Dark web

The **dark web** is the World Wide Web content that exists on darknets (overlay networks) that use the Internet but require specific software, configurations, or authorization to access.[1][2][3][4] Through the dark web, private computer networks can communicate and conduct business anonymously without divulging identifying information, such as a user's location.[5][6] The dark web forms a small part of the deep web, the part of the web not indexed by web search engines, although sometimes the term *deep web* is mistakenly used to refer specifically to the dark web.[7][2][8]

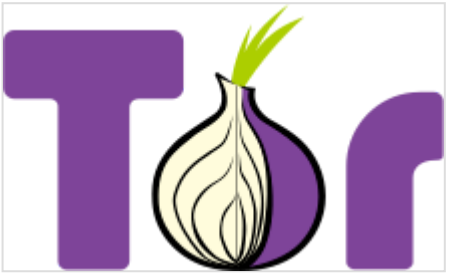
The darknets which constitute the dark web include small, friend-to-friend networks, as well as large, popular networks such as Tor, Hyphanet, I2P, and Riffle operated by public organizations and individuals.[6] Users of the dark web refer to the regular web as clearnet due to its unencrypted nature.[9] The Tor dark web or **onionland**[10] uses the traffic anonymization technique of onion routing under the network's top-level domain suffix .onion.

Terminology

Definition

The dark web has often been confused with the deep web, the parts of the web not indexed (searchable) by search engines. The term *dark web* first emerged in 2009; however, it is unknown when the actual dark web first emerged.[11] Many internet users only use the *surface web*, data that can be accessed by a typical web browser.[12] The dark web forms a small part of the deep web, but requires custom software in order to access its content. This confusion dates back to at least 2009.[13] Since then, especially in reporting on Silk Road, the two terms have often been conflated,[14] despite recommendations that they should be distinguished.[1][7]

The dark web, also known as darknet websites, are accessible only through networks such as Tor ("The Onion Routing" project) that are created specifically for the dark web.[12][15] Tor browser and Tor-accessible sites are widely used among the darknet users and can be identified by the domain ".onion".[16] Tor browsers create encrypted entry points and pathways for the user, allowing their dark web searches and actions to be anonymous.[12]


Tor software logo

Identities and locations of darknet users stay anonymous and cannot be tracked due to the layered encryption system. The darknet encryption technology routes users' data through a large number of intermediate servers, which protects the users' identity and guarantees anonymity. The transmitted information can be decrypted only by a subsequent node in the scheme, which leads to the exit node. The complicated system makes it almost impossible to reproduce the node path and decrypt the information layer by layer.[17] Due to the

high level of encryption, websites are not able to track geolocation and IP of their users, and users are not able to get this information about the host. Thus, communication between darknet users is highly encrypted allowing users to talk, blog, and share files confidentially.[18]

Content

Web-based onion services in February 2016[19][20]

Category	% of total	% of active
Violence	0.3	0.6
Arms	0.8	1.5
Illicit Social	1.2	2.4
Hacking	1.8	3.5
Illicit links	2.3	4.3
Illicit pornography	2.3	4.5
Extremism	2.7	5.1
Illicit Other	3.8	7.3
Illicit Finance	6.3	12
Illicit Drugs	8.1	15.5
Non-illicit+Unknown	22.6	43.2
Illicit total	29.7	56.8
Inactive	47.7	
Active	52.3	

A December 2014 study by Gareth Owen from the University of Portsmouth found that the most commonly hosted type of content on Tor was child pornography, followed by black markets, while the individual sites with the highest traffic were dedicated to botnet operations (see attached metric).[21] Many whistleblowing sites maintain a presence[22] as well as political discussion forums.[23] Sites associated with Bitcoin, fraud-related services, and mail order services are some of the most prolific.[21]

As of December 2020, the number of active Tor sites in .onion was estimated at 76,300 (containing a lot of copies). Of these, 18 000 would have original content.[24]

In July 2017, Roger Dingledine, one of the three founders of the Tor Project, said that Facebook is the biggest hidden service. The dark web comprises only 3% of the traffic in the Tor network.[25]

A February 2016 study from researchers at King's College London gives the following breakdown of content by an alternative category set, highlighting the illicit use of .onion services.[17][26]

Ransomware

The dark web is also used in certain extortion-related processes. It is common to observe data from ransomware attacks on several dark web sites, for example data sales sites or public data repository sites.[27][28]

Botnets

Botnets are often structured with their command-and-control servers based on a censorship-resistant hidden service, creating a large amount of bot-related traffic.[21][29]

Darknet markets

Commercial darknet markets mediate transactions for illegal goods and typically use Bitcoin as payment.[30] These markets have attracted significant media coverage, starting with the popularity of Silk Road and Diabolus Market and its subsequent seizure by legal authorities.[31] Silk Road was one of the first dark web marketplaces that emerged in 2011 and has allowed for the trading of illegal drugs, weapons and identity fraud resources.[30] These markets have no protection for its users and can be closed down at any time by authorities.[30] Despite the closures of these marketplaces, others pop up in their place.[30] As of 2020, there have been at least 38 active dark web market places, even though there can be many more.[30] These marketplaces are similar to that of eBay or Craigslist where users can interact with sellers and leave reviews about marketplace products.[30]

Examination of price differences in dark web markets versus prices in real life or over the World Wide Web have been attempted as well as studies in the quality of goods received over the dark web. One such study was performed on Evolution, one of the most popular crypto-markets active from January 2013 to March 2015.[32] Although it found the digital information, such as concealment methods and shipping country, "seems accurate", the study uncovered issues with the quality of illegal drugs sold in Evolution, stating that, "the illicit drugs purity is found to be different from the information indicated on their respective listings."[32] Less is known about consumer motivations for accessing these marketplaces and factors associated with their use.[33] Darknets markets also sell leaked credit cards[34] that can be downloaded for free or purchased for use in illegal activities.

Bitcoin services

Bitcoin is one of the main cryptocurrencies used in dark web marketplaces due to the flexibility and relative anonymity of the currency.[35] With bitcoin, people can hide their intentions as well as their identity.[36] A common approach was to use a digital currency exchanger service which converted bitcoin into an online game currency (such as gold coins in World of Warcraft) that will later be converted back into fiat currency.[37][38] Bitcoin services such as tumblers are often available on Tor, and some – such as Grams – offer darknet market integration.[39][40] A research study undertaken by Jean-Loup Richet, a research fellow at ESSEC, and carried out with the United Nations Office on Drugs and Crime, highlighted new trends in the use of bitcoin tumblers for money laundering purposes, using escrows.

