THE ONION ROUTER – OVERVIEW PT 1

Joas Antonio

About

The purpose of the book is to bring you materials for you to learn more about the TOR network

My LinkedIn:

https://www.linkedin.com/in/joas-antonio-dos-santos/

What is TOR?

In the 1990s, the lack of security on the internet and its ability to be used for tracking and surveillance was becoming clear, and in 1995, David Goldschlag, Mike Reed, and Paul Syverson at the U.S. Naval Research Lab (NRL) asked themselves if there was a way to create internet connections that don't reveal who is talking to whom, even to someone monitoring the network. Their answer was to create and deploy the first research designs and prototypes of onion routing.

The goal of onion routing was to have a way to use the internet with as much privacy as possible, and the idea was to route traffic through multiple servers and encrypt it each step of the way. This is still a simple explanation for how Tor works today.

In the early 2000s, Roger Dingledine, a recent Massachusetts Institute of Technology (MIT) graduate, began working on an NRL onion routing project with Paul Syverson. To distinguish this original work at NRL from other onion routing efforts that were starting to pop up elsewhere, Roger called the project Tor, which stood for The Onion Routing. Nick Mathewson, a classmate of Roger's at MIT, joined the project soon after.

From its inception in the 1990s, onion routing was conceived to rely on a decentralized network. The network needed to be operated by entities with diverse interests and trust assumptions, and the software needed to be free and open to maximize transparency and decentralization. That's why in October 2002 when the Tor network was initially deployed, its code was released under a free and open software license. By the end of 2003, the network had about a dozen volunteer nodes, mostly in the U.S., plus one in Germany.

What is TOR?

Recognizing the benefit of Tor to digital rights, the Electronic Frontier Foundation (EFF) began funding Roger's and Nick's work on Tor in 2004. In 2006, the Tor Project, Inc., a 501(c)(3) nonprofit organization, was founded to maintain Tor's development.

In 2007, the organization began developing bridges to the Tor network to address censorship, such as the need to get around government firewalls, in order for its users to access the open web.

Tor began gaining popularity among activists and tech-savvy users interested in privacy, but it was still difficult for less-technically savvy people to use, so starting in 2005, development of tools beyond just the Tor proxy began. Development of Tor Browser began in 2008.

With Tor Browser having made Tor more accessible to everyday internet users and activists, Tor was an instrumental tool during the Arab Spring beginning in late 2010. It not only protected people's identity online but also allowed them to access critical resources, social media, and websites which were blocked.

The need for tools safeguarding against mass surveillance became a mainstream concern thanks to the Snowden revelations in 2013. Not only was Tor instrumental to Snowden's whistleblowing, but content of the documents also upheld assurances that, at that time, Tor could not be cracked.

People's awareness of tracking, surveillance, and censorship may have increased, but so has the prevalence of these hindrances to internet freedom. Today, the network has thousands of relays run by volunteers and millions of users worldwide. And it is this diversity that keeps Tor users safe.

We, at the Tor Project, fight every day for everyone to have private access to an uncensored internet, and Tor has become the world's strongest tool for privacy and freedom online.

But Tor is more than just software. It is a labor of love produced by an international community of people devoted to human rights. The Tor Project is deeply committed to transparency and the safety of its users.

HOW TO WORK?

https://tb-manual.torproject.org/about/

HOW TO WORK?

