor? A beginner's guide to the privacy tool" (https://www.theguardian.com/technology/2013/nov/05/tor-beginners-guide-nsa-browser). *The Guardian*. Retrieved 30 August 2014.
72. Fowler, Geoffrey A. (17 December 2012). "Tor: An Anonymous, And Controversial, Way to Web-Surf" (https://online.wsj.com/news/articles/SB10001424127887324677204578185382377144280) *The Wall Street Journal*. Retrieved 30 August 2014.
73. Tveten, Julianne (2017-04-12). "Where Domestic Violence and Cybersecurity Intersect" (https://rewire.news/article/2017/04/12/domestic-violence-cybersecurity-intersect/). *Rewire*. Retrieved 2017-08-09.
74. LeVines, George (7 May 2014). "As domestic abuse goes digital, shelters turn to counter-surveillance with Tor" (http://betaboston.com/news/2014/05/07/as-domestic-abuse-goes-digital-shelters-turn-to-counter-surveillance-with-tor/) *Boston Globe*. Retrieved 8 May 2014.
75. Ellis, Justin (5 June 2014). "The Guardian introduces SecureDrop for document leaks" (http://www.niemanlab.org/2014/06/the-guardian-introduces-securedrop-for-document-leaks/). *Nieman Journalism Lab*. Retrieved 30 August 2014.
76. O'Neill, Patrick Howell (9 March 2015). "U.K. Parliament says banning Tor is unacceptable and impossible" (http://www.dailydot.com/politics/uk-briefing-tor-child-abuse-minor-role/). *The Daily Dot*. Retrieved 19 April 2015.
77. Kelion, Leo (22 August 2014). "NSA and GCHQ agents 'leak Tor bugs', alleges developer" (http://www.bbc.com/news/technology-28886462). *BBC News*.
78. "Doesn't Tor enable criminals to do bad things?" (https://www.torproject.org/docs/faq-abuse.html.en#WhatAboutCriminals) *Tor Project*. Retrieved 28 August 2013.
79. "Tor: Bridges" (https://www.torproject.org/docs/bridges) *Tor Project*. Retrieved 9 January 2011.
80. "Configuring Hidden Services for Tor" (https://www.torproject.org/docs/tor-hidden-service). *Tor Project*. Retrieved 9 January 2011.
81. Mathewson, Nick. "Add first draft of rendezvous point document" (https://gitweb.torproject.org/tor.git/commit/?id=3d538f6d7029372e3bec33b3bdd62f9fba9d2a3). *Tor Source Code*. Retrieved 23 September 2016.
82. Øverlier, Lasse; Syverson, Paul (21 June 2006). "Locating Hidden Servers" (http://www.onion-router.net/Publications/locating-hidden-servers.pdf) (PDF). *Proceedings of the 2006 IEEE Symposium on Security and Privacy*. IEEE Symposium on Security and Privacy (http://www.ieee-security.org/TC/SP-Index.html). Oakland, CA: IEEE CS Press. p. 1. doi:10.1109/SP.2006.24 (https://doi.org/10.1109%2FSP.2006.24). ISBN 0-7695-2574-1. Retrieved 9 November 2013.
83. "Tor: Hidden Service Protocol, Hidden services" (https://www.torproject.org/docs/hidden-services.html) *Tor Project*. Retrieved 9 January 2011.
84. Goodin, Dan (10 September 2007). "Tor at heart of embassy passwords leak" (https://www.theregister.co.uk/2007/09/10/misuse_of_tor_led_to_embassy_password_breach/). *The Register*. Retrieved 20 September 2007.
85. Cox, Joseph (2016-04-06). "A Tool to Check If Your Dark Web Site Really Is Anonymous: 'OnionScan' will probe dark web sites for security weaknesses" (https://motherboard.vice.com/en_us/article/kb7bg3/onionscan-checks-if-your-dark-web-site-really-is-anonymous) *Motherboard*. Retrieved 2017-07-07.
86. Zetter, Kim (12 December 2008). "New Service Makes Tor Anonymized Content Available to All" (https://www.wired.com/threatlevel/2008/12/tor-anonymized/). *Wired*. Retrieved 22 February 2014.
87. Koebler, Jason (23 February 2015). "The Closest Thing to a Map of the Dark Net: Pastebin" (http://motherboard.vice.com/read/the-closest-thing-to-a-map-of-the-dark-net-pastebin). *Motherboard*. Retrieved 14 July 2015.
88. "ARM Official Website" (https://www.atagar.com/arm/).
89. "Tor Project: Arm" (https://www.torproject.org/projects/arm.html.en). *torproject.org*.