Due to its relevance in the digital world, bitcoin has become a popular product for users to scam companies with.[35] Cybercriminal groups such as DDOS"4" have led to over 140 cyberattacks on companies since the emergence of bitcoins in 2014.[35] These attacks have led to the formation of other cybercriminal groups as well as Cyber Extortion.[35]

Hacking groups and services

Many hackers sell their services either individually or as a part of groups.[41] Such groups include xDedic, hackforum, Trojanforge, Mazafaka, dark0de and the TheRealDeal darknet market.[42] Some have been known to track and extort apparent pedophiles.[43] Cyber crimes and hacking services for financial institutions and banks have also been offered over the dark web.[44] Attempts to monitor this activity have been made through various government and private organizations, and an examination of the tools used can be found in the *Procedia Computer Science* journal.[45] Use of Internet-scale DNS distributed reflection denial of service (DRDoS) attacks have also been made through leveraging the dark web.[46] There are many scam .onion sites also present which end up giving tools for download that are infected with trojan horses or backdoors.

Recently, around 100,000 compromised ChatGPT users' login information was sold on the dark web in 2023. Additionally, the logs showed, in the opinion of the researchers, that the majority of the compromised ChatGPT passwords had been extracted by the data-stealing virus Raccoon.[47]

Financing and fraud

Scott Dueweke the president and founder of Zebryx Consulting states that Russian electronic currency such as WebMoney and Perfect Money are behind the majority of the illegal actions.[36] In April 2015, Flashpoint received a 5 million dollar investment to help their clients gather intelligence from the deep and dark web.[48] There are numerous carding forums, PayPal and bitcoin trading websites as well as fraud and counterfeiting services.[49] Many such sites are scams themselves.[50] Phishing via cloned websites and other scam sites are numerous,[51][52] with darknet markets often advertised with fraudulent URLs.[53][54]

Illegal pornography

The type of content that has the most popularity on the dark web is illegal pornography—more specifically, child pornography.[35] About 80% of its web traffic is related to accessing child pornography despite it being difficult to find even on the dark web.[35] A website called Lolita City, which has since been taken down, contained over 100 GB of child pornographic media and had about 15,000 members.[35]

There is regular law enforcement action against sites distributing child pornography[55][56] – often via compromising the site and tracking users' IP addresses.[57][58] In 2015, the FBI investigated and took down a website called Playpen.[35] At the time, Playpen was the largest child pornography website on the dark web with over 200,000 members.[35] Sites use complex systems of guides, forums and community regulation.[59] Other content includes sexualised torture and killing of animals[60] and revenge porn.[61] In May 2021, German police said that they had dismantled one of the world's biggest child pornography networks on the dark web known as Boystown; the website had over 400,000 registered users. Four

people had been detained in raids, including a man from Paraguay, on suspicion of running the network. Europol said several pedophile chat sites were also taken down in the German-led intelligence operation.[62][63]

Terrorism

Terrorist organizations took to the internet as early as the 1990s; however, the birth of the dark web attracted these organizations due to the anonymity, lack of regulation, social interaction, and easy accessibility.[64] These groups have been taking advantage of the chat platforms within the dark web to inspire terrorist attacks.[64] Groups have even posted "How To" guides, teaching people how to become and hide their identities as terrorists.[64]

The dark web became a forum for terrorist propaganda, guiding information, and most importantly, funding.[64] With the introduction of Bitcoin, an anonymous transactions were created which allowed for anonymous donations and funding.[64] By accepting Bitcoin, terrorists were now able to fund purchases of weaponry.[64] In 2018, an individual named Ahmed Sarsur was charged for attempting to purchase explosives and hire snipers to aid Syrian terrorists, as well as attempting to provide them financial support, all through the dark web.[35]

There are at least some real and fraudulent websites claiming to be used by ISIL (ISIS), including a fake one seized in Operation Onymous.[65] With the increase of technology, it has allowed cyber terrorists to flourish by attacking the weaknesses of the technology.[66] In the wake of the November 2015 Paris attacks, an actual such site was hacked by an Anonymous-affiliated hacker group, GhostSec, and replaced with an advert for Prozac.[67] The Rawti Shax Islamist group was found to be operating on the dark web at one time.[68]

Social media

Within the dark web, there exists emerging social media platforms similar to those on the World Wide Web, this is known as the Dark Web Social Network (DWSN).[69] The DWSN works a like a regular social networking site where members can have customizable pages, have friends, like posts, and blog in forums. Facebook and other traditional social media platforms have begun to make dark-web versions of their websites to address problems associated with the traditional platforms and to continue their service in all areas of the World Wide Web.[70] Unlike Facebook, the privacy policy of the DWSN requires that members are to reveal absolutely no personal information and remain anonymous.[69]

Hoaxes and unverified content

There are reports of crowdfunded assassinations and hitmen for hire;[71][72] however, these are believed to be exclusively scams.[73][74] The creator of Silk Road, Ross Ulbricht, was arrested by Homeland Security investigations (HSI) for his site and allegedly hiring a hitman to kill six people, although the charges were later dropped.[75][76] There is an urban legend that one can find live murder on the dark web. The term "*Red Room*" has been coined based on the Japanese animation and urban legend of the same name; however, the evidence points toward all reported instances being hoaxes.[77][78]

On June 25, 2015, the indie game *Sad Satan* was reviewed by YouTubers *Obscure Horror Corner* which they claimed to have found via the dark web. Various inconsistencies in the channel's reporting cast doubt on the reported version of events.[79] There are several websites which analyze and monitor the deep web and dark web for threat intelligence.[80]

Policing the dark web

There have been arguments that the dark web promotes civil liberties, like "free speech, privacy, anonymity".[5] Some prosecutors and government agencies are concerned that it is a haven for criminal activity.[81] The deep and dark web are applications of integral internet features to provide privacy and anonymity. Policing involves targeting specific activities of the private web deemed illegal or subject to internet censorship.

When investigating online suspects, police typically use the IP (Internet Protocol) address of the individual; however, due to Tor browsers creating anonymity, this becomes an impossible tactic.[82] As a result, law enforcement has employed many other tactics in order to identify and arrest those engaging in illegal activity on the dark web.[83] OSINT, or Open Source Intelligence, are data collection tools that legally collect information from public sources.[82] OSINT tools can be dark web specific to help officers find bits of information that would lead them to gaining more knowledge about interactions going on in the dark web.[82]

In 2015 it was announced that Interpol now offers a dedicated dark web training program featuring technical information on Tor, cybersecurity and simulated darknet market takedowns.[84] In October 2013 the UK's National Crime Agency and GCHQ announced the formation of a "Joint Operations Cell" to focus on cybercrime. In November 2015 this team would be tasked with tackling child exploitation on the dark web as well as other cybercrime.[85] In March 2017 the Congressional Research Service released an extensive report on the dark web, noting the changing dynamic of how information is accessed and presented on it; characterized by the unknown, it is of increasing interest to researchers, law enforcement, and policymakers.[86] In August 2017, according to reportage, cybersecurity firms which specialize in monitoring and researching the dark web 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.[87]

