What is On the Dark Web?

By Ravi Das

What Is On The Dark Web?

Introduction

In our last whitepaper, we took a deep dive into what the Dark Web is all about. Specifically, the following topics were covered:

- The Key Differences between the Public Web, the Deep Web, and the Public Web;
- How to access the Dark Web, using the following tools:

  *The TOR Web Browser;

  *Making use of a very reliable and solid VPN package;

  *Making use of the Duck Duck Go search engine (this is only exclusive through the Dark Web).

- Understanding how the entire process of accessing the Dark Web actually works;
- The various challenges that Law Enforcement agencies, especially those of Digital Forensics teams face, when they attempt to gather and collect latent evidence.

In this whitepaper, we continue with the theme of the Dark Web. In this particular piece we examine in more detail what is available in the Dark Web.

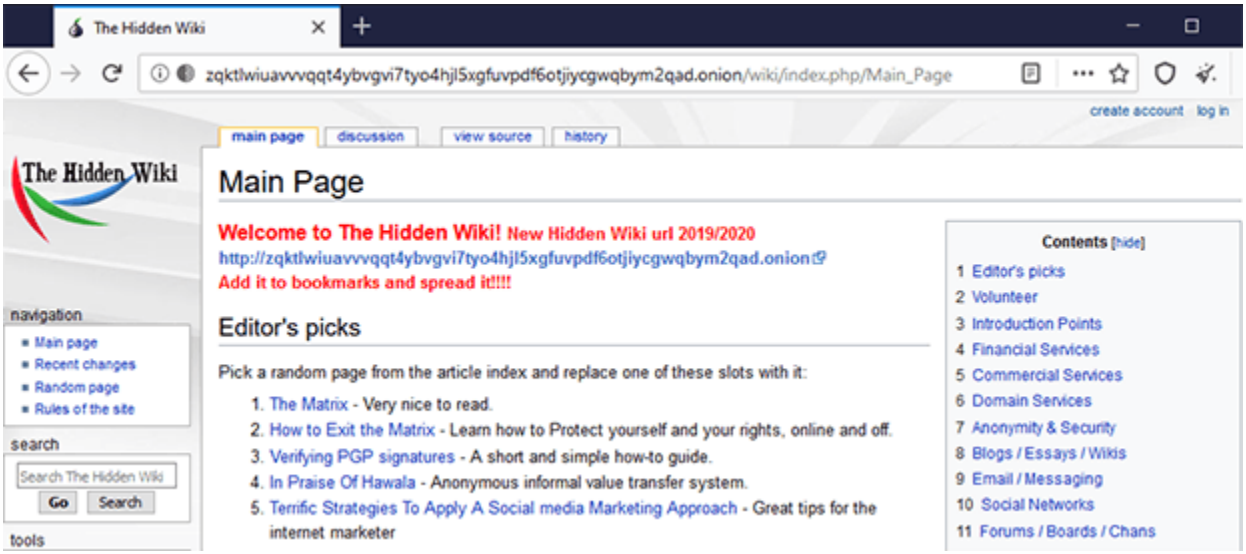
What Is Actually Down There

The Other Search Engines

Although DuckDuckGo seems to be a rather popular search engine for the Dark Web, there are some others as well, which are as follows:

1) The Hidden Wiki:

   As its name implies, there is a version of the Wikipedia that has been created solely for the Dark Web. With this portal, you can actually access different websites that are available on the Dark Web. Unlike the Wikipedia that is available on the Public Web, many of the of the search results that are returned back to you are actually garbled, and in a way, rather meaningless. For example, instead of giving you a valid domain, only alphanumeric text (which consists primarily of integers and letters all mixed up together), but the Hidden Wiki will take you to you these sites. But be cautioned, be extremely careful of what you actually click on. For example, it does not simply search for those websites that are actually legal. It will also search and index those websites as well which are extremely nefarious in nature. And in fact, yes, there are even spoofed up versions of the Hidden Wiki on the Dark Web as well. An example of this is seen in the illustration below:



(SOURCE: 1).