https://tb-manual.torproject.org/about/

BRIDGES
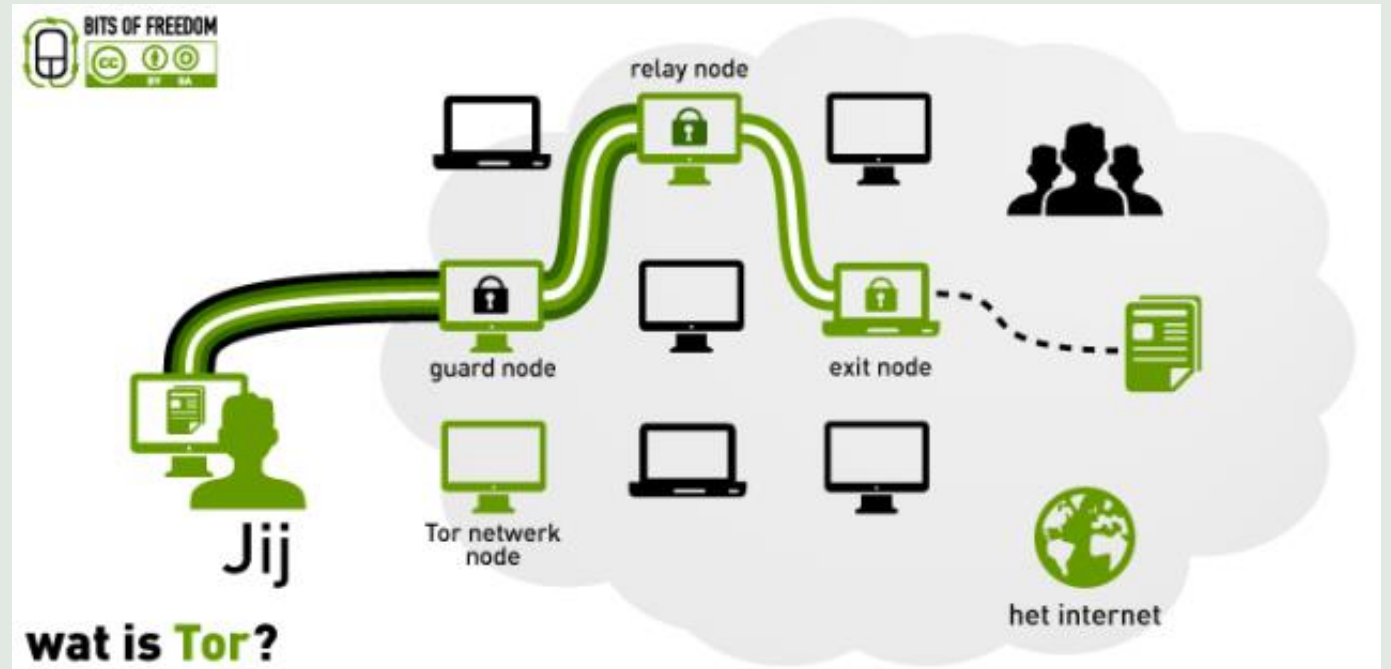
https://tb-manual.torproject.org/bridges/

Bridge relays are Tor relays that are not listed in the public Tor directory. That means that ISPs or governments trying to block access to the Tor network can't simply block all bridges. Bridges are useful for Tor users under oppressive regimes, and for people who want an extra layer of security because they're worried somebody will recognize that they are contacting a public Tor relay IP address.

A bridge is just a normal relay with a slightly different configuration. See How do I run a bridge for instructions.

Several countries, including China and Iran, have found ways to detect and block connections to Tor bridges. Obfsproxy bridges address this by adding another layer of obfuscation. Setting up an obfsproxy bridge requires an additional software package and additional configurations. See our page on pluggable transports for more info.

