**International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)**
*Volume 7, Issue 2, 2020, PP 1-8*
*ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online)*
*DOI: http://dx.doi.org/10.20431/2349-4859.0702001*
*www.arcjournals.org*

# How Really Secure is TOR and the Privacy it Offers?

**Christos P. Beretas***

*PhD Candidate (full scholarship) in Cyber Security at Innovative Knowledge Institute, Paris, France*

***Corresponding Author:** **Christos P. Beretas,** PhD Candidate (full scholarship) in Cyber Security at Innovative Knowledge Institute, Paris, France*

**Keywords:** *Tor, Onion Servers, Security, Privacy, Attack, Vulnerabilities, Networks*

**TOR** is a very popular Project, a global anonymity network loved by millions of internet users, used by people who want to express their opinion online, take malicious actions, transfer files from one location to another without these files are compromised, their location is not detected, etc. All the above actions are performed so as not to be detected by ISPs or to log their online data from the websites they want to visit, thus significantly reducing the risk to be detected, although the ISP knows when a user is connecting to the TOR network but without being able to see the contents of the packets. TOR started for another purpose and ended up being used for another purpose. Designed by the U.S Navy for the exchange of confidential data and ended up an open source project, this in itself is questionable and needs a lot of skepticism, how an anonymity project that was designed to be used for the secrecy of communications was left free to users making life difficult for the secret services worldwide to detect dangerous online transactions and prevent malicious actions, isn't that true after all? Did the government create an anonymity project to make its life more difficult? is this whole endeavor a delusion? Is this whole project deliberately in the interest of governments?

Most internet anonymity users prefer TOR over a **VPN**, thinking that the VPN service provider could keep log files that could easily be passed on to governments or other stakeholders, depending on international agreements. as well as by the country of operation of the VPN service provider and the privacy and confidential communications policies it implements in accordance with its legislation. According to research i have done, below I point out some points which are a **red flag** for the integrity of the data circulating in the TOR network and which in some of the following ways individually or as a whole could be intercepted.

- *Fake Relays (Middle or Exit Nodes).*
- *Malicious Code injected in target web sites.*
- *Back doors in encryption algorithms.*
- *Malicious software installed in target computer systems.*
- *Fake HTTPS.*

Let's analyze the above **5** points one by one:

## 1. Fake Relays (Middle or Exit Nodes)

To understand this section there must be a substantive knowledge of the operation of the TOR. A user of the TOR network every time he/she browse the internet goes through different Relays as this means when the data reaches the TOR exit Node its IP address changes as it appears to be browsing the internet from a different location. Here comes on mind the following question, most IP detection and IP analysis systems are able to know if an IP address is a not a TOR IP address (regular IP address) or TOR exit Node. I think you know why. I return to my above analysis, think for a moment about the project **5 eyes, 9 eyes, 14 eyes** and the participating countries, then ponder if **fake middle relays** or **exit TOR nodes** are installed in these countries, how easily could the packages be intercepted? the packages could have been copied without the user realizing the slightest thing, while continuing the communication of the user uninterruptedly so the user would not perceive the slightest thing.

## 2. Malicious Code Injected in Target Web Sites

Intelligence services can easily create fake web pages that are tailored to the target user's interest, which direct the target user to other methods to visit them, or these web pages are hosted on **Onion Servers** that will pique the target user's interest. The target user will then visit the fake website for lack of special monitoring software or with other words **Back door** which is able to monitor the activities of the target user.

## 3. Back Doors in Encryption Algorithms

Do governments and intelligence services possess **master keys** that can decrypt any content that has been encrypted by any encryption method? is a question that needs deeper research, but I find it unlikely that governments will not have a back door to recognized encryption algorithms and encryption methods. I do not believe that a government should allow the creation of an encryption algorithm or a method of data encryption without the existence of a security backdoor.

## 4. Malicious Software Installed in Target Computer Systems

This method works either by physically accessing a computer system or by accessing the system remotely after locating a security hole that allows remote control and installation of monitoring software such as a **custom keylogger**. This method does not require the interception of data from the TOR network as the data is stolen before entering it.

## 5. Fake HTTPS

The philosophy is often stated that if the user visits a website that uses encryption (**https**) then it is impossible to locate the real visitor behind TOR, while if a website is visited that does not support encryption method (**http**) it is possible to reveal the real visitor behind TOR. **The above reasoning applies only to the theory**, the reasons I mention this are that **1)** there are many fake websites that use fake https, **2)** SSL can be violated and while it seems that a website shows a secure and provide valid connection something that applies, then the transferred data is copied without the user realizing the slightest thing. The average user may not realize the difference, intelligence services that have ways to spy on data from websites that use SSL know the difference.

In conclusion, we can say that the TOR network is a secure anonymous web browsing network that offers a degree of anonymity to users who use it, but anonymity that is visible to ordinary users and not to governments and intelligence services. who know the ways and have the methods to penetrate into it? The TOR network is a completely secure network in the eyes of ordinary users. In a world where **important information is expensive,** the creation and free use of an anonymity project that important people would not be able to access would never be allowed.

## References

[1] Christos Beretas. (Chronicle Journal of Engineering Science, 2020). The role of IoT in Smart Cities: Security and Privacy in Smart World.

[2] Christos Beretas. (Biomedical Journal of Scientific & Technical Research, 2020). Smart Cities and Smart Devices: The Back Door to Privacy and Data Breaches.

[3] Christos Beretas. (International Journal of Innovative Research in Electronics and Communications, 2019). Governments Failure on Global Digital Geopolitical Strategy.

[4] Christos Beretas. (Research in Medical & Engineering Sciences, 2018). Security and Privacy in Data Networks.

[5] Christos Beretas. (International Journal of Modern Communication Technologies & Research, 2018). Internet of Things, Internet Service Providers and Unsuspecting Users.