90. "Ubuntu Manpage: arm – Terminal Tor status monitor" (http://manpages.ubuntu.com/manpages/precise/man1/arm.1.html) *Ubuntu.com*.
91. "Summer Conclusion (ARM Project)" (https://blog.torproject.org/blog/summer-conclusion-arm-project) *torproject.org*. Retrieved 19 April 2015.
92. "Interview with Damien Johnson by Brenno Winter" (https://www.atagar.com/arm/resources/HFM_INT_0001.mp3) *atagar.com*. Retrieved 4 June 2016.
93. Dingledine, Roger (18 February 2009). "One cell is enough to break Tor's anonymity" (https://blog.torproject.org/blog/one-cell-enough) *Tor Project*. Retrieved 9 January 2011.
94. "TheOnionRouter/TorFAQ" (https://wiki.torproject.org/noreply/TheOnionRouter/TorFAQ?action=recall&rev=554#EntryGuards) Retrieved 18 September 2007. "Tor (like all current practical low-latency anonymity designs) fails when the attacker can see both ends of the communications channel"
95. Herrmann, Dominik; Wendolsky, Rolf; Federrath, Hannes (13 November 2009). "Website Fingerprinting: Attacking Popular Privacy Enhancing Technologies with the Multinomial Naïve-Bayes Classifier" (http://epub.uni-regensburg.de/11919/1/authorsversion-ccsw09.pdf) (PDF). *Proceedings of the 2009 ACM Cloud Computing Security Workshop (CCSW)*. Cloud Computing Security Workshop. New York, USA: Association for Computing Machinery Retrieved 2 September 2010.
96. Judge, Peter (20 August 2013). "Zmap's Fast Internet Scan Tool Could Spread Zero Days In Minutes" (http://www.techweekeurope.co.uk/news/zmap-internet-scan-zero-day-125374). *TechWeek Europe*. Retrieved 28 April 2014.
97. Akhoondi, Masoud; Yu, Curtis; Madhyastha, Harsha V. (May 2012). *LASTor: A Low-Latency AS-Aware Tor Client* (http://lastor.cs.ucr.edu/oakland12.pdf) (PDF). IEEE Symposium on Security and Privacy Oakland, USA. Retrieved 28 April 2014.
98. Zetter, Kim (10 September 2007). "Rogue Nodes Turn Tor Anonymizer Into Eavesdropper's Paradise" (https://www.wired.com/politics/security/news/2007/09/embassy_hacks?currentPage=all) *Wired*. Retrieved 16 September 2007.
99. Lemos, Robert (8 March 2007). "Tor hack proposed to catch criminals" (http://www.securityfocus.com/news/11447) *SecurityFocus*.
100. Gray, Patrick (13 November 2007). "The hack of the year" (http://www.smh.com.au/news/security/the-hack-of-the-year/2007/11/12/1194766589522.html?page=fullpage#contentSwap2). *Sydney Morning Herald* Retrieved 28 April 2014.

101. "Tor anonymizing network compromised by French researchers" (http://thehackernews.com/2011/10/tor-anonymizing-network-compromised-by.html). *The Hacker News*. 24 October 2011. Retrieved 10 December 2011.
102. "Des chercheurs Francais cassent le reseau d'anonymisation Tor" (http://pro.01net.com/editorial/544024/des-chercheurs-francais-cassent-le-reseau-danonymisation-tor/) *01net.com* (in French). Retrieved 17 October 2011.
103. phobos (24 October 2011). "Rumors of Tor's compromise are greatly exaggerated" (https://blog.torproject.org/blog/rumors-tors-compromise-are-greatly-exaggerated) *Tor Project*. Retrieved 20 April 2012.
104. Murdoch, Steven J.; Danezis, George (19 January 2006). "Low-Cost Traffic Analysis of Tor" (http://www.cl.cam.ac.uk/~sjm217/papers/oakland05torta.pdf) (PDF). Retrieved 21 May 2007.
105. "BBC iPlayer Help - Why does BBC iPlayer think I'm outside the UK?" (https://www.bbc.co.uk/iplayer/help/troubleshooting/tv-games-consoles/in_the_uk_message) *www.bbc.co.uk*. Retrieved 2017-09-10.
106. Le Blond, Stevens; Manils, Pere; Chaabane, Abdelberi; Ali Kaafar, Mohamed; Castelluccia, Claude; Legout, Arnaud; Dabbous, Walid (March 2011). *One Bad Apple Spoils the Bunch: Exploiting P2P Applications to Trace and Profile Tor Users* (https://www.usenix.org/events/leet11/tech/full_papers/LeBlond.pdf) (PDF). 4th USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET '11). National Institute for Research in Computer Science and Control. Retrieved 13 April 2011.