https://support.torproject.org/censorship/censorship-7/

RELAYS

https://tb-manual.torproject.org/bridges/

https://community.torproject.org/relay/setup/bridge/
https://support.torproject.org/relay-operators/
https://medium.com/coinmonks/tor-nodes-explained-580808c29e2d
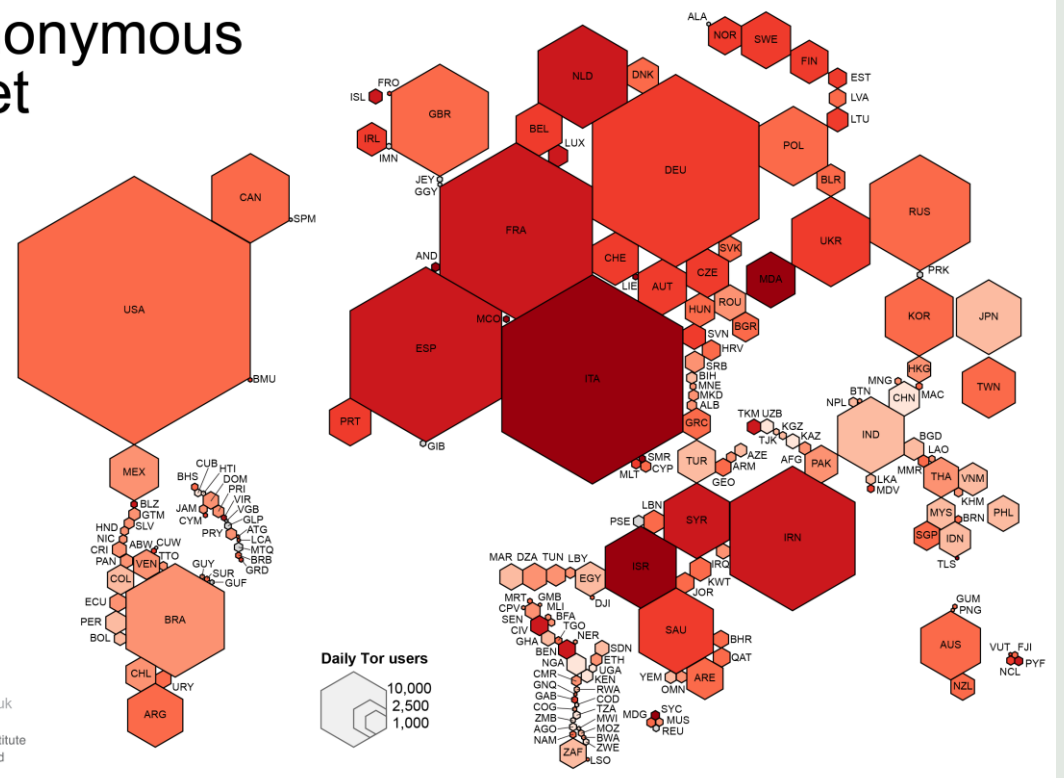
MANAGING IDENTITIES

https://tb-manual.torproject.org/bridges/

When you connect to a website, it is not only the operators of that website who can record information about your visit. Most websites now use numerous third-party services, including social networking "Like" buttons, analytics trackers, and advertising beacons, all of which can link your activity across different sites.

Using the Tor network stops observers from being able to discover your exact location and IP address, but even without this information they might be able to link different areas of your activity together. For this reason, Tor Browser includes some additional features that help you control what information can be tied to your identity.

https://tb-manual.torproject.org/managing-identities/

TOR Secure Connections

- https://tb-manual.torproject.org/secure-connections/
- https://tb-manual.torproject.org/security-settings/
- https://www.vpnmentor.com/blog/tor-browser-work-relate-using-vpn/
- https://portswigger.net/daily-swig/tor-security-everything-you-need-to-know-about-the-anonymity-network
- https://community.torproject.org/onion-services/advanced/https/
- https://www.youtube.com/watch?v=9J0GUQhag-0&ab_channel=Techlore
- https://thesafety.us/tor-browser-setup
- https://ssd.eff.org/en/module/how-use-tor-windows
- https://www.techradar.com/how-to/how-to-protect-your-privacy-online-with-tor-browser-improve-your-security-and-stay-anonymous
- https://www.theverge.com/2020/2/21/21138403/tor-privacy-tools-private-network-browser-settings-security

Plugins Tor

- https://tb-manual.torproject.org/pt-BR/plugins/
- https://tb-manual.torproject.org/plugins/
- https://support.torproject.org/tbb/tbb-14/
- https://tb-manual.torproject.org/pt-BR/circumvention/

O acesso direto à rede Tor às vezes pode estar sendo bloqueado pelo seu provedor de Internet, ou pelo governo. O Navegador Tor tem incluídas algumas ferramentas de evasão para contornar esses bloqueios. Essas ferramentas são denominadas "transportes plugáveis".

Direct access to the Tor network can sometimes be blocked by your ISP, or the government. Tor Browser has included some evasion tools to bypass these locks. These tools are called "pluggable transports".

Plugins Tor

- https://tb-manual.torproject.org/pt-BR/plugins/
- https://tb-manual.torproject.org/plugins/
- https://support.torproject.org/tbb/tbb-14/
- https://tb-manual.torproject.org/pt-BR/circumvention/

O acesso direto à rede Tor às vezes pode estar sendo bloqueado pelo seu provedor de Internet, ou pelo governo. O Navegador Tor tem incluídas algumas ferramentas de evasão para contornar esses bloqueios. Essas ferramentas são denominadas "transportes plugáveis".