2) Sear X:

This is also deemed to be a rather "safe" search engine to use in the Dark Web. In fact, in some ways, it is even deemed to be more powerful than Google, as you can create search queries that are even much more granular. For example, you can build out these queries on the following permutations:

*Various different files;

*Certain images;

*Maps;

*All flavors of different music styles;

*News and science;

*Videos,

*Social media posts across ***all of the platforms*** that are currently available.

In fact, this search engine has been deemed to be more robust in returning results to you that are safe and legal to visit.

3) Daniel:

This is also yet another search engine that you can use in the Dark Web that is closely related to the Sear X. For example, there are well over 7,000 links which have already been indexed, which will help you getting more refined searches as you enter your query keywords into this search engine. Another very unique functionality of the Daniel search engine is that it will actually notify you if a website that you want to visit on the Dark Web is actually online and available. The primary advantage of this is that you don't have to spend waste hours combing through

each website to see if it is real or not. Another rule of thumb here: As it was mentioned in our last whitepaper, you don't want to stay of the Dark Web for a very long period of time – just for your own safety.

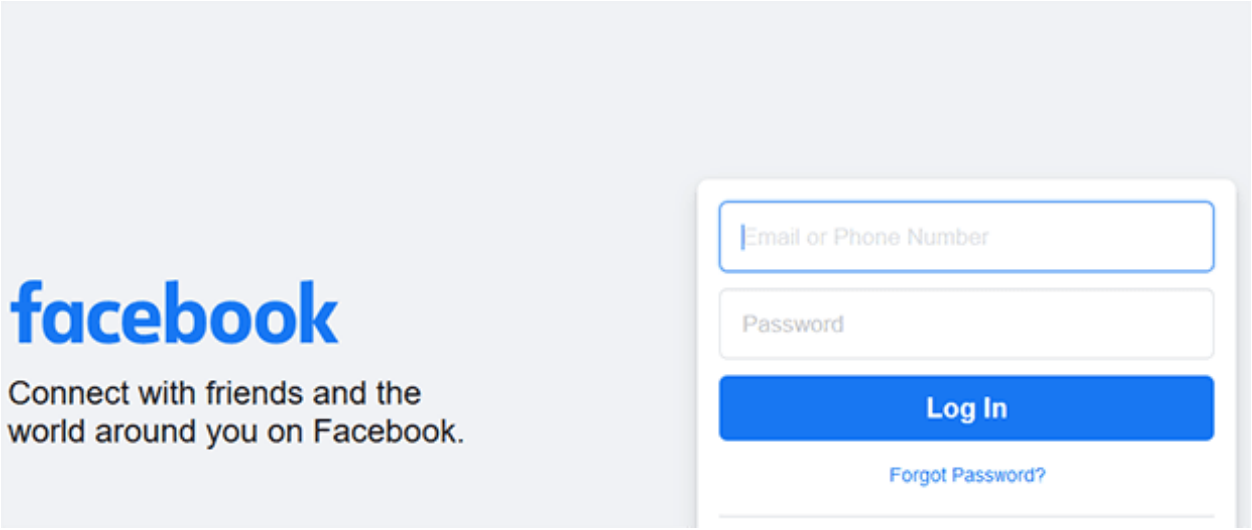
The Available Resources Worth Taking A Look At

In the Public Internet, while the freedom of speech and expression for the most part is protected, there are certain geographic regions around the world where there this is strictly forbidden. Therefore, there are many individuals, and even business entities that create specialized forums and websites so that they can express their views freely, without the fear of censorship.

In a way, this can be considered a good aspect of the Dark Web. But even then, one still has to be careful, because even a website and/or forum that has been created with good intentions can still be spoofed into a malicious one. So in this regard, here some other websites that are available for accessing and viewing on the Dark Web:

1) Facebook:

   Believe it or not, there is another version of this that lurks down there. One can create an anonymous account, in order to help protect their identity. But given how stealthy people are on the Dark Web, this probably will not last for too long. This "other version" of Facebook has been created for the sole purpose of avoiding censorship, as just discussed. The image below illustrates what this version of Facebook actually looks like:



   (SOURCE: 1).