107. McCoy, Damon; Bauer, Kevin; Grunwald, Dirk; Kohno, Tadayoshi; Sicker, Douglas (2008). "Shining Light in Dark Places: Understanding the Tor Network" (http://www.cs.washington.edu/homes/yoshi/papers/Tor/PETS2008_37.pdf) (PDF). *Proceedings of the 8th International Symposium on Privacy Enhancing Technologies*. 8th International Symposium on Privacy Enhancing Technologies. Berlin, Germany: Springer-Verlag. pp. 63–76. doi:10.1007/978-3-540-70630-4_5 (https://doi.org/10.1007%2F978-3-540-70630-4_5) ISBN 978-3-540-70629-8.
108. Manils, Pere; Abdelberri, Chaabane; Le Blond, Stevens; Kaafar, Mohamed Ali; Castelluccia, Claude; Legout, Arnaud; Dabbous, Walid (April 2010). *Compromising Tor Anonymity Exploiting P2P Information Leakage* (http://hal.inria.fr/docs/00/47/15/56/PDF/TorBT.pdf) (PDF). 7th USENIX Symposium on Network Design and Implementation. arXiv:1004.1461 (https://arxiv.org/abs/1004.1461). Bibcode:2010arXiv1004.1461M (http://adsabs.harvard.edu/abs/2010arXiv1004.1461M).
109. Jansen, Rob; Tschorsch, Florian; Johnson, Aaron; Scheuermann, Björn (2014). *The Sniper Attack: Anonymously Deanonymizing and Disabling the Tor Network* (http://www.robgjansen.com/publications/sniper-ndss2014.pdf) (PDF). 21st Annual Network & Distributed System Security Symposium. Retrieved 28 April 2014.
110. Dingledine, Roger (7 April 2014). "OpenSSL bug CVE-2014-0160" (https://blog.torproject.org/blog/openssl-bug-cve-2014-0160) *Tor Project*. Retrieved 28 April 2014.
111. Dingledine, Roger (16 April 2014). "Rejecting 380 vulnerable guard/exit keys" (https://lists.torproject.org/pipermail/tor-relays/2014-April/004336.html) *tor-relays* (Mailing list). Retrieved 28 April 2014.
112. Lunar (16 April 2014). "Tor Weekly News — 16 April 2014" (https://blog.torproject.org/blog/tor-weekly-news-%E2%80%94-april-16th-2014) *Tor Project*. Retrieved 28 April 2014.
113. Gallagher, Sean (18 April 2014). "Tor network's ranks of relay servers cut because of Heartbleed bug" (https://arstechnica.com/security/2014/04/tor-networks-ranks-of-relay-servers-cut-because-of-heartbleed-bug/) *Ars Technica*. Retrieved 28 April 2014.
114. Mimoso, Michael (17 April 2014). "Tor begins blacklisting exit nodes vulnerable to Heartbleed" (http://threatpost.com/tor-begins-blacklisting-exit-nodes-vulnerable-to-heartbleed/105519). *Threat Post*. Retrieved 28 April 2014.
115. Cimpanu, Catalin (10 March 2016). "Tor Users Can Be Tracked Based on Their Mouse Movements" (http://news.softpedia.com/news/tor-users-can-be-tracked-based-on-their-mouse-movements-501602.shtml) *Softpedia*. Retrieved 11 March 2016.
116. Garanich, Gleb (10 March 2016). "Click bait: Tor users can be tracked by mouse movements" (https://www.rt.com/viral/335112-tor-mouse-movements-fingerprint/) *Reuters*. Retrieved 10 March 2016.
117. Anonymous (10 March 2016). "Tor Users Can Be Tracked Based On Their Mouse Movements" (http://news.slashdot.org/story/16/03/11/0045203/tor-users-can-be-tracked-based-on-their-mouse-movements) *Slashdot*. Retrieved 11 March 2016.
118. Greenberg, Andy. "Agora, the Dark Web's Biggest Drug Market, Is Going Offline" (https://www.wired.com/2015/08/agora-dark-websbiggest-drug-market-going-offline/). *wired.com*. Retrieved 13 September 2016.
119. https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-kwon.pdf
120. "The Economics of Mass Surveillance and the Questionable Value of Anonymous Communications" (http://www.econinfosec.org/archive/weis2006/docs/36.pdf) (PDF). Retrieved 4 January 2017.