Journalism

Many journalists, alternative news organizations, educators, and researchers are influential in their writing and speaking of the darknet, and making its use clear to the general public.[88][89] Media coverage typically reports on the dark web in two ways; detailing the power and freedom of speech the dark web allows people to express, or more commonly reaffirms the illegality and fear of its contents, such as computer hackers.[69] Many headlines tie the dark web to child pornography with headlines such as, "N.J. man charged with surfing 'Dark Web' to collect nearly 3K images of child porn",[90] along with other illegal activities where news outlets describe it as "a hub for black markets that sell or distribute drugs".[91][69]

Specialist Clearweb news sites such as DeepDotWeb[92][93] and All Things Vice[94] provide news coverage and practical information about dark web sites and services; however, DeepDotWeb was shut down by authorities in 2019.[95] The Hidden Wiki and its mirrors and forks hold some of the largest directories of content at any given time. Traditional media and news channels such as ABC News have also featured articles examining the darknet.[96][97]

See also

- List of Tor onion services
- Tor (network)

References

1. "Going Dark: The Internet Behind The Internet" (https://www.npr.org/sections/alltechconsidered/2014/05/25/315821415/going-dark-the-internet-behind-the-internet). *NPR*. 25 May 2014. Archived (https://web.archive.org/web/20150527071850/http://www.npr.org/sections/alltechconsidered/2014/05/25/315821415/going-dark-the-internet-behind-the-internet) from the original on 27 May 2015. Retrieved 29 May 2015.
2. Greenberg, Andy (19 November 2014). "Hacker Lexicon: What Is the Dark Web?" (https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/). *Wired*. Archived (https://web.archive.org/web/20150607062159/http://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/) from the original on 7 June 2015. Retrieved 6 June 2015.
3. "Clearing Up Confusion – Deep Web vs. Dark Web" (http://www.brightplanet.com/2014/03/clearing-confusion-deep-web-vs-dark-web/). *BrightPlanet*. 2014-03-27. Archived (https://web.archive.org/web/20150516160539/http://www.brightplanet.com/2014/03/clearing-confusion-deep-web-vs-dark-web/) from the original on 2015-05-16.
4. Egan, Matt (12 January 2015). "What is the dark web? How to access the dark website – How to turn out the lights and access the dark web (and why you might want to)" (http://www.pcadvisor.co.uk/how-to/internet/what-is-dark-web-how-access-dark-web-3593569/). Archived (https://web.archive.org/web/20150619001447/http://www.pcadvisor.co.uk/how-to/internet/what-is-dark-web-how-access-dark-web-3593569/) from the original on 19 June 2015. Retrieved 18 June 2015.
5. Ghappour, Ahmed (2017-09-01). "Data Collection and the Regulatory State" (https://scholarship.law.bu.edu/faculty_scholarship/255). *Connecticut Law Review*. **49** (5): 1733. Archived (https://web.archive.org/web/20210501094925/https://scholarship.law.bu.edu/faculty_scholarship/255/) from the original on 2021-05-01. Retrieved 2020-09-06.
6. Ghappour, Ahmed (2017-04-01). "Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web" (https://scholarship.law.bu.edu/faculty_scholarship/204). *Stanford Law Review*. **69** (4): 1075. Archived (https://web.archive.org/web/20210420104454/https://scholarship.law.bu.edu/faculty_scholarship/204/) from the original on 2021-04-20. Retrieved 2020-09-06.
7. Solomon, Jane (6 May 2015). "The Deep Web vs. The Dark Web: Do You Know The Difference?" (http://blog.dictionary.com/dark-web/). Archived (http://webarchive.loc.gov/all/20150509023641/http://blog.dictionary.com/dark-web/) from the original on 9 May 2015. Retrieved 26 May 2015.
8. "The dark web Revealed" (https://www.popsci.com/dark-web-revealed/). *Popular Science*. pp. 20–21. Archived (https://web.archive.org/web/20150318195338/https://www.popsci.com/dark-web-revealed/) from the original on 2015-03-18. Retrieved 2021-04-15.

9. "Clearnet vs hidden services – why you should be careful" (https://web.archive.org/web/20150628204337/https://www.deepdotweb.com/jolly-rogers-security-guide-for-beginners/clearnet-vs-hidden-services-why-you-should-be-careful/). *DeepDotWeb*. Archived from the original (http://www.deepdotweb.com/jolly-rogers-security-guide-for-beginners/clearnet-vs-hidden-services-why-you-should-be-careful/) on 28 June 2015. Retrieved 4 June 2015.
10. Chacos, Brad (12 August 2013). "Meet Darknet, the hidden, anonymous underbelly of the searchable Web" (http://www.pcworld.com/article/2046227/meet-darknet-the-hidden-anonymous-underbelly-of-the-searchable-web.html). *PC World*. Archived (https://web.archive.org/web/20150812065847/http://www.pcworld.com/article/2046227/meet-darknet-the-hidden-anonymous-underbelly-of-the-searchable-web.html) from the original on 12 August 2015. Retrieved 16 August 2015.
11. Hatta, Masayuki (December 2020). "Deep web, dark web, dark net: A taxonomy of "hidden" Internet" (https://doi.org/10.7880%2Fabas.0200908a). *Annals of Business Administrative Science*. **19** (6): 277–292. doi:10.7880/abas.0200908a (https://doi.org/10.7880%2Fabas.0200908a).
12. Lacey, David; Salmon, Paul M (2015). "It's Dark in There: Using Systems Analysis to Investigate Trust and Engagement in Dark Web Forums". In Harris, Don (ed.). *Engineering Psychology and Cognitive Ergonomics*. Lecture Notes in Computer Science. Vol. 9174. Cham: Springer International Publishing. pp. 117–128. doi:10.1007/978-3-319-20373-7_12 (https://doi.org/10.1007%2F978-3-319-20373-7_12). ISBN 978-3-319-20372-0.
13. Beckett, Andy (26 November 2009). "The dark side of the internet" (https://www.theguardian.com/technology/2009/nov/26/dark-side-internet-freenet). Archived (https://web.archive.org/web/20130908073158/http://www.theguardian.com/technology/2009/nov/26/dark-side-internet-freenet) from the original on 8 September 2013. Retrieved 9 August 2015.
14. "NASA is indexing the 'Deep Web' to show mankind what Google won't" (http://fusion.net/story/145885/nasa-is-indexing-the-deep-web-to-show-mankind-what-google-wont/). *Fusion*. Archived (https://web.archive.org/web/20150630010143/http://fusion.net/story/145885/nasa-is-indexing-the-deep-web-to-show-mankind-what-google-wont/) from the original on 2015-06-30.
15. "The Deep Web and Its Darknets – h+ Media" (https://web.archive.org/web/20150706093936/http://hplusmagazine.com/2015/06/29/the-deep-web-and-its-darknets/). *h+ Media*. 2015-06-29. Archived from the original (http://hplusmagazine.com/2015/06/29/the-deep-web-and-its-darknets/) on 2015-07-06. Retrieved 2016-11-18.
16. Lacson, Wesley; Jones, Beata (2016). "The 21st Century Darknet Market: Lessons From The Fall Of Silk Road" (https://web.archive.org/web/20201212034310/http://cybercrimejournal.com/Lacson%26Jonesvol10issue1IJCC2016.pdf) (PDF). *International Journal of Cyber Criminology*. **10**: 40–61. doi:10.5281/zenodo.58521 (https://doi.org/10.5281%2Fzenodo.58521). Archived from the original (http://cybercrimejournal.com/Lacson%26Jonesvol10issue1IJCC2016.pdf) (PDF) on 2020-12-12. Retrieved 2019-10-02.
17. Moore, Daniel (2016). "Cryptopolitik and the Darknet" (https://doi.org/10.1080%2F00396338.2016.1142085). *Survival*. **58** (1): 7–38. doi:10.1080/00396338.2016.1142085 (https://doi.org/10.1080%2F00396338.2016.1142085).
18. Wimmer, Andreas. "Dark net, Social Media and Extremism: Addressing Indonesian Counterterrorism on the Internet" (https://web.archive.org/web/20170604003640/http://www.academia.edu/20813843/DARKNET_SOCIAL_MEDIA_AND_EXTREMISM_ADDRESSING_INDONESIAN_COUNTERTERRORISM_ON_THE_INTERNET). Archived from the original (https://www.academia.edu/20813843/Dark_net_Social_Media_and_Extremism_Addressing_Indonesian_Counter_terrorism_on_the_Internet) on June 4, 2017 – via www.academia.edu.
19. Moore, Daniel. "Cryptopolitik and the Darknet" (http://www.tandfonline.com/doi/abs/10.1080/00396338.2016.1142085). *Survival: Global Politics and Strategy*. Retrieved 2016-03-20.
20. Cox, Joseph (2016-02-01). "Study Claims Dark Web Sites Are Most Commonly Used for Crimes" (https://motherboard.vice.com/read/study-claims-dark-web-sites-are-most-commonly-used-for-crimes). Retrieved 2016-03-20.

