Conference Paper

Money Laundering and Terrorist Financing through the Onion Routing (on the Example of TOR Browser)

Laishevskii S. D., Politova A. V., and Zasypkina A. E.

National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Kashirskoe shosse 31, Moscow, 115409, Russia

Abstract

This article is devoted to the use of onion routing for AML/CFT and the question of its regulation through various legal acts. The browser TOR is examined as the best implementation of this type of routing. The article describes precedents of TOR misuse.

Keywords: money laundering, onion routing, TOR browser

Corresponding Author:
Laishevskii S. D.
lai-stas@yandex.ru

Received: 11 December 2017
Accepted: 20 January 2018
Published: 13 February 2018

Publishing services provided by Knowledge E

Selection and Peer-review under the responsibility of the FinTech and RegTech: Possibilities, Threats and Risks of Financial Technologies Conference Committee.

1. Introduction

In our time, information technology is making huge strides, innovative software and new advanced systems appear almost every day. Each of the new inventions can be applied not only for legitimate purposes, but also as an instrument for committing crimes. This article discusses obtaining anonymity for money laundering and terrorist financing through TOR proxy server system.The sphere of combating money laundering and the financing of terrorism is regulated by legislation at the international level (through 40 FATF Recommendations) and at the level of the Russian Federation (through 115-FZ and other legislative acts).

2. Analytical part

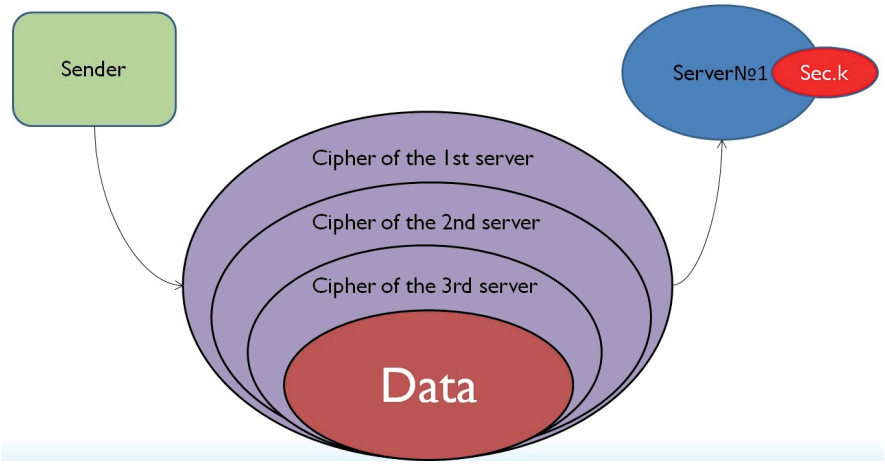
In accordance with the Federal Law № 115 on Counteracting Legalization (Laundering) of Proceeds Obtained By Criminal Means And Terrorism Financing legalization (laundering) of proceeds obtained by criminal means is giving a lawful form of possession, use or disposal of funds or other property obtained as a result of the commission of a crime.

Each criminal pursuing the goal of disposing of the funds received after committing a predicate offense seeks to give them a legal appearance and transfer them from the shadow economy to the legal one.

Onion routing is based on the technology of anonymous exchange through a computer network. Any information which can help to identify contents, header, sender or recipient of messages should not be transmitted openly. Instead of sending messages directly to the recipient computer a connection is established through a sequence of computers. These computers called onion routers are defined once while creating a connection and cannot be changed until this connection is interrupted. The onion is a data structure that is encrypted several times. Anonymous connection established through onion routing is robust to traffic analysis. The dominant technology that uses onion routing is a TOR network. We will take a closer look at the anonymous exchange technologies and take TOR as an example.

The TOR network is the group of volunteer servers that allow people to maintain their privacy and security on the Internet. TOR users utilize this network by connecting through several virtual tunnels to the resources they are interested in. This connection is not direct and allows both organizations and individuals to exchange information through public networks without threatening their privacy. Also TOR is one of the tools for circumventing censorship and allows users to reach blocked content. TOR performs some social functions: chats and web forums for victims of violence and harassment, as well as people with diseases. TOR can be useful to journalists for safer communication with informants and dissidents. Law enforcement authorities use this anonymous network to visit or monitor websites without leaving government IP addresses in the web logs.