Direct access to the Tor network can sometimes be blocked by your ISP, or the government. Tor Browser has included some evasion tools to bypass these locks. These tools are called "pluggable transports".

Hops configuration

- https://tor.stackexchange.com/questions/1312/how-to-decrease-number-of-tor-hops
- https://support.torproject.org/misc/misc-11/
- https://stackoverflow.com/questions/11288148/tor-not-able-to-create-single-hop-circuit-one-hop-tunnel
- https://www.reddit.com/r/onions/comments/117fvh/questions_about_tor_and_traceroutesserver_hops/
- https://attack.mitre.org/techniques/T1090/003/
- https://github.com/moxie0/tortunnel

TOR Tunnels

- https://www.whonix.org/wiki/Tunnels/Introduction
- https://www.reddit.com/r/TOR/comments/5zonjq/tunnel_tor_through_vpn/
- https://www.youtube.com/watch?v=USBaUj2pc2M&ab_channel=EasyPrivacy
- https://superuser.com/questions/1133032/tunnel-tor-traffic-through-a-vpn
- https://www.whonix.org/wiki/Transporting_UDP_Tunnels_over_Tor
- https://www.reddit.com/r/TOR/comments/lyzd2q/tor_relay_and_dslite_no_public_ipv4_tunnel/
-

TOR + Python

- https://stackoverflow.com/questions/30286293/make-requests-using-python-over-tor
- https://sylvaindurand.org/use-tor-with-python/
- https://www.youtube.com/watch?v=KDsmVH7eJCs&ab_channel=AcuteGaming
- https://www.youtube.com/watch?v=h7ibO9qUnNQ&ab_channel=SATSifaction
- https://medium.com/@jasonrigden/using-tor-with-the-python-request-library-79015b2606cb
- https://pypi.org/project/requests-tor/

Onion Routing

Onion routing is a technique for anonymous communication over a computer network. In an **onion network**, messages are encapsulated in layers of encryption, analogous to layers of an onion. The encrypted data is transmitted through a series of network nodes called **onion routers**, each of which "peels" away from a single layer, uncovering the data's next destination. When the final layer is decrypted, the message arrives at its destination. The sender remains anonymous because each intermediary knows only the location of the immediately preceding and following nodes.[1] While onion routing provides a high level of security and anonymity, there are methods to break the anonymity of this technique, such as timing analysis.[2]

https://en.wikipedia.org/wiki/Onion_routing
https://www.onion-router.net/
https://www.youtube.com/watch?v=QRYzre4bf7I&ab_channel=Computerphile
https://www.youtube.com/watch?v=gIkzx7-s2RU&ab_channel=HusseinNasser

Onion Routing

- **https://www.geeksforgeeks.org/onion-routing/**
- https://www.sciencedirect.com/topics/computer-science/onion-router
- https://www.pcmag.com/encyclopedia/term/onion-routing
- https://www.onion-router.net/Publications/DISCEX-2000.pdf
- https://apps.dtic.mil/sti/pdfs/ADA465335.pdf
- https://community.torproject.org/onion-services/setup/
- https://www.coursera.org/lecture/security-and-privacy-in-tor-network/welcome-to-tor-networking-gUCiC

DNS Configuration and Security

- **https://developers.cloudflare.com/1.1.1.1/other-ways-to-use-1.1.1.1/dns-over-tor**
- https://2019.www.torproject.org/projects/tordnsel.html.en
- https://resources.infosecinstitute.com/topic/tor-part-2/
- https://nusenu.medium.com/who-controls-tors-dns-traffic-a74a7632e8ca
- https://www.youtube.com/watch?v=LT1ICNPQLX8&ab_channel=YouTux
- https://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=5517&context=etd
- https://tor.stackexchange.com/questions/711/onion-domains-dns-lookup
- https://cdn.hackaday.io/files/12985555550240/Linux%20DNS%20Resolver%20for%20Onions.txt
- https://forum.opnsense.org/index.php?topic=15097.0