121. Vigier, Nicolas (28 September 2017). "Tor Browser 7.0.6 is released" (https://blog.torproject.org/tor-browser-706-released) *boklm's blog*. Tor Project. Retrieved 6 October 2017.
122. Vigier, Nicolas (28 September 2017). "Tor Browser 7.5a5 is released" (https://blog.torproject.org/tor-browser-75a5-released) *boklm's blog*. Tor Project. Retrieved 6 October 2017.
123. "Tor Browser" (https://www.torproject.org/projects/torbrowser.html.en). *The Tor Project*. Retrieved 4 June 2016.
124. "Tor Browser Bundle" (https://web.archive.org/web/20140623203436/https://www.torproject.org/projects/torbrowser.html.en). *Tor Project*. 2014-06-23. Archived from the original (https://www.torproject.org/projects/torbrowser.html.en) on 2014-06-23. Retrieved 2017-05-21.
125. Perry, Mike; Clark, Erinn; Murdoch, Steven (15 March 2013). "The Design and Implementation of the Tor Browser [DRAFT]" (https://www.torproject.org/projects/torbrowser/design/). *Tor Project*. Retrieved 28 April 2014.
126. Alin, Andrei (2 December 2013). "Tor Browser Bundle Ubuntu PPA" (http://www.webupd8.org/2013/12/tor-browser-bundle-ubuntu-ppa.html) *Web Upd8*. Retrieved 28 April 2014.
127. Knight, John (1 September 2011). "Tor Browser Bundle-Tor Goes Portable" (http://www.linuxjournal.com/content/tor-browser-bundle-tor-goes-portable) *Linux Journal*. Retrieved 28 April 2014.
128. Dredge, Stuart (5 November 2013). "What is Tor? A beginner's guide to the privacy tool" (https://www.theguardian.com/technology/2013/nov/05/tor-beginners-guide-nsa-browser). *The Guardian*. Retrieved 28 April 2014.
129. Samson, Ted (5 August 2013). "Tor Browser Bundle for Windows users susceptible to info-stealing attack" (http://www.infoworld.com/t/data-security/tor-browser-bundle-windows-users-susceptible-info-stealing-attack-224157) *InfoWorld*. Retrieved 28 April 2014.
130. Poulsen, Kevin (8 May 2013). "Feds Are Suspects in New Malware That Attacks Tor Anonymity" (https://www.wired.com/2013/08/freedom-hosting/). *Wired*. Retrieved 29 April 2014.
131. Owen, Gareth. "FBI Malware Analysis" (http://ghowen.me/fbi-tor-malware-analysis) Retrieved 6 May 2014.
132. Best, Jessica (21 January 2014). "Man branded 'largest facilitator of child porn on the planet' remanded in custody again" (http://www.mirror.co.uk/news/world-news/eric-eoin-marques-man-branded-3046701) *Daily Mirror*. Retrieved 29 April 2014.
133. Dingledine, Roger (5 August 2013). "Tor security advisory: Old Tor Browser Bundles vulnerable" (https://blog.torproject.org/blog/tor-security-advisory-old-tor-browser-bundles-vulnerable). *Tor Project*. Retrieved 28 April 2014.
134. Poulsen, Kevin (13 September 2013). "FBI Admits It Controlled Tor Servers Behind Mass Malware Attack" (https://www.wired.com/threatlevel/2013/09/freedom-hosting-fbi/). *Wired*. Retrieved 22 December 2013.
135. Schneier, Bruce (4 October 2013). "Attacking Tor: how the NSA targets users' online anonymity" (https://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity). *The Guardian*. Retrieved 22 December 2013.
136. Poulsen, Kevin (8 May 2014). "Visit the Wrong Website, and the FBI Could End Up in Your Computer" (https://www.wired.com/2014/08/operation_torpedo/). *Wired*.
137. Singh, Sukhbir (29 October 2015). "Tor Messenger Beta: Chat over Tor, Easily" (https://blog.torproject.org/blog/tor-messenger-beta-chat-over-tor-easily) *The Tor Blog*. The Tor Project. Retrieved 31 October 2015.
138. Singh, Sukhbir (28 September 2017). "Tor Messenger 0.5.0b1 is released" (https://blog.torproject.org/tor-messenger-050b1-released) *sukhbir's blog*. The Tor Project. Retrieved 6 October 2017.
139. "Tor Messenger Design Document" (https://trac.torproject.org/projects/tor/wiki/doc/TorMessenger/DesignDoc) *The Tor Project*. 13 July 2015. Retrieved 22 November 2015.
140. "Tor" (http://wiki.vuze.com/w/Tor). *Vuze*. Retrieved 3 March 2010.