21. Mark, Ward (30 December 2014). "Tor's most visited hidden sites host child abuse images" (https://www.bbc.co.uk/news/technology-30637010). *BBC*. Archived (https://web.archive.org/web/20150425053436/http://www.bbc.co.uk/news/technology-30637010) from the original on 25 April 2015. Retrieved 28 May 2015.
22. "Everything You Need to Know on Tor & the Deep Web" (http://www.whoishostingthis.com/blog/2013/12/17/tor-deep-web/). *whoishostingthis*. Archived (https://web.archive.org/web/20150702225459/http://www.whoishostingthis.com/blog/2013/12/17/tor-deep-web/) from the original on 2 July 2015. Retrieved 18 June 2015.
23. Cox, Joseph (25 February 2015). "What Firewall? China's Fledgling Deep Web Community" (http://motherboard.vice.com/read/what-firewall-chinas-fledgling-deep-web-community). Archived (https://web.archive.org/web/20150620001458/http://motherboard.vice.com/read/what-firewall-chinas-fledgling-deep-web-community) from the original on 20 June 2015. Retrieved 19 June 2015.
24. "Le Dark web en chiffres" (https://www.aleph-networks.com/le-dark-web-en-chiffres/). Archived (https://web.archive.org/web/20210201081906/https://www.aleph-networks.com/le-dark-web-en-chiffres/) from the original on 2021-02-01.
25. Thomson, Iain. "Dark web doesn't exist, says Tor's Dingledine. And folks use network for privacy, not crime" (https://www.theregister.co.uk/2017/07/29/tor_dark_web/). *The Register*. Archived (https://web.archive.org/web/20170731042137/https://www.theregister.co.uk/2017/07/29/tor_dark_web/) from the original on 2017-07-31. Retrieved 2017-07-31.
26. 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). Archived (https://web.archive.org/web/20160312075836/http://motherboard.vice.com/read/study-claims-dark-web-sites-are-most-commonly-used-for-crime) from the original on 12 March 2016. Retrieved 20 March 2016.
27. "Ransomwares, divulgation de données et malware-as-a-service dans le Dark Web. Partie 1/2" (https://www.aleph-networks.com/ransomwares-divulgation-de-donnees-et-malware-as-a-service-dans-le-dark-web-partie-1-2/). Archived (https://web.archive.org/web/20210521235634/https://www.aleph-networks.com/ransomwares-divulgation-de-donnees-et-malware-as-a-service-dans-le-dark-web-partie-1-2/) from the original on 2021-05-21.
28. "Ransomwares, divulgation de données et malware-as-a-service dans le Dark Web. Partie 2/2" (https://www.aleph-networks.com/ransomwares-divulgation-de-donnees-et-malware-as-a-service-dans-le-dark-web-partie-2-2/). Archived (https://web.archive.org/web/20210604094153/https://www.aleph-networks.com/ransomwares-divulgation-de-donnees-et-malware-as-a-service-dans-le-dark-web-partie-2-2/) from the original on 2021-06-04.
29. Reeve, Tom (30 September 2015). "Extortion on the cards" (http://www.scmagazineuk.com/extortion-on-the-cards/article/440385/). Archived (https://web.archive.org/web/20151210184104/http://www.scmagazineuk.com/extortion-on-the-cards/article/440385/) from the original on 10 December 2015. Retrieved 8 December 2015.
30. ElBahrawy, Abeer; Alessandretti, Laura; Rusnac, Leonid; Goldsmith, Daniel; Teytelboym, Alexander; Baronchelli, Andrea (December 2020). "Collective dynamics of dark web marketplaces" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7608591). *Scientific Reports*. **10** (1): 18827. arXiv:1911.09536 (https://arxiv.org/abs/1911.09536). Bibcode:2020NatSR..1018827E (https://ui.adsabs.harvard.edu/abs/2020NatSR..1018827E). doi:10.1038/s41598-020-74416-y (https://doi.org/10.1038%2Fs41598-020-74416-y). PMC 7608591 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7608591). PMID 33139743 (https://pubmed.ncbi.nlm.nih.gov/33139743).
31. Burleigh, Nina (19 February 2015). "The Rise and Fall of Silk Road, the dark web's Amazon" (http://www.newsweek.com/2015/02/27/silk-road-hell-307732.html). Archived (https://web.archive.org/web/20150525141207/http://www.newsweek.com/2015/02/27/silk-road-hell-307732.html) from the original on 25 May 2015. Retrieved 25 May 2015.