Web Server Onion

- **https://www.youtube.com/watch?v=GVMjk9pj2Cw&ab_channel=NullByte**
- https://www.youtube.com/watch?v=QI3_DfjhMUQ&ab_channel=gnewlinux
- https://www.youtube.com/watch?v=4xFBE6pw1Rc&ab_channel=DASGeek
- https://nordvpn.com/pt-br/blog/how-to-register-onion-domain/
- https://medium.com/axon-technologies/hosting-anonymous-website-on-tor-network-3a82394d7a01
- https://riseup.net/pt/security/network-security/tor/onionservices-best-practices
- https://www.whonix.org/wiki/Onion_Services
- https://www.makeuseof.com/tag/create-hidden-service-tor-site-set-anonymous-website-server/
- https://github.com/davidmoreno/onion
- https://github.com/DanWin/hosting
- https://github.com/OnionIoT/Onion-Sensor-Server
- https://github.com/DanWin/onion-link-list

TOR Projects Community

- **https://github.com/Edu4rdSHL/tor-router**
- https://github.com/ajvb/awesome-tor
- https://github.com/jeremy-jr-benthum/onion-browser-button
- https://github.com/Jesse-V/OnioNS-client
- https://github.com/torproject/manual
- https://github.com/ralphwetzel/theonionpack
- https://github.com/katmagic/Shallot
-

TOR Proxy

- **https://www.techwalla.com/articles/how-to-use-tor-proxy**
- https://tor.stackexchange.com/questions/6939/configure-tor-as-proxy
- https://www.tecmint.com/use-tor-network-in-web-browser/
- https://www.youtube.com/watch?v=5iLCgRHp_2k&ab_channel=Thinknoodles
- https://www.youtube.com/watch?v=zf_eN7bqE8A&ab_channel=Proxy-SellerPrivateproxies
- https://www.youtube.com/watch?v=JXbIAX7UxNM&ab_channel=MakeTechEasier
- https://www.avg.com/en/signal/vpn-vs-proxy-vs-tor
- https://www.avast.com/c-vpn-proxy-tor-which-is-best
- https://opensource.com/article/20/4/tor-proxy-raspberry-pi

Whonix and Tails Configuration

- **https://www.whonix.org/wiki/Configuration_Files**
- https://www.whonix.org/wiki/Whonix-Gateway_System_DNS
- https://www.youtube.com/watch?v=y82TgJNivOI&ab_channel=KnowledgeSharingTech
- https://www.youtube.com/watch?v=2kHrmJoxsJI&ab_channel=LinuxVideoTutorials
- https://www.youtube.com/watch?v=wdirr08MkL4&ab_channel=Tunisiatuto
- https://www.youtube.com/watch?v=g8SzRhA8NXI&ab_channel=HackerSploit
- https://www.youtube.com/watch?v=T4Q0Mfo9lSc&ab_channel=SwitchedtoLinux
- https://www.youtube.com/watch?v=nRztIE_hRzM&ab_channel=KnowledgeSharingTech
- https://www.youtube.com/watch?v=Lopmyi6dZd0&ab_channel=%D8%A7%D9%84%D8%B3%D9%84%D8%B7%D8%A9%D8%A7%D9%84%D8%B3%D8%A7%D8%A8%D8%B9%D8%A9
- https://www.youtube.com/watch?v=eblHjIrMFYo&ab_channel=Herbertech
- https://www.youtube.com/watch?v=eVp1qZ7HrE4&ab_channel=TheCryptoDad

