ЕКОНОМИКА
ISSN 0350-137X, EISSN 2334-9190, UDK 338 (497,1)
Vol. 63, january-march 2017, № 1
P. 73-82

Zaklina Spalevic[1]
Singidunum University, Faculty of Tourism and Hospitality Management, Belgrade

Milos Ilic[2]
University of Pristina, Faculty of Technical Science, Kosovska Mitrovica

SCIENTIFIC REVIEW ARTICLE
doi:10.5937/ekonomika1701073S
Received: December, 27, 2016
Accepted: January, 31, 2017

THE USE OF DARK WEB FOR THE PURPOSE OF ILLEGAL ACTIVITY SPREADING

Abstract

The development of information and communication technologies, especially the Internet, has led to drastic changes in all spheres of human life and work. Although some of these changes have very positive effects, others are extremely negative. One example of the latter is a new kind of terrorism and criminal activity which is based on the use of the non-indexed part of the Internet which is called dark Web. Generally positive features such as access to information about Internet users, anonymity and protection of personal data are used with the evil intention of acquiring illegal profit and spreading ethnic hatred and intolerance. This paper gives a brief overview of documented ways for accessing this part of web, and examples of abuses of its features.

Key words: *Dark web, Deep Web, Cyber terrorism, Tor, I2P.*

JEL classification: K24

УПОТРЕБА DARK WEB-А У У ЦИЉУ ШИРЕЊА ИЛЕГАЛНИХ АКТИВНОСТИ

Апстракт

Развој информационо комуникационих технологија, пре свега Интернета, довео је до драстичних промена у свим доменима људског живота и рада. Неке од ових промена имале су веома позитивне ефекте, док су поједине имале крајње негативне и непожељне. Једна од таквих промена јесте појава нове врсте тероризма и криминалних активности која се заснива на употреби неиндексираног дела Интернета који је назван дарк веб. Позитивне могућности у виду доступности информација сваком од корисника Интернета, анонимности и заштите личних података овде су искоришћене са крајње злом намером стицања нелегелне добити и ширења националне мржње и нетрпељивости. Рад даје кратак преглед документованих начина приступа овом делу веб-а, као и примере злоупотребе његових могућности.

Ključne reči: *Tamni web, Duboki web, Cyber terorizam, Tor, I2P*

[1] zspalevic@singidunum.ac.rs.

[2] milos.ilic@pr.ac.rs

Introduction

The Internet, used on a daily basis by personal users, as well as by commercial companies and organizations, includes all sites and portals that are indexed by a public web browser. These sites and portals are connected with each other via the incoming and outgoing links. These pages are crawled by indexing robots using links that lead to them and links that lead from them to other websites (PC, 2015).

These pages are expected to be static, installed on the servers and to have visible html code. Any change to the web portal or any page results with new content being uploaded to the server. In this way, the entire process is visible and public. Another feature of the Internet is the DNS (Domain Name System) database, which associates hostnames with their IP addresses. DNS databases are defined and used to enable transparency, to control the flow of information and to protect users from spam or certain contents. Increasing control and monitoring of Internet users in terms of information and content they publish and portals that visit, has led to development of a different version of the Internet, where the degree of anonimity is higher. Many users are aware that everything that is published on the Internet remains permanently visible in some form. That is why even the average user comes to the idea that at least for some of the activities should use so-called dark Web, or deep Web. Dark Web is a general network which can be accessed only by using specific software, configuration, or with the authorization, often using non-standard communication protocols and ports.

Unlike static pages from the indexed part of the Internet (visible Internet), dark web pages are dynamic, with html code created based on results of contents retrieved from their own databases. This method for creating independent web site makes crawling this site imposible for indexing robots. Precisely, this is one of the reasons why these pages remain non-indexed by the public Internet browser (Goodman, 2015). From another side dark web weba sites contain rich content used for routine communication and propaganda dissemination (Abbasi & Chen; 2005). These forums contain static and dynamic text files, archive files, and various forms of multimedia. Collection of such diverse-content types introduces many unique challenges not encountered with standard spidering of indexable files. On a related note, a Dark Web forum crawler also must assess the merits of various collection-update strategies. It is for this reason that the idea of high degree of anonymity in communication and work was used by malicious users in order to address the various illegal activities, from rental services, through drug trafficking and weapons, to human trafficking.

