We entered the Deep Web, and this was what we saw...

The 'Deep Web', is a hidden part of the Internet, where traditional browsers such as Google SE or Bing do not reach, and until now very few have dared to explore it.

- More than 90% of the Internet remains enclosed from our traditional Internet search engines in the Deep Web - from news information, discussion forums, newspaper libraries to compilations of historical data. Google, Yahoo!, Bing, etc. they are only able to find the indexed content, which is a tiny 10% of the entire Internet.

But far below, lurks the dark web, which is notorious for heavily encrypted data, featuring adult sites and other malicious content.

Navigating the Deep Web

My curiosity of navigating the depraved Internet was undeniable. I was wondering how it all works. So I am ready to share with you, what I have found.

To begin with, in order to descend deeper, one will need a specific browser, the most popular of the browsers is TOR, to navigate anonymously, minimizing the risks that may occur. Search engines, working for TOR network: Torch, Candle, DuckDuckGo, Not Evil, etc.

- Some Darknet search engines are capable of non-indexing content: non-published, or password-protected data, search results, archived materials. The addresses of the websites, have the characteristic of having a domain usually not easy to identify, but does have the suffix .onion.
- There are some pages that contain a directory of sites. Within these addresses, there are some websites where one can get personal information.

- One can visit the portal dnstats.net, which shows information about the availability of some of the most used sites. This monitoring tool is very useful to check the quality in terms of availability of Deep Web sites. Graphically, you can see the history of the selected sites, an image of the page, comments.
- Another part of the statistics about visited domains is related to the infrastructure of control panels (C & C), which are used for the administration of financial botnets and other malicious codes such as ransomware, file sharing applications or chat clients, forums, and political debates.

Deep Web threats are not unique

I have heard about the dangers that exist in "the hidden Internet." However, without diminishing their danger, I must say that the same risks we have in the conventional Internet. Malware, exploits and various types of attacks can be found on both networks. In terms of drug trafficking, government investigations found that in many cases social networks such as YouTube were used to mask messages between posters.

Perhaps the issue is not the presence or absence of these contents, but the ease with which you can access it.

Finally, I can mention that with .onion sites it is also possible to find vulnerabilities linked to web applications, which are normally used to upload malicious codes that will be exploited in the visitor's browser, for the purpose of stealing information or even an e-wallet.

Many users navigate relatively anonymously and safely, using a liveCd or from a virtual machine with operating systems prepared for that, as is the case of Tails, which isolates the system.

Some revealing data

I have learned that day by day more curious people decide to enter the Deep web, knowing that they may be exposing themselves to different threats and malicious codes. However, little is known about the current state of Deep Web.

- According to experts, the Tor network currently consists of approximately 30,000 active ".onion" websites, which makes it much smaller than previously thought.
- Regarding the languages used in the sites, at least 32 different ones were found; leading the podium with 76%, as expected, is English, followed by German with only 4%, and finally the Chinese with 3.7%.

Malware

Of course, remember to have your antivirus, antimalware and firewall active at all times. Do not share your data, not even your email; if necessary create a dedicated email account just for this.

Under no circumstances make any payment through Tor, be it for the service or product that is, and, finally, do not download anything and if you do, pass the antivirus test before opening it, and always open it while offline (without Internet). These files can open web pages that access malware or any type of service that reveals your IP and data.

Bitcoin - digital currency

The last characteristic that we are going to develop is linked to the type of cryptocurrency, that is mostly used in this network, namely, the famous bitcoin. Transactions made with this cryptocurrency cannot be reversed, meaning that no entity can intercede in case there is a dispute.

The identity of the user who owns the address is not known, unless it is revealed during a purchase or for some other circumstance. This is one of the reasons why bitcoin addresses are usually used only once.

Conclusion

Maybe, it's time to demystify the Deep Web as the place where bad things of the Internet hide, and to understand it better. After all, depending on how it is used, anonymous browsing can be seen as a privacy tool or as another tool for cybercriminals.

The lack of control in this type of communications can be used improperly, although, in times where every day we lose some privacy, leaving traces of all kinds on the Internet, this network could be valuable. One of the reasons is linked to the fact that it allows expressing ideas of people who, for various political reasons or of another nature, must remain anonymous, such as the famous Wikileaks.

We are at a time when we have access to a large amount of information, so the way we take advantage of its use depends largely on the responsibility with which we handle it.

As you can see, Deep Web threats are real. It can expose you to harmful aspects of the internet. You have to be more and more careful, when protecting yourself while surfing the net, especially the Deep Web.