141. "Bitmessage FAQ" (https://bitmessage.org/wiki/FAQ). *Bitmessage*. Retrieved 17 July 2013.
142. "About" (https://guardianproject.info/) *The Guardian Project* Retrieved 10 May 2011.
143. "ChatSecure: Private Messaging" (https://guardianproject.info/apps/chatsecure/) *The Guardian Project*. Retrieved 20 September 2014.
144. "Orbot: Mobile Anonymity + Circumvention" (https://guardianproject.info/apps/orbot/) *The Guardian Project* Retrieved 10 May 2011.
145. "Orweb: Privacy Browser" (https://guardianproject.info/apps/orweb/) *The Guardian Project*. Retrieved 10 May 2011.
146. n8fr8 (30 June 2015). "Orfox: Aspiring to bring Tor Browser to Android" (https://guardianproject.info/2015/06/30/orfox-aspiring-to-bring-tor-browser-to-android/) *guardianproject.info*. Retrieved 17 August 2015. "Our plan is to actively encourage users to move from Orweb to Orfox, and stop active development of Orweb, even removing to from the Google Play Store".
147. "ProxyMob: Firefox Mobile Add-on" (https://guardianproject.info/apps/proxymob-firefox-add-on/). *The Guardian Project* Retrieved 10 May 2011.
148. "Obscura: Secure Smart Camera" (https://guardianproject.info/apps/obscuracam/) *The Guardian Project* Retrieved 19 September 2014.
149. Жуков, Антон (15 December 2009). "Включаем Tor на всю катушку" (https://web.archive.org/web/20130901035137/http://eng.xakep.ru/link/51074/) [Make Tor go the whole hog]. *Xakep*. Archived from the original (http://eng.xakep.ru/link/51074/) on 1 September 2013. Retrieved 28 April 2014.
150. "Tor Project: Pluggable Transports" (https://www.torproject.org/docs/pluggable-transports.html.en). *torproject.org*. Retrieved 2016-08-05.
151. Brandom, Russell (9 May 2014). "Domestic violence survivors turn to Tor to escape abusers" (https://www.theverge.com/2014/5/9/5699600/domestic-violence-survivors-turn-to-tor-to-escape-abusers) *The Verge*. Retrieved 30 August 2014.
152. Gurnow, Michael (1 July 2014). "Seated Between Pablo Escobar and Mahatma Gandhi: The Sticky Ethics of Anonymity Networks" (http://dissidentvoice.org/2013/06/seated-between-pablo-escobar-and-mahatma-gandhi/) *Dissident Voice*. Retrieved 17 July 2014.

153. Lawrence, Dune (23 January 2014). "The Inside Story of Tor, the Best Internet Anonymity Tool the Government Ever Built" (http://mobile.businessweek.com/articles/2014-01-23/tor-anonymity-software-vs-dot-the-national-security-agency) *Businessweek magazine* Retrieved 30 August 2014.
154. Zetter, Kim (1 June 2010). "WikiLeaks Was Launched With Documents Intercepted From Tor" (https://www.wired.com/2010/06/wikileaks-documents/). *Wired*. Retrieved 30 August 2014.
155. Lee, Timothy B. (10 June 2013). "Five ways to stop the NSA from spying on you" (https://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/10/five-ways-to-stop-the-nsa-from-spying-on-you/) *Washington Post*. Retrieved 30 August 2014.
156. Norton, Quinn (9 December 2014). "Clearing the air around Tor" (http://pando.com/2014/12/09/clearing-the-air-around-tor/) *PandoDaily*.
157. McKim, Jenifer B. (8 March 2012). "Privacy software, criminal use" (https://web.archive.org/web/20120312225054/http://articles.boston.com/2012-03-08/business/31136655_1_law-enforcement-free-speech-technology/2) *The Boston Globe*. Archived from the original (http://articles.boston.com/2012-03-08/business/31136655_1_law-enforcement-free-speech-technology/2) on 12 March 2012.
158. Fowler, Geoffrey A. (17 December 2012). "Tor: an anonymous, and controversial, way to web-surf" (https://www.wsj.com/articles/SB10001424127887324677204578185382377144280). *Wall Street Journal*. Retrieved 19 May 2013.
159. Moore, Daniel; Rid, Thomas. "Cryptopolitik and the Darknet". Survival. Feb2016, Vol. 58 Issue 1, p7-38. 32p.
160. Inc., The Tor Project,. "Tor: Sponsors". www.torproject.org. Retrieved 2016-10-28.
161. Fung, Brian (6 September 2013). "The feds pay for 60 percent of Tor's development. Can users trust it?" (https://www.washingtonpost.com/blogs/theswitch/wp/2013/09/06/the-feds-pays-for-60-percent-of-tors-development-can-users-trust-it/) *The Switch*. Washington Post. Retrieved 6 February 2014.