32. Rhumorbarbe, Damien; Staehli, Ludovic; Broséus, Julian; Rossy, Quentin; Esseiva, Pierre (2016). "Buying drugs on a Darknet market: A better deal? Studying the online illicit drug market through the analysis of digital, physical and chemical data" (https://serval.unil.ch/notice/serval:BIB_670B021B4620). *Forensic Science International*. **267**: 173–182. doi:10.1016/j.forsciint.2016.08.032 (https://doi.org/10.1016%2Fj.forsciint.2016.08.032). PMID 27611957 (https://pubmed.ncbi.nlm.nih.gov/27611957). Archived (https://web.archive.org/web/20180917143209/https://serval.unil.ch/notice/serval:BIB_670B021B4620) from the original on 2018-09-17. Retrieved 2018-09-10.
33. "Characterising dark net marketplace purchasers in a sample of regular psychostimulant users". *International Journal of Drug Policy*. **35**.
34. "One Million Credit Cards Leaked in a Cybercrime Forum for Free" (https://cyble.com/blog/one-million-credit-cards-leaked-in-a-cybercrime-forum-for-free/). *Cyble*. August 8, 2021. Archived (https://web.archive.org/web/20231112092952/https://cyble.com/blog/one-million-credit-cards-leaked-in-a-cybercrime-forum-for-free/) from the original on November 12, 2023. Retrieved August 9, 2023.
35. Kaur, Shubhdeep; Randhawa, Sukhchandan (June 2020). "Dark Web: A Web of Crimes". *Wireless Personal Communications*. **112** (4): 2131–2158. doi:10.1007/s11277-020-07143-2 (https://doi.org/10.1007%2Fs11277-020-07143-2). S2CID 212996728 (https://api.semanticscholar.org/CorpusID:212996728).
36. Kirkpatrick, Keith (2017-02-21). "Financing the dark web". *Communications of the ACM*. **60** (3): 21–22. doi:10.1145/3037386 (https://doi.org/10.1145%2F3037386). S2CID 32696030 (https://api.semanticscholar.org/CorpusID:32696030).
37. Richet, Jean-Loup (June 2013). "Laundering Money Online: a review of cybercriminals methods". arXiv:1310.2368 (https://arxiv.org/abs/1310.2368) [cs.CY (https://arxiv.org/archive/cs.CY)].
38. Richet, Jean-Loup (2012). "How to Become a Black Hat Hacker? An Exploratory Study of Barriers to Entry Into Cybercrime" (http://aim.asso.fr/index.php/mediatheque/finish/26-aim-2012/816-how-to-become-a-black-hat-hacker-an-exploratory-study-of-barriers-to-entry-into-cybercrime/0). *17th AIM Symposium*. Archived (https://archive.today/20170105033105/http://aim.asso.fr/index.php/mediatheque/finish/26-aim-2012/816-how-to-become-a-black-hat-hacker-an-exploratory-study-of-barriers-to-entry-into-cybercrime/0) from the original on 2017-01-05.
39. * Allison, Ian (11 February 2015). "Bitcoin tumbler: The business of covering tracks in the world of cryptocurrency laundering" (http://www.ibtimes.co.uk/bitcoin-tumbler-business-covering-tracks-world-cryptocurrency-laundering-1487480). *International Business Times*. Archived (https://web.archive.org/web/20150924045528/http://www.ibtimes.co.uk/bitcoin-tumbler-business-covering-tracks-world-cryptocurrency-laundering-1487480) from the original on 24 September 2015. Retrieved 8 December 2015.
40. "Helix Updates: Integrated Markets Can Now Helix Your BTC" (https://web.archive.org/web/20160221052629/https://www.deepdotweb.com/2014/08/05/helix-updates-integrated-markets-can-now-helix-your-btc/). 5 August 2015. Archived from the original (https://www.deepdotweb.com/2014/08/05/helix-updates-integrated-markets-can-now-helix-your-btc/) on 21 February 2016. Retrieved 8 December 2015.
41. Holden, Alex (15 January 2015). "A new breed of lone wolf hackers are roaming the deep web – and their prey is getting bigger" (http://www.ibtimes.co.uk/new-breed-lone-wolf-hackers-are-roaming-deep-web-their-prey-getting-bigger-1483347). *International Business Times*. Archived (https://web.archive.org/web/20150628214900/http://www.ibtimes.co.uk/new-breed-lone-wolf-hackers-are-roaming-deep-web-their-prey-getting-bigger-1483347) from the original on 28 June 2015. Retrieved 19 June 2015.

42. "Hacking communities in the Deep Web" (http://resources.infosecinstitute.com/hacking-communities-in-the-deep-web/). 15 May 2015. Archived (https://archive.today/20160428194946/https://webcache.googleusercontent.com/search?q=cache:H8DbduIEh7sJ:resources.infosecinstitute.com/hacking-communities-in-the-deep-web/) from the original on 28 April 2016. Retrieved 5 September 2017.
43. Cox, Joseph (12 November 2015). "A Dark Web Hacker Is Hunting Potential Pedophiles to Extort Them for Money" (https://www.vice.com/en/article/aekzjz/a-dark-web-hacker-is-hunting-potential-pedophiles-to-extort-them-for-money). Archived (https://web.archive.org/web/20151115071739/http://motherboard.vice.com/en_uk/read/a-dark-web-hacker-is-hunting-potential-pedophiles-to-extort-them-for-money) from the original on 15 November 2015. Retrieved 12 November 2015.
44. "The Dark Net: Policing the Internet's Underworld". *World Policy Journal*. **32**.
45. "Large-Scale Monitoring for Cyber Attacks by Using Cluster Information on Darknet Traffic Features". *Procedia Computer Science*. **53**.
46. Fachkha, Claude; Bou-Harb, Elias; Debbabi, Mourad (2015). "Inferring distributed reflection denial of service attacks from darknet". *Computer Communications*. **62**: 59–71. doi:10.1016/j.comcom.2015.01.016 (https://doi.org/10.1016%2Fj.comcom.2015.01.016).
47. Cluley, Graham (June 20, 2023). "100,000 hacked ChatGPT accounts up for sale on the dark web" (https://www.bitdefender.com/blog/hotforsecurity/100-000-hacked-chatgpt-accounts-up-for-sale-on-the-dark-web/). *Bitdefender*. Archived (https://web.archive.org/web/20230902100332/https://www.bitdefender.com/blog/hotforsecurity/100-000-hacked-chatgpt-accounts-up-for-sale-on-the-dark-web/) from the original on September 2, 2023. Retrieved September 2, 2023.
48. "Flashpoint, Leading Deep and Dark Web Intelligence Provider, Raises $5 Million in Financing Round" (https://www.prnewswire.com/news-releases/flashpoint-leading-deep-and-dark-web-intelligence-provider-raises-5-million-in-financing-round-300067671.html) (Press release). New York: PRNewswire. April 17, 2015. Archived (https://web.archive.org/web/20191002162237/https://www.prnewswire.com/news-releases/flashpoint-leading-deep-and-dark-web-intelligence-provider-raises-5-million-in-financing-round-300067671.html) from the original on October 2, 2019. Retrieved October 2, 2019.
49. Cox, Joseph (14 January 2016). "Dark Web Vendor Sentenced for Dealing Counterfeit Coupons" (http://motherboard.vice.com/read/dark-web-vendor-sentenced-for-dealing-counterfeit-coupons). Archived (https://web.archive.org/web/20160124030533/http://motherboard.vice.com/read/dark-web-vendor-sentenced-for-dealing-counterfeit-coupons) from the original on 24 January 2016. Retrieved 24 January 2016.
50. "Secrets to Unmasking Bitcoin Scams – 4 Eye Opening Case Studies" (https://web.archive.org/web/20151116122618/https://www.deepdotweb.com/2015/05/28/secrets-to-unmasking-bitcoin-scams-4-eye-opening-case-studies/). 28 May 2015. Archived from the original (https://www.deepdotweb.com/2015/05/28/secrets-to-unmasking-bitcoin-scams-4-eye-opening-case-studies/) on 16 November 2015. Retrieved 12 November 2015.
51. Stockley, Mark (1 July 2015). "Hundreds of Dark Web sites cloned and "booby trapped" " (https://nakedsecurity.sophos.com/2015/07/01/hundreds-of-dark-web-sites-cloned-and-booby-trapped/). Archived (https://web.archive.org/web/20151211024549/https://nakedsecurity.sophos.com/2015/07/01/hundreds-of-dark-web-sites-cloned-and-booby-trapped/) from the original on 11 December 2015. Retrieved 8 December 2015.
52. Fox-Brewster, Thomas (18 November 2014). "Many Sites That Fell In Epic Onymous Tor Takedown 'Were Scams Or Legit' " (https://www.forbes.com/sites/thomasbrewster/2014/11/18/tor-takedown-misinformation/). *Forbes*. Archived (https://web.archive.org/web/20150619220607/http://www.forbes.com/sites/thomasbrewster/2014/11/18/tor-takedown-misinformation/) from the original on 19 June 2015. Retrieved 19 June 2015.