The paper is organized as follows. The second part shows the theoretical background of deep web and dark web, different ways of accessing as well as similarities and differences with the visible part of the Internet. The third part presents examples of the use of dark web services, from the user perspective. Also, examples of different illegal activities that can be found by searching dark web are presented. The fourth part discusses the key conclusions of this study. Last section provides a list of references used to gather information about dark web and illegal activities on it.

Deep and dark web

In the literature and everyday use, when referring to non-indexed part of the Internet two terms are intertwined: dark and deep web. Deep Web is a term that encompasses

everything that Google and other public Internet browsers are not indexing, and therefore can not be returned as search result. These may be trivial, such as comments on the forums that can be accessed only by registered users, Facebook posts that are set so that only friends can see, private YouTube content which can be accessed only via forwarded link. Also, academic articles that require subsription fee in order to gain access, as well as many other similar item (Todorovic, 2015).

Dark Web is a certain amount of content on the deep web used for promotion or distribution of illegal activities. Web sites that allow dealing with illegal activities are mostly hidden behind *.onion* web domain and can be accessed using special search engines (Todorovic, 2015). Dark Web is almost completely anonymous, and it is therefore used by groups that want to remain hidden from the government institutions and agencies in charge of law enforcement. To further protect the users of such systems, money transactions are performed using a specially created digital currency called Bitcoin. Creation and encryption of the currency is supported by the organization that manages the payment, bitcoins transfer and their conversion into conventional money flows.

One of the ways to access dark web is Tor (*The Onion Router*) network, whose primary purpose is to serve as a gateway to this part of the Internet. To hide the address of the Internet user, Tor redirect signals through nearly 6,000 servers (Cekerevac, Dvorak, & Cekerevac, 2016). So as to create a private and secure connection inside the Tor network, the client application incrementally builds a connection between the source and destination of data packets, which consists of encrypted connection between randomly selected server nodes. This relationship occurs in steps, so that individual server knows only from which server packets are received and to which server they should be forwarded. This is achieved by using a special key for encryption at every step. Once the connection is established it is possible to transmit different types of data using different software packages (CARNet, 2007).

Apart from Tor-a which is in most cases used to share files, I2P (*Invisible Internet Project*) network layer is used to provide anonymous communication between applications. This layer supports a variety of protocols and applications. Each established connection between two users is being protected using special encryption. The comparison of functionality and security offered by Tor and I2P has shown that I2P is more resistant to attacks by analyzing traffic flow data (Mergen, 2015).

Freenet is another similar solution that is simpler and more convenient use by the broad masses. Access is done from the browser, while in the background the application establishes a connection. The user can choose the level of security on the network. All the communication and sharing of files is via P2P, and every time one establishes the connection, new path is created. For this reason, every reopening of pages takes more time than in the case with the other aforementioned sector and technologies.

The police fact that close to 300,000 Germans are using some form of access dark web network testifies to the popularity of this service. The data show that, at global level, more than three million users access the content of dark web. If we compare the amount of data stored in the dark web, it is forty times larger than the visible part of the web and is about 750 terabytes. The entire content is mostly stored in specific databases, as property of the organizations and individuals (Arslani, 2015). Based on this, the visible part of web is about 4%, while the remaining 96% belong to the deep web.

Examples of the use of dark web services

In different types of researches five categories of terroristic activities on the Internet are identified. Those categories are: propaganda (to disseminate radical messages), recruitment and training (to encourage people to join the Jihad or other terrorist organizations, and get online training), fundraising (to transfer funds, conduct credit card fraud and other money laundering activities), communications (to provide instruction, resources, and support via email, digital photographs, and chat session), and targeting (to conduct online surveillance and identify vulnerabilities of potential targets such as airports). Besides these categories, dark web services are in use for many other abuses (Tsfati, & Weimann, 2002). Some of the examples collected from different sources are described in following paragraphs.