162. "Tor is Not as Safe as You May Think" (http://www.infosecurity-magazine.com/news/tor-is-not-as-safe-as-you-may-think/) *Infosecurity magazine*. 2 September 2013. Retrieved 30 August 2014.
163. "'Tor Stinks' presentation – read the full document" (https://www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document) *The Guardian*. 4 October 2014. Retrieved 30 August 2014.
164. O'Neill, Patrick Howell (2 October 2014). "The real chink in Tor's armor" (http://www.dailydot.com/crime/silk-road-tor-arrests/) *The Daily Dot*.
165. "Dark net experts trade theories on 'de-cloaking' after raids" (http://www.bbc.co.uk/news/technology-29987373) 7 November 2014. Retrieved 12 November 2014.
166. SPIEGEL Staff (28 December 2014). "Prying Eyes: Inside the NSA's War on Internet Security" (http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html) *Der Spiegel*. Retrieved 23 January 2015.
167. "Presentation from the SIGDEV Conference 2012 explaining which encryption protocols and techniques can be attacked and which not" (http://www.spiegel.de/media/media-35535.pdf) (PDF). *Der Spiegel*. 28 December 2014. Retrieved 23 January 2015.
168. "2010 Free Software Awards announced" (http://www.fsf.org/news/2010-free-software-awards-announced) *Free Software Foundation*. Retrieved 23 March 2011.
169. Wittmeyer, Alicia P.Q. (26 November 2012). "The FP Top 100 Global Thinkers" (https://foreignpolicy.com/articles/2012/11/26/the_fp_100_global_thinkers?page=0,48) *Foreign Policy*. Archived (https://www.webcitation.org/6CVUyRpk?url=http://www.foreignpolicy.com/articles/2012/11/26/the_fp_100_global_thinkers?page=0,33) from the original on 28 November 2012. Retrieved 28 November 2012.
170. Sirius, R. U. (11 March 2013). "Interview uncut: Jacob Appelbaum" (https://www.theverge.com/2013/3/11/4091186/interview-uncut-jacob-appelbaum) *theverge.com*.
171. Gaertner, Joachim (1 July 2013). "Darknet – Netz ohne Kontrolle" (https://web.archive.org/web/20130704075422/http://www.daserste.de/information/wissen-kultur/ttt/sendung/br/20130630-ttt-darknet-102.html) *Das Erste* (in German). Archived from the original (http://www.daserste.de/information/wissen-kultur/ttt/sendung/br/20130630-ttt-darknet-102.html) on 4 July 2013. Retrieved 28 August 2013.
172. Gallagher, Sean (25 July 2014). "Russia publicly joins war on Tor privacy with $111,000 bounty" (https://arstechnica.com/security/2014/07/russia-publicly-joins-war-on-tor-privacy-with-111000-bounty/) *Ars Technica*. Retrieved 26 July 2014.
173. Lucian, Constantin (25 July 2014). "Russian government offers huge reward for help unmasking anonymous Tor users" (http://www.pcworld.com/article/2458420/russian-government-offers-money-for-identifying-tor-users.html). *PC World*. Retrieved 26 July 2014.
174. O'Neill, Patrick Howell (26 March 2015). "Tor's great rebranding" (http://www.dailydot.com/politics/tor-media-public-relations-perception/) *The Daily Dot*. Retrieved 19 April 2015.
175. Peterson, Andrea (28 May 2015). "U.N. report: Encryption is important to human rights — and backdoors undermine it" (https://www.washingtonpost.com/blogs/theswitch/wp/2015/05/28/un-report-encryption-is-important-to-human-rights-and-backdoors-undermine-it). *The Washington Post*.
176. "Tor Exit Nodes in Libraries – Pilot (phase one)" (https://blog.torproject.org/blog/tor-exit-nodes-libraries-pilot-phase-one) *Tor Project.org*. Retrieved 15 September 2015.
177. "Library Freedom Project" (https://libraryfreedomproject.org/) *libraryfreedomproject.org* Retrieved 15 September 2015.