53. "Beware of Phishing Scams On Clearnet Sites! (darknetmarkets.org)" (https://web.archive.org/web/20160222003543/https://www.deepdotweb.com/2015/07/03/beware-of-phishing-scams-on-clearnet-sites-darknetmarkets-org/). DeepDotWeb. 3 July 2015. Archived from the original (https://www.deepdotweb.com/2015/07/03/beware-of-phishing-scams-on-clearnet-sites-darknetmarkets-org/) on 22 February 2016. Retrieved 8 December 2015.
54. "Warning: More Onion Cloner Phishing Scams" (https://web.archive.org/web/20151220111815/https://www.deepdotweb.com/2015/04/22/reminder-onion-cloner-phishing-scams/). 22 April 2015. Archived from the original (https://www.deepdotweb.com/2015/04/22/reminder-onion-cloner-phishing-scams/) on 20 December 2015. Retrieved 8 December 2015.
55. Willacy, Mark (26 August 2015). "Secret 'dark net' operation saves scores of children from abuse; ringleader Shannon McCoole behind bars after police take over child porn site" (http://www.abc.net.au/news/2015-08-26/secret-anti-paedophile-operation-saves-children-from-abuse/6720304). Archived (https://web.archive.org/web/20150826064840/http://www.abc.net.au/news/2015-08-26/secret-anti-paedophile-operation-saves-children-from-abuse/6720304) from the original on 26 August 2015. Retrieved 26 August 2015.
56. Conditt, Jessica (8 January 2016). "FBI hacked the Dark Web to bust 1,500 pedophiles" (https://web.archive.org/web/20160108092655/http://www.engadget.com/2016/01/07/fbi-hacked-the-dark-web-to-bust-1-500-pedophiles/). Archived from the original (https://www.engadget.com/2016/01/07/fbi-hacked-the-dark-web-to-bust-1-500-pedophiles/) on 8 January 2016. Retrieved 8 January 2016.
57. *Cox, Joseph (5 January 2016). "The FBI's 'Unprecedented' Hacking Campaign Targeted Over a Thousand Computers" (https://motherboard.vice.com/read/the-fbis-unprecedented-hacking-campaign-targeted-over-a-thousand-computers). Archived (https://web.archive.org/web/20160108050547/http://motherboard.vice.com/read/the-fbis-unprecedented-hacking-campaign-targeted-over-a-thousand-computers) from the original on 8 January 2016. Retrieved 8 January 2016.
58. Farivar, Cyrus (16 June 2015). "Feds bust through huge Tor-hidden child porn site using questionable malware" (https://arstechnica.com/tech-policy/2015/07/feds-bust-through-huge-tor-hidden-child-porn-site-using-questionable-malware/). *Ars Technica*. Archived (https://web.archive.org/web/20150809031658/http://arstechnica.com/tech-policy/2015/07/feds-bust-through-huge-tor-hidden-child-porn-site-using-questionable-malware/) from the original on 9 August 2015. Retrieved 8 August 2015.
59. Evans, Robert (16 June 2015). "5 Things I Learned Infiltrating Deep Web Child Molesters" (http://www.cracked.com/personal-experiences-1760-5-things-i-learned-infiltrating-deep-web-child-molesters.html). Archived (https://web.archive.org/web/20150826045459/http://www.cracked.com/personal-experiences-1760-5-things-i-learned-infiltrating-deep-web-child-molesters.html) from the original on 26 August 2015. Retrieved 29 August 2015.
60. Cox, Joseph (11 November 2014). "As the FBI Cleans the Dark Net, Sites Far More Evil Than Silk Road Live On" (http://motherboard.vice.com/read/as-the-fbi-cleans-the-dark-net-sites-far-more-evil-than-silk-road-live-on). Archived (https://web.archive.org/web/20150726082027/http://motherboard.vice.com/read/as-the-fbi-cleans-the-dark-net-sites-far-more-evil-than-silk-road-live-on) from the original on 26 July 2015. Retrieved 3 August 2015.
61. Markowitz, Eric (10 July 2014). "The Dark Net: A Safe Haven for Revenge Porn?" (http://www.vocativ.com/tech/internet/dark-net-safe-haven-revenge-porn/?PageSpeed=noscript). Archived (https://web.archive.org/web/20151126051539/http://www.vocativ.com/tech/internet/dark-net-safe-haven-revenge-porn/?PageSpeed=noscript) from the original on 26 November 2015. Retrieved 3 August 2015.
62. "4 arrested in takedown of dark web child abuse platform with some half a million users" (https://www.europol.europa.eu/newsroom/news/4-arrested-in-takedown-of-dark-web-child-abuse-platform-some-half-million-users). *Europol*. 3 May 2021. Archived (https://web.archive.org/web/20210503235306/https://www.europol.europa.eu/newsroom/news/4-arrested-in-takedown-of-dark-web-child-abuse-platform-some-half-million-users) from the original on 3 May 2021. Retrieved 3 May 2021.