TOR Vulnerability, bad-relays and Attacks

- https://www.cvedetails.com/vulnerability-list/vendor_id-12287/product_id-23219/Torproject-TOR.html
- https://www.zdnet.com/article/multiple-tor-security-issues-disclosed-more-to-come/
- https://www.securityweek.com/tor-browser-patches-application-probing-vulnerability
- https://www.cs.utexas.edu/~ecprice/papers/tor.pdf
- https://security.stackexchange.com/questions/79438/can-a-malicious-tor-exit-node-perform-a-https-man-in-the-middle-attack-to-see-mo
- https://www.makeuseof.com/tor-exit-nodes-spying/
- https://www.schneier.com/blog/archives/2007/12/maninthemiddle.html
- https://gitlab.torproject.org/legacy/trac/-/wikis/doc/badRelays
- https://blog.1871.com/hacking-irl-what-mr.-robot-teaches-us-about-the-dark-web
- https://www.alctraining.com.au/staging/blog/the-realistic-tor-hack-of-mr-robot/
- https://tor.stackexchange.com/questions/8636/is-the-rons-coffee-tor-related-hack-technically-possible-in-episode-1x01-of-m
- https://www.zdnet.com/article/exploit-vendor-drops-tor-browser-zero-day-on-twitter/
- https://www.hackerfactor.com/blog/index.php?/archives/902-Tor-0day-Uniquely-Tracking-Computers.html

TOR Block Connections and bypass

- https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIRtCAK
- https://kb.smoothwall.com/hc/en-us/articles/360002033490-Blocking-Tor-Using-Smoothwall-Filter-Firewall
- https://www.sonicwall.com/support/knowledge-base/how-to-block-websites-when-accessed-from-tor-browser/170505675183808/
- https://www.youtube.com/watch?v=Qge3gQaQB1A&ab_channel=SystemZone
- https://www.sonicwall.com/support/video-tutorials/how-to-block-tor-using-app-control-advanced-signatures/5413958973001/
- https://community.sophos.com/utm-firewall/f/network-protection-firewall-nat-qos-ips/38804/block-tor
- https://systemzone.net/how-to-block-tor-browser-with-mikrotik-router/
- https://www.youtube.com/watch?v=qO8XsQiQSKU&ab_channel=SafeerKadambodan
- https://www.wikihow.com/Bypass-an-Internet-Filter-With-Tor
- https://tech.michaelaltfield.net/2018/02/22/bypassing-check-point-firewall-dpi-tor-blocking/

Links Onion

- hxxp://marketojbwagqnwx[.]onion/ - Marketo
- hxxp://cuba4mp6ximo2zlo[.]onion/ - Cuba
- hxxp://gtmx56k4hutn3ikv[.]onion/ - Babuk Locker
- hxxp://ixltdyumdlthrtgx[.]onion/ - Hades
- hxxp://ransomocmou6mnbquqz44ewosbkjk3o5qjsl3orawojexfook2j7es ad[.]onion/ - Everest
- hxxp://lockbit-blog[.]com/ - Lockbit
- hxxp://mountnewsokhwilx[.]onion/ - Mount Locker
- hxxp://wj3b2wtj7u2bzup75tzhnso56bin6bnvsxcbwbfcuvzpc4vcixbywlid[.]onion/ - Xinof - Raas (Login Required)
- hxxp://msaoyrayohnp32tcgwcanhjouetb5k54aekgnwg7dcvtgtecpumrx pqd[.]onion/ - Prolock
- hxxp://nbzzb6sa6xuura2z[.]onion/ - Suncrypt
- hxxp://sekhmetleaks[.]top/ - Sekhmet
- hxxp://dnpscnbaix6nkwvystl3yxglz7nteicqrou3t75tpcc5532cztc46qyd[.] onion/ - Revil
- hxxp://rnsm777cdsjrsdlbs4v5qoeppu3px6sb2igmh53jzrx7ipcrbjz5b2ad[.]onion/ - Ransomexx (Defray777)
- hxxp://rgleaktxuey67yrgspmhvtnrqtgogur35lwdrup4d3igtbm3pupc4lyd[.]onion/ - Ragnar Locker