178. Doyle-Burr, Nora (16 September 2015). "Despite Law Enforcement Concerns, Lebanon Board Will Reactivate Privacy Network Tor at Kilton Library" (https://web.archive.org/web/20150918031540/http://www.vnews.com/photos/inthenews/18620952-95/despite-law-enforcement-concerns-lebanon-board-will-reactivate-privacy-network-tor-at-kilton-library) *Valley News*. Archived from the original (http://www.vnews.com/photos/inthenews/18620952-95/despite-law-enforcement-concerns-lebanon-board-will-reactivate-privacy-network-tor-at-kilton-library) on 18 September 2015. Retrieved 20 November 2015.
179. "Lofgren questions DHS policy towards TOR Relays" (https://lofgren.house.gov/news/documentsingle.aspx?DocumentID=398038) *house.gov*. 10 December 2015. Retrieved 4 June 2016.
180. Geller, Eric (11 December 2015). "Democratic lawmaker wants to know if DHS is sabotaging plans for Tor exit relays" (http://www.dailydot.com/politics/tor-libraries-dhs-zoe-lofgren-letter/) *The Daily Dot*. Retrieved 4 June 2016.
181. Kopfstein, Janus (12 December 2015). "Congresswoman Asks Feds Why They Pressured a Library to Disable Its Tor Node" (https://motherboard.vice.com/read/congresswoman-asks-feds-why-they-pressured-a-library-to-disable-its-tor-node) *Motherboard*. Archived (https://web.archive.org/web/20151222171028/http://motherboard.vice.com/read/congresswoman-asks-feds-why-they-pressured-a-library-to-disable-its-tor-node) from the original on 22 December 2015.
182. "Tor crusader discuss privacy freedom with ExpressVPN" (https://www.expressvpn.com/blog/chuck-mcandrew-defends-tor/) *Home of internet privacy*. 2016-08-04. Retrieved 2017-09-11.
183. Gonzalo, Marilín (26 January 2016). "Esta biblioteca valenciana es la segunda del mundo en unirse al proyecto Tor" (http://www.eldiario.es/cultura/tecnologia/privacidad/biblioteca-Valencia-primera-Unidos-Tor_0_476303147.html) *El Diario* (in Spanish). Retrieved 4 March 2016.
184. Broersma, Matthew (26 August 2015). "IBM Tells Companies To Block Tor Anonymisation Network" (http://www.techweekeurope.co.uk/security/ibm-companies-tor-175468). *TechWeekEurope UK*. Retrieved 15 September 2015.
185. Greenberg, Andy (14 September 2015). "Mapping How Tor's Anonymity Network Spread Around the World" (https://www.wired.com/2015/09/mapping-tors-anonymity-network-spread-around-world/) *Wired*. Retrieved 9 February 2016.
186. Malivindi, Diandra (15 September 2015). "The New Map That Tracks Your TOR Activity" (https://www.gq.com.au/entertainment/tech/the+new+map+that+tracks+your+tor+activity/38999). *GQ Australia*. Retrieved 9 February 2016.
187. "This is What a Tor Supporter Looks Like: Daniel Ellsberg" (https://blog.torproject.org/blog/what-tor-supporter-looks-daniel-ellsberg) *The Tor Blog*. 26 December 2015. Retrieved 4 June 2016.
188. "This is What a Tor Supporter Looks Like: Cory Doctorow" (https://blog.torproject.org/blog/what-tor-supporter-looks-cory-doctorow) *The Tor Blog*. 18 December 2015. Retrieved 4 June 2016.
189. "This is What a Tor Supporter Looks Like: Edward Snowden" (https://blog.torproject.org/blog/what-tor-supporter-looks-edward-snowden) *The Tor Blog*. 30 December 2015. Retrieved 4 June 2016.
190. "This is what a Tor Supporter looks like: MollyCrabapple" (https://blog.torproject.org/blog/what-tor-supporter-looks-molly-crabapple) *The Tor Blog*. 9 December 2015. Retrieved 4 June 2016.
191. "House Bill 1508: An Act allowing public libraries to run certain privacy software" (http://www.gencourt.state.nh.us/bill_status/billText.aspx?id=796&txtFormat=html) *New Hampshire State Government* 10 March 2016. Retrieved 4 June 2016.
192. O'Neill, Patrick Howell (18 February 2016). "New Hampshire bill allows for libraries' usage of encryption and privacy software" (http://www.dailydot.com/politics/new-hampshire-tor-library-legislation/) *The Daily Dot*. Retrieved 10 March 2016.
193. "New Hampshire HB1508 – 2016 – Regular Session" (https://legiscan.com/NH/text/HB1508/id/1288060) *legiscan.com*. Retrieved 4 June 2016.