One of the examples of the dark web usage disclosed by the competent anti-drug entities is a portal for drug and other illegal goods trafficking called Silk Road. Its founder and owner was Ross Ulbrich, 29 year old programmer, who introduced himself under a pseudonym Dread Pirate Roberts. Ample evidence was found on his laptop. From 2011 to 2013 he created an empire worth $ 1.2 billion, only with the help of a laptop and the Internet. After only three weeks of trial, the jury of twelve declared Ulbricht guilty on all seven counts, including one on charges of money laundering, drug trafficking and computer hacking. He was discovered when the police found his message from 2010 where, at the time of carelessness, he was referring interested parties to visit the Silk Road, signed a different name ("altoid"), under which he sought professionals in bitcoin community to be the leading developers, and gave the address for communication (Amika, 2016; Zetter, 2013). This site was operated like any other portal for online purchases. Ordered goods were delivered by postal companies. Postal companies do not check the contents of the shipment in order to provide better services to users, making this method of delivery a very convinient way for illegal trade. At the same time postal company can face problems if the competent authorities establish that the it is often used for these types of delivery (Spalevic, Ilic, & Palevic, 2016). The elentlessness of people who deal with this kind of crime is evidenced by the fact that only a month after Ulbrich arrest and closing of the portal, portal became active again in the dark web, this time in version 2.0. The site quickly expanded and, according to data from the FBI, had an average of 150,000 visitors and monthly income of around $ 8 million from the sale of goods and services. After a year's work site was shut down, while the administrator Blake Benthall arrested (Cook, 2014). That lasted only an hour, after which portal was started again and continued to work, this time in version 3.0. This fact demonstrates the strength of dark web and stability of portals on it (Knibbs, 2014).

Until 2012, the Silk Road owned a sister site - The Armory, which specializes in trade of firearms, blunt and sharp object for injuring and killing. The same site went off due to poor attendance after a period of time. Sales of weapons and ammunition is carried out in a similar manner across other sites, some of which guarantee the delivery around the globe, under the motto *"We deliver globally, because all people have the right to protection themselves"* (Lukovic, 2014). Everithing can be found, from pistols to C4 explosives. Delivery is made in special packages so that they can pass x-ray inspection, or often packed in toys, various other instruments and electrical appliances (N1, 2015).

There are a number of examples where children were used for geining money. During 2011, Europol, in coordination with thirteen different countries, arrested 184

people suspected of child abuse and the spread of children pornography in form of images (Europol, 2014). A similar campaign was carried out in the UK. In this action 650 people accused of different forms of child abuse, from possession of child pornography images to pandering were arested (BBC, 2014). In 2015, on the territory of Northern Ireland 37 people were arrested based on charges of pedophilia and distribution of child pornography using Tor (BBC, 2015).

There are examples showing that dark web is the perfect place for Cyber Crime. Users here can buy a variety of malware. At the same time, visitors of websites can become victims of various types of malware, distributed using phishing. One of such malware is vawtrak - banking Trojan distributed via e-mail (Sancho, 2015). Another large group of malware that can be found on the dark web are the CryptoLocker malwares. These malware, after accessing victim files, perform the encryption. After encrypting files, the victim is being redirected to a page where it is asked to make the payment if they want to regain control of their data. Very often the request for payment and information necessary to complete the transactions are written in the native language of the victim. The role of Tor in these transactions is hosting sites for payment in order to execute transactions using bitcoins (Ciancaglini, Balduzzi, McArdle, & Rosler, 2015). In addition to malware, interested parties can use dark web to hire hackers to carry out various types of hacker attacks on their behalf. Depending on the complexity and risk of the task, rates range from a few dozen to several thousand dollars. They offer a variety of services, from correcting assessment in schools through the theft of access codes for different functions and sensitive autorithative data. The Chinese group Hidden Lynx claims to have up to hundreds of professional cyber thieves, who broke into the computer systems of Google, Adobe and Lockheed Martin.

For people with more sinister intentions and serious willingness to go down in the dark world of the dark web, there are also services of professional assassins. One of the examples described in (Lukovic, 2014) describes a person with moral and highly flexible business principles, supposedly verified mercenary "with eight-year experience" which offers services which are exclusively paid forward in Bitcoin's. During the contact with such persons, onlyexchanging information on the victim is allowed. The requirement is that all communications, as well as any contact by email must be encrypted. If any part of the communication is not encrypted, it will be deleted.

