UDC 004.738.5.056(07)

DARKNET – ONE OF THE SIDES OF THE INTERNET

YULIYA SHVETS, ELENA SETKO
Yanka Kypala State University of Grodno, Belarus

This article is about resources, which can open access to illegal systems of the World Internet space and information protection methods which provide anonymity of the systems work.

The Internet is a global network, which can give us access to all digital resources. We use it with different aims every day. Every user can get any information, if he knows where he should search for it. On the one hand, implementation of IT-technologies in different areas made person's life more comfortable, but on the other hand, due to this process, a number of crimes have been increased in this area.

As a result , teaching of informatics or modern computer technologies , it is necessary to form culture and skills of correct activity in networks and cloud spaces , using internet resources and network services in the process of education and further professional activity, also experience of making own content on the base of different services.

The aim of the article is the necessity to inform people, which study work on the Internet, about existence of "Depth Internet" and principles of its functioning, effective and legal work on the Internet.

Darknet is a small part of Deep Web [1], which means a diversified content, which is unavailable for most part of search engines. All resources are hidden from accessible search systems in Darknet. Information is defended with special computer software, which provides encryption and anonymity of users.

Anonymous network, where there are own laws and regulations. Place, where you can buy and find everything, regardless of some moral standards. It is a network with a huge choice of related sites. You can find any information. But due to absolute freedom and lack of laws, illegal business is very developed.

Well, "Darknet" is a number of private networks, which use only trusted connection(full anonymity).No one can track a man in this networks and due to this illegal business has become widespread. None of search engines or web browsers gives you access to these resources, none except Tor [2]. Tor or The Onion Router is a free software for enabling anonymous communication. Tor was made in a secret lab of the naval forces of the United States, this system was a secret project, but later the source code was opened.

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

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

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

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

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

Other than the database that stores the hidden-service descriptors, Tor is decentralized by design; there is no direct readable list of all hidden services, although a number of hidden services catalog publicly known onion addresses.

Because hidden services do not use exit nodes, connection to a hidden service is encrypted end-to-end and not subject to eavesdropping. There are, however, security issues involving Tor hidden services. For example, services that are reachable through Tor hidden services and the public Internet are susceptible to correlation attacks and thus not perfectly hidden. Other pitfalls include misconfigured services (e.g. identifying information included by default in web server error responses), uptime and downtime statistics, intersection attacks, and user error. Hidden services could be also accessed from a standard web browser without client-side connection to the Tor network, using services like Tor2web.

Ensuring the anonymity of users an illegal business has been widely adopted. It is possible to find everything in Darknet: from hard drugs and weapon to the materials of pornographic content involving minors. However it also contains a great number of libraries full of rare literature that is not available in the public domain, it allows to exchange information between witnesses of various incidents, informants, intelligence agents (for safety) and many other things[3]. Various special services use these resources.

Buyers and sellers carry out all money transactions through the use of cryptcurrency bitcoin, which in combination with Tor can ensure anonymity of the parties to the transaction and the inability to lock payment. Bitcoin is a cryptocurrency and a payment system, invented by an unidentified programmer, or group of programmers, under the name of Satoshi Nakamoto. The system is peer-to-peer and transactions take place between users directly, without an intermediary. These transactions are verified by network nodes and recorded in a public distributed ledger called the blockchain,which uses bitcoin as its unit of account(The blockchain is a public ledger that records bitcoin transactions.). Bitcoin is a decentralized virtual currency[4].

Bitcoin is pseudonymous, meaning that funds are not tied to real-world entities but rather bitcoin addresses. Owners of bitcoin addresses are not explicitly identified, but all transactions on the blockchain are public. In addition, transactions can be linked to individuals and companies through "idioms of use" (e.g., transactions that spend coins from multiple inputs indicate that the inputs may have a common owner) and corroborating public transaction data with known information on owners of certain addresses. Additionally, bitcoin exchanges, where bitcoins are traded for traditional currencies, may be required by law to collect personal information.

To heighten financial privacy, a new bitcoin address can be generated for each transaction. For example, hierarchical deterministic wallets generate pseudorandom "rolling addresses" for every transaction from a single seed, while only requiring a single passphrase to be remembered to recover all corresponding private keys. The legal status of bitcoin varies substantially from country to country and is still undefined or changing in many of them. While some countries have explicitly allowed its use and trade, others have banned or restricted it. Likewise, various government agencies, departments, and courts have classified bitcoins differently. Regulations and bans that apply to bitcoin probably extend to similar cryptocurrency systems.

Bitcoin is not recognized as official currency (mostly it is used for buying illegal things).

Despite the fact that Tor has a high level of protection there are quite a lot of security problems that enable to trace a user and transmitted data. Tor is aimed at hiding the link between a client and a server. However it cannot essentially provide transmitted data to be fully hidden as enciphering in this case is only a means of achieving anonymity on the Internet. Therefore additional protection of communication is necessary for maintaining a higher level of confidentiality. Enciphering of the files transferred through Tor by means of their packing in cryptographic containers and the methods of a steganography is also important. The modern student of IT specialties studying a course on information security has to know all this.

REFERENCES

1. Darknet [Electronic resource]. – Mode of access: https://ru.wikinews.org/wiki/Darknet. – Date of access: 28.01.2017.
2. The system of proxy servers [Electronic resource]. – Mode of access: https://ru.wikinews.org/wiki/ Tor. – Date of access: 28.01.2017.
3. What are bought in Darknet. – Mode of access: http://www.zdnet.com/article/seven-things-you-did-not-know-about-the-deep-web. – Date of access: 28.01.2017.
4. Bitcoin [Electronic resource]. – Mode of access: https://en.wikipedia.org/wiki/Bitcoin. – Date of access: 28.01.2017.