TOR protects users from a common form of Internet surveillance known as traffic analysis. Traffic analysis can be used to determine who communicates with whom in the public network. Knowing the source and Internet traffic content allows the third parties to monitor user behavior and interests. Traffic analysis works as follows: data packets have two parts: payload and header used for routing. Even if the useful information related to the message is encrypted, the traffic analysis still will show a lot about your online activities. This happens due to the fact that the focus is on the header which contains the source, purpose, size and time of the packet transmission. The main problem is that the message recipient can see who sent it by looking at the headers. A very simple form of traffic analysis can track the sender and receiver location on the network by looking at the headers. There are more powerful types of traffic analysis. Some attackers monitor several parts of the Internet network and



Picture 1

use complex statistical methods to track communication patterns of many different organizations and individuals. Encryption does not help in fighting with these attackers as it hides only the content of Internet traffic, not the headers.

All file sharing in the TOR system occurs through the network of proxy servers scattered around the world. Unlike other networks the data packet is sent through 3 randomly selected nodes creating a virtual tunnel.

Before transferring of the data the sender forms a packet. He randomly selects 3 proxy servers and requests their public keys, then performs multi-layer data encryption. Each stage has the instructions written for each server to send the packet to the next server. The so-called "onion" is formed.

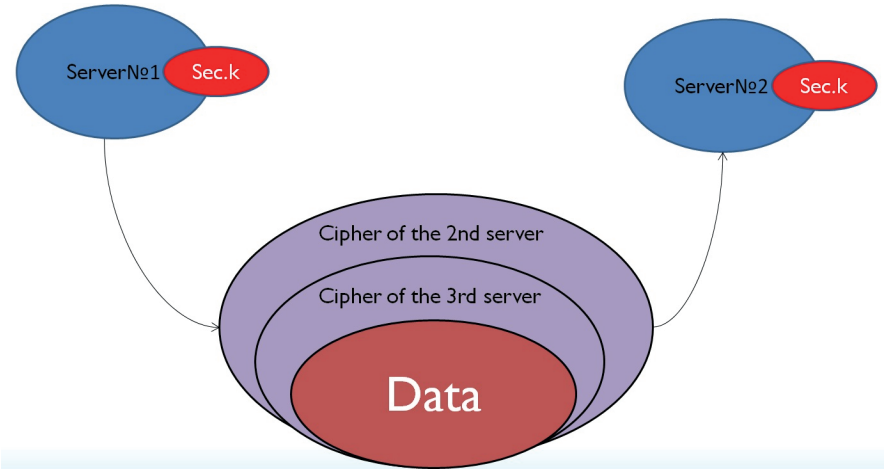
The system uses asymmetric cryptographic algorithm RSA. It is effective and has been implemented in many means of communication. For an attacker the complexity of cracking an RSA cryptosystem using a 1024-bit encryption key is equivalent to the complexity of factoring a 309-digit integer.

When the packet is generated, the sender sends it to the first node (Pic.1).

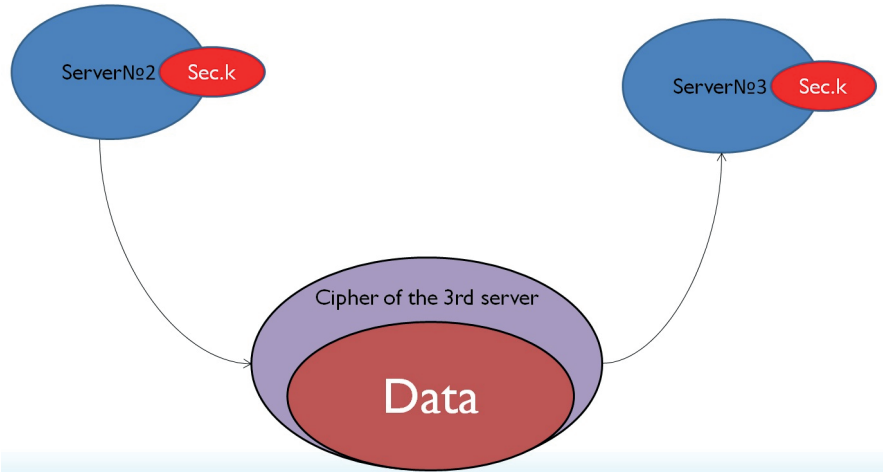
The server decrypts the first layer using its secret key and finds out where further to send the packet. Then the server 1 forwards the packet to the server 2 (pic.2).

The server 2 redirects the bulb to server 3 performing the same actions. Thus, at each stage the server does not have access to data and information about the entire chain. The proxy server knows only where the packet came from and finds out where to send it removing the next layer (Pic.3).