63. "Child sexual abuse: Four held in German-led raid on huge network" (https://www.bbc.com/news/world-europe-56969414). *BBC*. 3 May 2021. Archived (https://web.archive.org/web/20210503220614/https://www.bbc.com/news/world-europe-56969414) from the original on 3 May 2021. Retrieved 3 May 2021.
64. Weimann, Gabriel (2016-03-03). "Going Dark: Terrorism on the Dark Web" (https://doi.org/10.1080%2F1057610X.2015.1119546). *Studies in Conflict & Terrorism*. **39** (3): 195–206. doi:10.1080/1057610X.2015.1119546 (https://doi.org/10.1080%2F1057610X.2015.1119546). ISSN 1057-610X (https://search.worldcat.org/issn/1057-610X).
65. Cub, Nik (17 November 2014). "FBI seizes fake Tor hosted Jihad funding website as part of Operation Onymous, leaves up real site" (https://www.nikcub.com/posts/fbi-seizes-fake-tor-hosted-jihad-funding-website-as-part-of-operation-onymous-leaves-up-real-site/). Archived (https://web.archive.org/web/20160114103244/https://www.nikcub.com/posts/fbi-seizes-fake-tor-hosted-jihad-funding-website-as-part-of-operation-onymous-leaves-up-real-site/) from the original on 14 January 2016. Retrieved 25 November 2015.
66. Vilić, Vida M. (December 2017). "Dark Web, Cyber Terrorism and Cyber Warfare: Dark Side of the Cyberspace" (http://js.ugd.edu.mk/index.php/BSSR/article/download/1939/1708) (PDF). *Balkan Social Science Review*. **10** (10): 7–24. Archived (https://web.archive.org/web/20191002162239/http://js.ugd.edu.mk/index.php/BSSR/article/download/1939/1708) from the original on 2019-10-02. Retrieved 2019-10-02.
67. Cuthbertson, Anthony (25 November 2015). "Hackers replace dark web Isis propaganda site with advert for Prozac" (http://www.ibtimes.co.uk/hackers-replace-dark-web-isis-propaganda-site-advert-prozac-1530385). *International Business Times*. Archived (https://web.archive.org/web/20151126061126/http://www.ibtimes.co.uk/hackers-replace-dark-web-isis-propaganda-site-advert-prozac-1530385) from the original on 26 November 2015. Retrieved 25 November 2015.
68. "Jihadist cell in Europe 'sought recruits for Iraq and Syria' " (https://www.bbc.com/news/world-europe-34802317). *BBC*. 12 November 2015. Archived (https://web.archive.org/web/20160418173322/http://www.bbc.com/news/world-europe-34802317) from the original on 18 April 2016.
69. Gehl RW (August 2016). "Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network" (https://doi.org/10.1177%2F1461444814554900). *New Media & Society*. **18** (7): 1219–1235. doi:10.1177/1461444814554900 (https://doi.org/10.1177%2F1461444814554900).
70. Brooke, Zach (Spring 2016). "A Marketer's Guide to the Dark Web". *Marketing Insights*. **28** (1): 23–27.
71. Holden, Alex (10 February 2015). "Ukraine crisis: Combatants scouring dark web for advice on bridge bombing and anti-tank missiles" (http://www.ibtimes.co.uk/ukraine-combatants-turn-dark-web-advice-bridge-bombing-anti-tank-missiles-1487256). *International Business Times*. Archived (https://web.archive.org/web/20150529033616/http://www.ibtimes.co.uk/ukraine-combatants-turn-dark-web-advice-bridge-bombing-anti-tank-missiles-1487256) from the original on 29 May 2015. Retrieved 28 May 2015.
72. Greenberg, Andy (18 November 2013). "Meet The 'Assassination Market' Creator Who's Crowdfunding Murder With Bitcoins" (https://www.forbes.com/sites/andygreenberg/2013/11/18/meet-the-assassination-market-creator-whos-crowdfunding-murder-with-bitcoins/). *Forbes*. Archived (https://web.archive.org/web/20150905112902/http://www.forbes.com/sites/andygreenberg/2013/11/18/meet-the-assassination-market-creator-whos-crowdfunding-murder-with-bitcoins/) from the original on 5 September 2015. Retrieved 29 August 2015.
73. * Cox, Joseph (18 May 2016). "This Fake Hitman Site Is the Most Elaborate, Twisted Dark Web Scam Yet" (http://motherboard.vice.com/read/this-fake-hitman-site-is-the-most-elaborate-twisted-dark-web-scam-yet). Archived (https://web.archive.org/web/20160621162426/http://motherboard.vice.com/read/this-fake-hitman-site-is-the-most-elaborate-twisted-dark-web-scam-yet) from the original on 21 June 2016. Retrieved 20 June 2016.

74. Ormsby, Eileen (3 August 2012). "Conversation with a hitman (or not)" (http://allthingsvice.com/2012/08/03/conversation-with-a-hitman-or-not/). Archived (https://web.archive.org/web/20150904041728/http://allthingsvice.com/2012/08/03/conversation-with-a-hitman-or-not/) from the original on 4 September 2015. Retrieved 29 August 2015.
75. Hong N (May 29, 2015). "Silk Road Founder Ross Ulbricht Sentenced to Life in Prison" (https://web.archive.org/web/20170613152211/https://www.wsj.com/articles/silk-road-founder-ross-ulbricht-sentenced-to-life-in-prison-1432929957). *The Wall Street Journal*. Archived from the original (https://www.wsj.com/articles/silk-road-founder-ross-ulbricht-sentenced-to-life-in-prison-1432929957) on 2017-06-13.
76. Greenberg A (May 29, 2015). "Silk Road Creator Ross Ulbricht Sentenced to Life in Prison" (https://web.archive.org/web/20150529215648/http://www.wired.com/2015/05/silk-road-creator-ross-ulbricht-sentenced-life-prison/). *Wired*. Archived from the original (https://www.wired.com/2015/05/silk-road-creator-ross-ulbricht-sentenced-life-prison/) on 2015-05-29.
77. Ormsby, Eileen (29 August 2015). "Waiting in the Red Room" (http://allthingsvice.com/2015/08/29/waiting-in-the-red-room/). Archived (https://web.archive.org/web/20150829232621/http://allthingsvice.com/2015/08/29/waiting-in-the-red-room/) from the original on 29 August 2015. Retrieved 29 August 2015.
78. Howell O'Neill, Patrick (28 August 2015). "Dark Net site promised to livestream torture and execution of 7 ISIS jihadists" (http://www.dailydot.com/politics/isis-red-room-dark-net-live-stream/). Archived (https://web.archive.org/web/20150911183336/http://www.dailydot.com/politics/isis-red-room-dark-net-live-stream/) from the original on 11 September 2015. Retrieved 29 August 2015.
79. Barton, Hannah (25 October 2015). "The spooky, twisted saga of the Deep Web horror game 'Sad Satan' " (http://kernelmag.dailydot.com/issue-sections/features-issue-sections/14763/sad-satan-deep-web-horror-game/#sthash.axwtQ6De.dpuf). Archived (https://web.archive.org/web/20151123034014/http://kernelmag.dailydot.com/issue-sections/features-issue-sections/14763/sad-satan-deep-web-horror-game/#sthash.axwtQ6De.dpuf) from the original on 23 November 2015. Retrieved 22 November 2015.
80. "The Deep Web and its Darknets" (http://hplusmagazine.com/2015/06/29/the-deep-web-and-its-darknets/). 2015-06-29. Archived (https://web.archive.org/web/20150706093936/http://hplusmagazine.com/2015/06/29/the-deep-web-and-its-darknets/) from the original on 2015-07-06. Retrieved 2016-11-22.
81. Lev Grossman (11 November 2013). "The Secret Web: Where Drugs, Porn and Murder Live Online" (http://content.time.com/time/magazine/article/0,9171,2156271,00.html). *Time*. Archived (https://web.archive.org/web/20140228175548/http://content.time.com/time/magazine/article/0,9171,2156271,00.html) from the original on 28 February 2014.
82. Davies, Gemma (October 2020). "Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers" (https://doi.org/10.1177%2F0022018320952557). *The Journal of Criminal Law*. **84** (5): 407–426. doi:10.1177/0022018320952557 (https://doi.org/10.1177%2F0022018320952557).
83. "7 Ways the Cops Will Bust You on the Dark Web" (https://www.vice.com/en/article/vv73pj/7-ways-the-cops-will-bust-you-on-the-dark-web). *www.vice.com*. Archived (https://web.archive.org/web/20210309001514/https://www.vice.com/en/article/vv73pj/7-ways-the-cops-will-bust-you-on-the-dark-web) from the original on 2021-03-09. Retrieved 2021-03-20.
84. Ricard (2 August 2015). "Interpol Dark Web Training Course" (https://archive.today/20160428194934/http://darkwebnews.com/news/interpol-dark-web-training-course/). Archived from the original (http://darkwebnews.com/news/interpol-dark-web-training-course/) on 28 April 2016. Retrieved 8 August 2015.
85. Cox, Joseph (8 November 2015). "The UK Will Police the Dark Web with a New Task Force" (http://motherboard.vice.com/read/the-uk-will-police-the-dark-web-with-a-new-task-force). Archived (https://web.archive.org/web/20151110192004/http://motherboard.vice.com/read/the-uk-will-police-the-dark-web-with-a-new-task-force) from the original on 10 November 2015. Retrieved 9 November 2015.