Links Onion 2

- hxxp://wobpitin77vdsdiswr43duntv6eqw4rvphedutpaxycjdie6gg3binad[.]onion/ - Ragnarok
- hxxp://p6o7m73ujalhgkiv[.]onion/ - Ragnar
- hxxp://wqmfzni2nvbbpk25[.]onion/partners.html - Pysa
- hxxp://rnfdsgm6wb6j6su5txkekw4u4y47kp2eatvu7d6xhyn5cs4lt4pdrqqd[.]onion/blog - Netwalker
- hxxp://hxt254aygrsziejn[.]onion/ - Nefilim (Corporate Leaks)
- hxxps://mazenews[.]online/ - Maze-News
- hxxp://xfr3txoorcyy7tikjgj5dk3rvo3vsrpyaxnclyohkbfp3h277ap4tiad[.]onion/ - Maze
- hxxp://egregoranrmzapcv[.]onion/ - Egregor
- hxxp://hpoo4dosa3x4ognfxpqcrjwnsigvslm7kv6hvmhh2yqczaxy3j6qnwad[.]onion/ - Dopple Paymer
- hxxp://darksidedxcftmqa[.]onion/ - Darkside
- hxxp://avaddongun7rngel[.]onion/ - Avaddon
- hxxp://37rckgo66iydpvgpwve7b2el5q2zhjw4tv4lmyewufnpx4lhkekxkoqd[.]onion/ - Ako (Ranzy)
- hxxp://htcltkjqoitnez5slo7fvhiou5lbno5bwczu7il2hmfpkowwdpj3q2yd[.]onion/ - Conti

Links Onion 3

- hxxp://continewsnv5otx5kaoje7krkto2qbu3gtqef22mnr7eaxw3y6ncz3ad[.]onion/ - Conti-2
- hxxps://continews[.]best/ - Conti (Clear web)
- hxxp://fylszpcqfel7joif[.]onion/ - Conti-News (Ryuk)
- hxxp://ekbgzchl6x2ias37[.]onion/ - Clops
- hxxp://e6wzjohnxejirqa2sgridvymv2jxhrqdfuyxvoxp3xpqh7kr4kbwpwad[.]onion/ - Tornode
- hxxp://no6m4wzdexe3auiupv2zwif7rm6qwxcyhslkcnzisxgeiw6pvjsgafad[.]onion/ - Submarine
- hxxp://gdarku42fzpyrfra[.]onion/gdark/search.php - GDark
- hxxp://phobosxilamwcg75xt22id7aywkzol6q6rfl2flipcqoc4e4ahima5id[.]onion/ - Phobos
- hxxp://dnmugu4755642434[.]onion/search - Kilos - Darknet Market Search Engine
- hxxp://xssforumv3isucukbxhdhwz67hoa5e2voakcfkuieq4ch257vsburuid[.]onion/ - XSS
- hxxp://ezdhgsy2aw7zg54z6dqsutrduhl22moami5zv2zt6urr6vub7gs6wfad[.]onion/ - Def Con Forums
- hxxp://gerkipwhfuqeeizl[.]onion/ - Gerki_TOR
- hxxp://bcbm4y7yusdxthg3[.]onion/ - SkyFraud
- hxxp://l5b5ugkok5owt5w7xz7fvrvd75io2hvnao4c4gonidjmkqsyifwkdryd[.]onion/ - DarkNetStreets

Links Onion 4

- hxxp://ucapoywa7wsbzlf5umrrdi2otooa5napma3r5s5ojysts46l5bic4gid[.]onion/ - FreedomForum
- hxxp://k5aintllrufq23khjnmmfli6uxioboe3ylcao7k72mk2bgvwqb5ek4ad[.]onion/ - TruthBoard
- hxxp://hsquad7ikj4ejivl7e52rdfcvtgpqueqzu27wq273noeoi27y6kglxad[.]onion/ - Hack_Squad
- hxxp://pwndb2am4tzkvold[.]onion/ - pwndb
- hxxp://guardday6e5nxblpojbhmx5ws2avautr7eswu3qg7gynh52rh744anyd[.]onion/ - DarkGuard
- hxxp://torbox36ijlcevujx7mjb4oiusvwgvmue7jfn2cvutwa6kl6to3uyqad[.]onion/ - TORBOX
- hxxp://secmail63sex4dfw6h2nsrbmfz2z6alwxe4e3adtkpd4pcvkhht4jdad[.]onion/src/login.php - secMail - Darknet email
- hxxp://oq7t5ihk4qew5t5s4zghicigokh2ktt575amirsbnilmyawpme6xmyyd[.]onion/ - Elude
- hxxp://darkzzx4avcsuofgfez5zq75cqc4mprjvfqywo45dfcaxrwqg6qrlfid[.]onion/ - Darknetlive
- hxxps://protonirockerxow[.]onion/ - Protonmail (Onion)