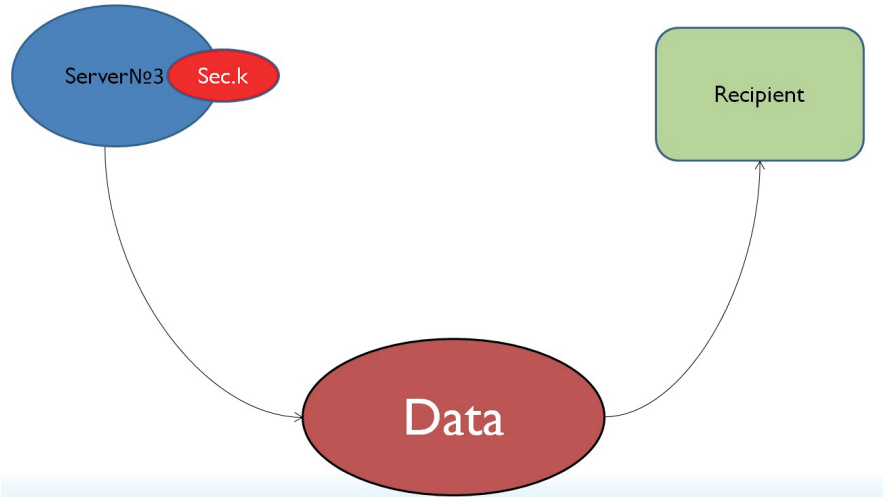
At the end of the chain the 3rd node transmits data to the recipient while the nformation about the sender remains confidential (Pic.4).



Picture 2



Picture 3



Picture 4

None of the servers has full information to restore the chain from the recipient to the sender. Thus, algorithmically TOR is absolutely anonymous.

It is possible to commit predicate crimes, such as buying drugs and weapons, smuggling, etc by using the technology of anonymous TOR exchange. It also simplifies the withdrawal of illegal proceeds through the purchase of goods which turnover is not limited by the legislation.

Examples of the technologies using TOR browser to conceal the committing of crimes are the creation and operation of Silk Road site and its Russian counterpart Ramp (Russian Anonymous Marketplace). Both sites were an anonymous trading Internet sites located in the.onion zone of the anonymous TOR network. The.onion zone is designed to provide access to anonymous or pseudo-anonymous TOR addresses. Such addresses are not usual DNS records (DNS is a system for obtaining information about domains), and information about them is not stored in the root servers of this system, but additional required software to access the TOR network is installed, programs that work with the Internet gain access to sites in the.onion domain zone by sending a request through the TOR server network. Both sites are currently closed.

The TOR network can also be an instrument of terrorist financing. It is virtually impossible to track transactions for the development, support and propaganda of terrorist organizations and individual terrorists and the financing of terrorist acts in case of joint use of the capabilities of this network and the crypto currency. For instance, some virtual currencies, such as bitcoin store all transactions in a public book called the Blockchain. Blockchain registers transactions, not user IDs. You can associate IP addresses with the protocols of bitcoins. However, TOR helps to hide the user IP address in this case providing complete anonymity of all transactions occurred. It should be noted that any TOR user can buy bitcoins for the euro, US dollars and other currencies. This situation is a huge danger in the AML / CFT sphere. For example, a criminal may agree to send bitcoins to a digital address that does not contain real contact information. Then a person can use the exchange to convert bitcoins into another currency deposited on an offshore account.

At the moment there is no optimal and inexpensive way to combat money laundering. In general case, an attacker could expose the sender by controlling all three proxy servers through which the packet passes, but in reality it is almost impossible. TOR has more than 7000 network nodes scattered across all continents of the Earth. Assume that an attacker has the resources of several advanced countries and has access to half of the servers. Nevertheless, the probability that the package will pass through 3 controlled nodes is equal to 12.5%.

$$P(A) = \frac{C_{3500}^3}{C_{7000}^3} = \frac{3500}{7000} * \frac{3499}{6999} * \frac{3498}{6998} = 0,125,$$

where $C_n^k = \frac{n!}{k!(n-k)!}$

To ensure a probability of 51%, the control over 5,600 nodes is needed. Since not every attacker is comparable to the whole country, the degree of privacy protection is very high, and the task of exposing the sender is almost impossible.

Until recently it was believed that there is a loophole through which we can identify the IP address of the computer where from they had been sent information due to vulnerabilities in the browser. When the user gets on a specially crafted web page, the operating system could circumvent the TOR browser, directly addressing the remote host. The vulnerability has received the name of TORMoil and has been confirmed for Mac and Linux. However, in the new version of TOR Browser 7.0.9 this problem has been fixed since it was revealed that it was related to a bug in the Firefox browser on which TOR is based. Let's assume that in the current situation only the adjustment of legislation in the sphere of TOR use browser can reduce the number of crimes.