Another portal that offers such services is known as Lovecraft. The ad states that the members of the organization are former soldiers and mercenaries of Foreign Legion. Moto of this organization is *"The best place to store your problem is grave."* This portal pays great attention to the protection and privacy of customer communications. Name, home and work address, as many photos and information about who the victim lives, license plate, description and picture of the vehicle used are informations needed about the target. Depending on the agreement, a team of killers states to prepare for a job, travel, locating and tracking targets require about two months, and the cost of purchasing airline tickets, weapons and accommodation, are not included the initial price. One portal called C'thulu offers different ways of murdering, from regular through torture and rape, to the bombing. Prices of services range from $ 3,000 to $ 180,000 depending on the chosen category and social status of the victim. Price, of course, differ on whether that person to be killed belonged to the masses, or is a public figure, a politician, a member of law enforcement, etc.

In the dark web, counterfeit money can be bought. In addition to the money, a guarantee is almost always given, as well as the description of the creation process showing that, as the sellers say, the counterfeit money is created in the same way as real money. All currencies that are worth falsified are available, but the quality and quantity vary. In these types of transactions, it is common for 600 US dollars to obtain 2,500 counterfeit, a 500 euro 2,000 counterfeit. All transactions are carried out with the promise that they can undergo standard checks, including that of ultraviolet light (Vijesti, 2015). In many cases, of course, pay for the counterfeit money uses Bitcoin.

Stolen information about the different accounts, credit card numbers, numbers of bank accounts, online auctions can also be purchased. Atlantic Carding is a location in a dark web where you can buy information about other people's credit cards, addresses and related personal information. Prices range between 5 and 80 dollars. The quality of information depends on the price. On the other hand, accounts sale is done in one of two ways. The first method involves the purchase of a single account, provided detailed information on the amount of funds on it. Another way involves the purchase of large quantities of accounts, of which a certain number probably valid. The first method is far more cost-effective, because the customer has insight into the amount of funds in the account, providing better guarantee that the funds invested will be recovered, and the extra money earned. In addition, there is the possibility of buying physical debit and credit cards of different banks (Ciancaglini, et al., 2015).

There are several sites on the dark web claiming to selling passports and identity documents. Price of these services depends on the country in which the documents are produced, as well as from the seller. The validity of these documents is difficult to verify, especially when it comes to citizenship. These services can also be created for fraud for immigrants who want citizenship of the country in which they are located at all costs. For example, price for passports, driving licenses and identity cards for Australia is 800 euros at portal called Fake ID. At the same portal, the most expensive document are for USA and the cheapest for Malaysia (Ciancaglini, et al., 2015).

In addition to the above, the more bizarre things can be found on the dark web, such as trafficking in human organs. According to the some websites, the kidney can be purchased for $ 200,000, heart for 120,000, liver for 150,000, a pair of eyes to 1,500 US dollars. In addition, various beauty products from human flesh and skin can be purchased (N1, 2015; Falconer, 2012). Also, it is possible to find a vide variety of topics that meet the various fetishes. Some of these contents are horrific footage of last conversation and words of passengers in a crashing plane, a prisoners on the day of execution (for example, the electric chair in prison in Texas) or pornographic materials in which women gauze small animals with heels. Different offers in which people offer themselves as food or other types of cannibalism also can be found. In the dark web there is well known portal reffered as Red Room, the place where the torture and killing of people are shown via live stream (Mitrovic, 2016).

Terrorists also share ideologies on the Web that provide religious commentaries to legitimize their actions. Based on a study of 172 members participating in the global Salafi Jihad, it is concluded that the Internet has created a concrete bond between individuals and a virtual religious community (Sageman, 2004). Web appeals to isolated individuals by easing loneliness through connections to people sharing some commonality. Such virtual community offers a number of advantages to terrorists. It no longer ties to any nation,

fostering a priority of fighting against the far enemy (e.g., the United States) rather than the near enemy. Internet chat rooms tend to encourage extreme, abstract, but simplistic solutions, thus attracting most potential Jihad recruits who are not Islamic scholars. The anonymity of Internet cafes also protects the identity of terrorists. However, Internet can not be in a direct contact with Jihad, because devotion to Jihad must be fostered by an intense period of face-to-face interaction (Chen, Chung, Qin, Reid, Sageman, & Weimann, 2008). In addition, existing studies about terrorists' use of the Web mostly use a manual approach to analyze voluminous data. Such an approach does not scale up to rapid growth of the Web and frequent change of terrorists'identities on the Web.