86. Finklea, Kristin (2017-03-10). "Dark Web" (https://fas.org/sgp/crs/misc/R44101.pdf) (PDF). Archived (https://web.archive.org/web/20170320192455/https://fas.org/sgp/crs/misc/R44101.pdf) (PDF) from the original on 2017-03-20.
87. 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*.
88. Burrell, Ian (August 28, 2014). "The Dark Net: Inside the Digital Underworld by Jamie Bartlett, book review" (https://www.independent.co.uk/arts-entertainment/books/reviews/the-dark-netinside-the-digital-underworld-by-jamie-bartlett-book-review-9696473.html). *The Independent*. Archived (https://web.archive.org/web/20150620142200/http://www.independent.co.uk/arts-entertainment/books/reviews/the-dark-netinside-the-digital-underworld-by-jamie-bartlett-book-review-9696473.html) from the original on June 20, 2015.
89. "The Growth of Dark Subcultures On the Internet, The Leonard Lopate Show" (http://www.wnyc.org/story/growth-dark-subcultures-internet/). *WNYC*. June 2, 2015. Archived (https://web.archive.org/web/20161020043736/http://www.wnyc.org/story/growth-dark-subcultures-internet/) from the original on October 20, 2016.
90. Attrino, Anthony G. (2020-12-22). "N.J. man charged with surfing 'Dark Web' to collect nearly 3K images of child porn, prosecutor says" (https://www.nj.com/bergen/2020/12/nj-man-charged-with-surfing-dark-web-to-collect-nearly-3k-images-of-child-porn-prosecutor-says.html). *nj*. Archived (https://web.archive.org/web/20210421023611/https://www.nj.com/bergen/2020/12/nj-man-charged-with-surfing-dark-web-to-collect-nearly-3k-images-of-child-porn-prosecutor-says.html) from the original on 2021-04-21. Retrieved 2021-04-21.
91. Pagliery, Jose (March 10, 2014). "The Deep Web you don't know about" (https://money.cnn.com/2014/03/10/technology/deep-web/). *CNN Business*. Archived (https://web.archive.org/web/20210303185528/https://money.cnn.com/2014/03/10/technology/deep-web/) from the original on March 3, 2021. Retrieved March 27, 2021.
92. * Swearingen, Jake (2 October 2014). "A Year After Death of Silk Road, Darknet Markets Are Booming" (https://finance.yahoo.com/news/death-silk-road-darknet-markets-142500702.html). Archived (https://web.archive.org/web/20150525021911/https://finance.yahoo.com/news/death-silk-road-darknet-markets-142500702.html) from the original on 25 May 2015. Retrieved 24 May 2015.
93. Franceschi-Bicchierai, Lorenzo (13 May 2015). "Hackers Tried To Hold a Darknet Market For a Bitcoin Ransom" (http://motherboard.vice.com/read/hackers-tried-to-hold-a-darknet-market-for-a-bitcoin-ransom). Archived (https://web.archive.org/web/20150517065101/http://motherboard.vice.com/read/hackers-tried-to-hold-a-darknet-market-for-a-bitcoin-ransom) from the original on 17 May 2015. Retrieved 19 May 2015.
94. Solon, Olivia (3 February 2013). "Police crack down on Silk Road following first drug dealer conviction" (https://arstechnica.com/tech-policy/2013/02/police-crack-down-on-silk-road-following-first-drug-dealer-conviction/). Archived (https://web.archive.org/web/20150528032024/http://arstechnica.com/tech-policy/2013/02/police-crack-down-on-silk-road-following-first-drug-dealer-conviction/) from the original on 28 May 2015. Retrieved 27 May 2015.
95. Kan, Michael (May 7, 2019). "Feds Seize DeepDotWeb for Taking Money From Black Market Sites" (https://www.pcmag.com/news/368198/feds-seize-deepdotweb-for-taking-money-from-black-market-sit). *PCMAG*. Archived (https://web.archive.org/web/20190507180831/https://www.pcmag.com/news/368198/feds-seize-deepdotweb-for-taking-money-from-black-market-sit) from the original on 2019-05-07. Retrieved 2019-12-28.
96. Viney, Steven (January 27, 2016). "What is the dark net, and how will it shape the future of the digital age?" (http://www.abc.net.au/news/2016-01-27/explainer-what-is-the-dark-net/7038878). *ABC*. Archived (https://web.archive.org/web/20161020060907/http://www.abc.net.au/news/2016-01-27/explainer-what-is-the-dark-net/7038878) from the original on October 20, 2016.
97. "The Other Internet". *Vanity Fair*. Vol. 58.

External links

- 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 (https://www.twitch.tv/videos/128466707)
- Attacks Landscape in the Dark Side of the Web (http://www.madlab.it/papers/sac17_darknets.pdf)