Since November 1, 2017, a law comes into force in Russia that prohibits VPN services and anonymizers (including TOR browser) to allow Russian users to access sites listed in the "black list" of Roskomnadzor. Such services should cooperate with the department receiving a list of sites banned in Russia.

FSS and MIA will monitor the work of VPN-services, and Roskomnadzor will warn them about the need to ban sites from the "black list". If the service does not comply with the request in 30 days after the warning, Roskomnadzor will be able to block it in Russia.

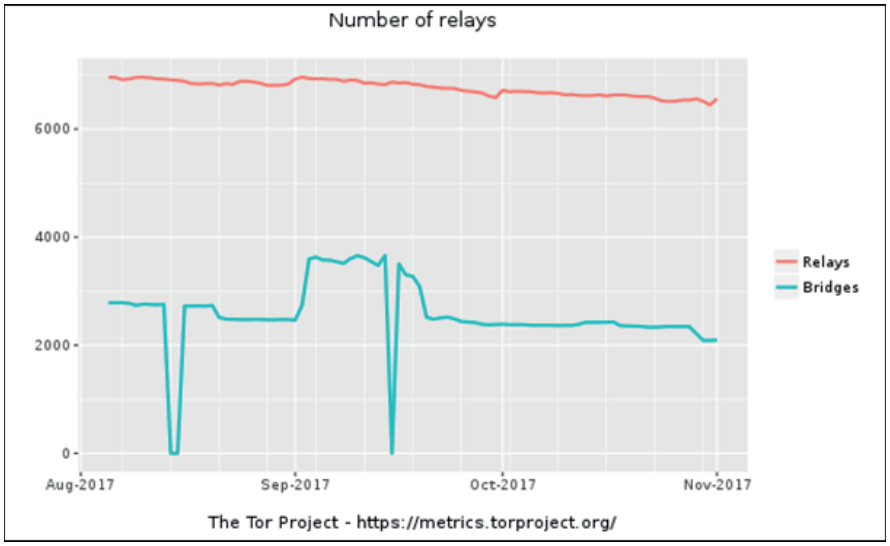
In addition, search engines will have to connect to the "black lists" at the request of Roskomnadzor. They will be required to exclude inquiries of banned sites in Russia.

Due to the law described above circumvention of site blocks will be complicated, but it will not be impossible. TOR provides protection against blockages with the help of so-called "bridges". Bridge relays (abbreviated "bridges") are transponders that are not listed in the main TOR directory. The main principle is the lack of the ability of the Internet provider to block all known bridges due to the inaccessibility of their full public list (there is a closed list of servers, and TOR can issue them at the user request).

3. Conclusion

Thus, money laundering using the capabilities of the TOR browser, even with the adoption of significant limitations in its use, however, might be a complex and an urgent issue.

In this article we examined the basic principles of the TOR browser and its characteristics. We also described the ways in which it can be used to commit crimes, in particular money laundering and the terrorist financing, and the importance of this issue. The following graph shows that the TOR project does not lose relevance and there are already almost 7,000 volunteers around the world who create nodes.



The TOR which is the best implementation of onion routing has great prospects. Science develops rapidly, new technologies appear intensively. But how can we prevent the criminals or terrorists to abuse new inventions and use them to commit crimes? Relatively effective way is to strengthen legislation in each of the areas. But because of computer technologies development speed the possibility to consider each aspect is missing. Therefore, a special role is played by the training of new specialists in areas such as fighting against fraud, crimes in the IT sector, money laundering and the financing of terrorism.

Acknowledgements

This work was supported by Competitiveness Growth Program of the Federal Autonomous Educational Institution of Higher Education National Research Nuclear University MEPhI (Moscow Engineering Physics Institute).

References

[1] *Michael G. Reed, Paul F. Syverson, David M. Goldschlag.* Anonymous Connections and Onion Routing

[2] *Paul Buder, Daniel Heyne, and Martin Peter Stenzel.* Performance of TOR

[3] Federal Law, dated 29.07.2017 N 276-FZ "On implementation of changes into the Federal Law "About information, information technologies and information sicurity"

[4] Roscomnadzor: Opera and others are testing locks of block bypasses through VPN-services [site]. URL: https://vc.ru/28254-roskomnadzor-opera-i-drugie-testiruyut-zapret-obhoda-blokirovok-cherez-vpn-servisy (10.11.2017)

[5] TOR: Power Digital Resistance [сайт]. URL: https://www.TORproject.org (1.11.2016)

[6] Access zone: the law on anonymizers has come into force in Russia [site]. URL: https://russian.rt.com/russia/article/445118-vpn-TOR-obhod-blokirovok (5.11.2017)