194. "Library in FIMS joins global network fighting back against digital surveillance, censorship, and the obstruction of information" (http://www.fims.uwo.ca/news/2016/library_in_fims_joins_global_network_fighting_back_against_digital_surveillance_censorship_and_the_obstruction_of_information.html) *FIMS News*. 14 March 2016. Retrieved 16 March 2016.
195. Pearson, Jordan (25 September 2015). "Can You Be Arrested for Running a Tor Exit Node In Canada?" (https://motherboard.vice.com/read/can-you-be-arrested-for-running-a-tor-exit-node-in-canada) *Motherboard*. Retrieved 16 March 2016.
196. Pearson, Jordan (16 March 2016). "Canadian Librarians Must Be Ready to Fight the Feds on Running a Tor Node" (https://motherboard.vice.com/en_ca/read/canadian-librarians-must-be-ready-to-fight-the-feds-on-running-a-tor-node-western-library-freedom-project). *Motherboard*. Retrieved 16 March 2016.
197. Pagliery, Jose (17 May 2016). "Developer of anonymous Tor software dodges FBI, leaves US" (http://money.cnn.com/2016/05/17/technology/tor-developer-fbi/index.html). *CNN*. Retrieved 17 May 2016.
198. Weiner, Anna (2016-12-02). "Trump Preparedness: Digital Security 101" (http://www.newyorker.com/culture/culture-desk/trump-preparedness-digital-security-101)
199. "Turkey Partially Blocks Access to Tor and Some VPNs" (https://www.bleepingcomputer.com/news/government/turkey-partially-blocks-access-to-tor-and-some-vpns/) 19 December 2016.
200. "Forfeiture Complaint" (https://www.justice.gov/opa/press-release/file/982821/download). Justice.gov. 20 July 2017. p. 27.
201. Leyden, John (2017-07-20). "Cops harpoon two dark net whales in megabust: AlphaBay and Hansa : Tor won't shield you, warn Feds" (https://www.theregister.co.uk/2017/07/20/dark_net_megabust/) *The Register*. Retrieved 2017-07-21.

202. McCarthy, Kieren (2017-07-20). "Alphabay shutdown: Bad boys, bad boys, what you gonna do? Not use your Hotmail... ...or the Feds will get you ♪" (https://www.theregister.co.uk/2017/07/20/alphabay_hotmail_fbi/) *The Register*. Retrieved 2017-07-21.
203. Johnson, Tim (2017-08-02). "Shocked by gruesome crime, cyber execs help FBI on dark web" (http://www.idahostatesman.com/news/nation-world/national/article164797842.html). *Idaho Statesman*.
204. "Want Tor to Really Work?" – Tor Project (https://www.torproject.org/download/download-easy.html.en#warning)
205. "Tor: Overview – Staying anonymous" (https://www.torproject.org/about/overview.html.en). Retrieved 21 September 2016.
206. "Building a new Tor that can resist next-generation state surveillance" (https://arstechnica.com/security/2016/08/building-a-new-tor-that-withstands-next-generation-state-surveillance/). *arstechnica.com*. Retrieved 13 September 2016.
207. "Clinton feared hack after getting porn link sent to her secret email" (http://www.dailymail.co.uk/news/article-3771474/Clinton-email-server-hit-dark-web-tools-Hillary-worried-hacked-getting-send-link-porn.html) *dailymail.co.uk*. Retrieved 13 September 2016.
208. "Aussie cops ran child porn site for months, revealed 30 US IPs" (https://arstechnica.com/tech-policy/2016/08/aussie-cops-ran-child-porn-site-for-months-revealed-30-us-ips/). *arstechnica.com*. Retrieved 13 September 2016.

References

- Anonymity Bibliography Retrieved: 21 May 2007
- Schneier, Bruce. *Applied Cryptography*. ISBN 0-471-11709-9
- Schneier, Bruce. *Email Security*. ISBN 0-471-05318-X
- Bacard, Andre. *Computer Privacy Handbook* ISBN 1-56609-171-3

External links

- Official website
- Tor: Hidden Services and Deanonymisation presentation at the 31st Chaos Computer Conference
- TorFlow, a dynamic visualization of data flowing over the Tor network
- Tor onion services: more useful than you think in a 2016 presentation at the 32nd Annual Chaos Communication Congress
- A core Tor developer lectures at the Radboud University Nijmegen in The Netherlands on anonymity systems in 2016
- A technical presentation given at the University of Waterloo in Canada: Tor's Circuit-Layer Cryptography: Attacks, Hacks, and Improvements
- Excuse Me, I Think Your Dark Web is Showing – A presentation at the March 2017 BSides Vancouver Security Conference on security practices on Tor's hidden services