One of terrorist web sites Alneda.com identified by the U.S. Government called itself the *"Center for Islamic Studies and Research,"* and provided information for Al Qaeda (Thomas, 2003). To group members, terrorists use the Web to share motivational stories and descriptions of operations. To mass media and non-members, they provide analysis and commentaries of recent events on their Web sites. For example, Azzam. com urged Muslims to travel to Pakistan and Afghanistan to fight the *"Jewish-backed American Crusaders"*. Another web site Qassam.net appealed for donations to purchase AK-47 rifles.

Web portals on the Dark Web are protected in various ways. One of the main ways is to check the behavior of visitors who do not follow the standard pattern. If administrators recognize suspect behaviour of visitors they launch a basic check. Surveillance can be identified if a visitor can see only active row in the text, but no previous rows (Fu, Abbasi, & Chen, 2010). The next step is to put the so-called key logger program on visitors computer, so as to record everything a visitor keystroke. In this way, maximum control over all visitor activities is achieved until administrators check who the visitors are and what their intentions are.

Conclusion

It is widely recognized that the Internet is the place where you can find information about everything and everyone. Whoever used a service on the Internet once, entered their data or created the account, is permanently remembered in one of the databases. In addition to the information generated using a large number of services, large-scale trade of different types of goods, even between countries at opposite ends of the world is performed daily. When taken into account that the visible part of the Internet represents 4% of all that is on it, large volume of contacts, information and trades might seem trivial in comparison to what is in the deep web. This fact chalenges everyday users to access services that are beyond the boundaries of the visible. The fact that the dark web is not indexed, is used for profit by the different traders of illegal goods. In addition to the profit purposes, it is often used by various terrorist organizations, so as to spread the ideology and communication, as well as to perform arms and human trafficking. Besides terrorist organizations large number of individuals use dark web for different types of trafficking and illegal activities. Some examples of use described in the work undoubtedly lead to the conclusion that in this part of the Internet there is much that is still unexplored and hidden from the general public.

References

Abbasi, A., & Chen, H. (2005). Identification and comparison of extremist-group web forum messages using authorship analysis. IEEE Intelligent Systems, 20(5), 67-75.

Amika. (2016). Deep web – hidden underworld of the Internet, b92 Blog. Retrieved October 20, 2016, from http://blog.b92.net/text/26912/DEEP-WEB-%E2%80%93-skriveno-podzemlje-Interneta/

Arslani, M. (2015). Dark internet: Underworld, which offers everything from guns to organs. Express. Retrieved November 11,2016, from http://www.express.hr/tehno/mracni-internet-kriminalno-podzemlje-koje-nudi-sve-od-oruzja-do-organa-635

BBC. (2014). Child abuse image investigation leads to 660 arrests. BBC News. Retrieved September 19, 2016, from www.bbc.com/news/uk- 28326128.

BBC. (2015). 50 arrests in NI online abuse images probe in past year, say police. BBC News. Retrieved October 20, 2016, from www.bbc.com/news/uk-northern-ireland-31896685

CARNet. (2007). Tor - a network of anonymity. CarNet-Croatian Academy and Research Network. 1-15.

Cekerevac, Z., Dvorak, Z., & Cekerevac, P. (2016). Is the "dark web" deep and dark? FBIM Transactions, 1-12.

Chen, H., Chung, W., Qin, J., Reid, E., Sageman, M., & Weimann, G. (2008). Uncovering the dark Web: A case study of Jihad on the Web. Journal of the American Society for Information Science and Technology, 59(8), 1347-1359.

Ciancaglini, V., Balduzzi, M., McArdle, R., & Rosler, M. (2015). Below the Surface: Exploring the Deep Web. Trend Micro. pp. 1-48.

Cook, J. (2014). FBI Arrests Former SpaceX Employee, Alleging He Ran The 'Deep Web' Drug Marketplace Silk Road 2.0, Business Insider. Retrieved October 15, 2016, from www.businessinsider.com/fbi-silk-road-seizedarrests-2014-11

Europol. (2014). Operation Rescue. Europol. Retrieved September 19, 2016, from www.europol.europa.eu/content/operation-rescue.

Falconer, J. (2012). Mail-order drugs, hitmen & child porn: A journey into the dark corners of the deep web. Insider. Retrieved October 30, 2016, from http://thenextweb.com/insider/2012/10/08/mail-order-drugs-hitmen-child-porn-a-journey-into-the-dark-corners-of-the-deep-web/

Fu, T., Abbasi, A., & Chen, H. (2010). A focused crawler for Dark Web forums. Journal of the American Society for Information Science and Technology, 61(6), 1213-1231.

Goodman, M. (2015). Most of the web is invisible to Google. Kere's what it contains. Popular Science, Retrieved November, 18, 2016, from http://www.popsci.com/dark-web-revealed.

Knibbs, K. (2014). Silk Road 3 Is Already Up, But It's Not the Future of Darknet Drugs. Gizmodo. Retrieved October 15, 2016, from http://gizmodo.com/silk-road-3-is-already-up-butits-not-the-future-of-da-1655512490

Lukovic, M. (2014). Deep internet - Drugs, murders, pornography - what is hidden in the black hole web?", Before After. Retrieved September 18, 2016, from http://www.beforeafter.rs/tehnologija/deep-internet/

Mergen, L. (2015). On anonymous networking in Haskell: announcing Tor and I2P for Haskell. Luctor et Emergen. Retrieved October, 3, 2016, from: http://www.leonmergen.com/haskell/privacy/2015/05/30/on-anonymous-networking-in-haskellannouncing-tor-and-i2p-for-haskell.html

Mitrovic, M. (2016). Dark secrets of global network. New Energy (Nova Energija), Retrieved November 01, 2016, from http://www.novaenergija.net/mracne-tajne-globalne-mreze

N1. (2015). Darknet - the dark side of internet surfing. N1 SCI-TECH portal Zagreb. Retrieved September 18, 2016, from http://rs.n1info.com/a50647/Sci-Tech/Sve-o-Deep-Web-ili-Darknetu.html

PC. (2015). Definition of: surface Web. PC Magazine Encyclopedia. Retrieved November 20, 2016, from http://www.pcmag.com/encyclopedia/ term/52273/surface-web.

Sageman, M. (2004). Understanding terror networks. Philadelphia, PA: University of Pennsylvania Press.

Sancho, D. (2015). Steganography and Malware: Why and How. TrendLabs Security Intelligence Blog. Retrieved October 30, 2016, from http://blog.trendmicro.com/trendlabs-security-intelligence/steganography-and-malware-why-and-how/

Spalevic, Z., Ilic, M., & Palevic, M. (2016). Electronic Tracking Of Postal Services. *In Proceedings of 3rd the International Scientific Conference on ICT and e-Business Related Research – Sinteza (pp. 479-485)*, Belgrade: University Singidunum. doi: 10.15308/Sinteza-2016-479-485.

Thomas, T.L. (2003). Al Qaeda and the Internet: The danger of cyberplanning. Parameters, 33(1), 112–123.

Todorovic, A. (2015). What is deep and dark web, you need to take care and how to protect myself? Kompijuteraš. Retrieved November, 18, 2016, from https://kompjuteras.com/sta-je-deep-dark-web-trebam-li-se-brinuti-kako-da-se-zastitim/.

Tsfati, Y., & Weimann, G. (2002). www. terrorism. com: Terror on the Internet. Studies in Conflict and Terrorism, 25(5), 317-332.

Vijesti. (2015). Dark internet: There are hackers, sellers of human organs, and weapons, Vijesti online. Retrieved October 30, 2016, from http://www.vijesti.me/techno/tamni-internet-tu-su-hakeri-prodavci-ljudskih-organa-oruzja-828308

Zetter, K. (2013). How the Feds Took Down the Silk Road Drug Wonderland. Wired. Retrieved October 20, 2016, from: www.wired.com/2013/11/silk-road/