2) The haven for Bitcoins:

   Many people very often have the notion that the Bitcoin and other Virtual Currencies are relatively new. While this may be true on the Public Internet, it is far from it on the Dark Web. They have been in existence for many years and is what is used to conduct financial transactions. The reason for this is simple: You never want to pay with a credit card, check, or even cash on the Dark Web. Not only is this the prime way to steal your identity, but law

enforcement will have a much easier time in tracking your movements. By paying with a Virtual Currency your anonymity remains relatively intact.

3) <u>BBC News</u>:

This famous news outlet also has its own website on the Dark Web as well. The idea here is to also avoid censorship in those countries where it is banned. Here, people can freely access news stories, and share thoughts, ideas, and comments. The news is not just restricted to that is happening in the United Kingdom, it covers events that happen on a global basis. An illustration of this Dark Web version is below:

(SOURCE: 1).

4) <u>A place for investigative journalism</u>:

Probably one of the more famous portals for this is known as “ProPublica”, as it maintains a rather strong presence on the Public Internet as well. In this regard, investigative journalism can thrive as much as it can, because with being on the Dark Web, people and groups can pretty much post anything they want to, or even provide evidence for an ongoing, investigative story that is going on. Another news portal that is similar in this regard is known as “Secure Drop”. This is specific place witnesses (aka “whistleblowers”) can meet with investigative journalists in order to share what they know while still remaining anonymous. In fact, some of the largest

news entities have even formed their own Secure Drop websites on the Dark Web, and examples of this include the following:

- Forbes;
- Reuters;
- The Financial Times.

The Communication Services

Yes, there are even various modes of communication on the Dark Web. Probably one of the most favored ones is that of posting on forums. But there is no guarantee of anonymity here. So, in an effort to do this, various Email services have thus emerged. A sampling of these are as follows:

1) Proton Mail:

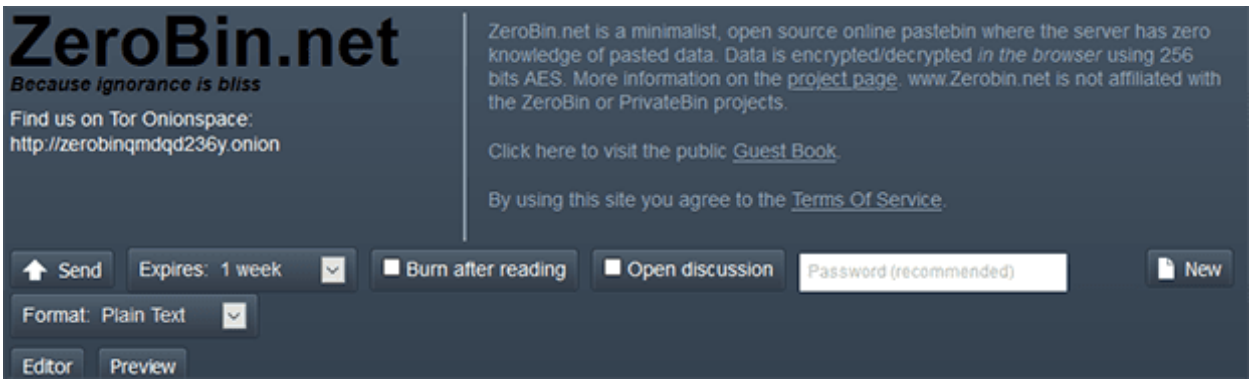
   This is an Email software package that was actually developed in Switzerland. This has been deemed to be one of the most robust and secure Email services that is available for use on the Dark Web. In fact, if you set up an account with them, you do not have to provide any sort of personal or confidential information about yourself. It has been designed to work in conjunction with the Tor Web Browser (which was reviewed in detail in the last whitepaper), thus making it more difficult for people to track your movements on the Dark Web - but keep in mind that there is no guarantee in this either.

2) SecMail:

   This is another Email service that is just as almost as popular as Proton Mail. The only drawback here is that you are allocated only 25 Mb of storage space.

3) Zero Bin:

   This Email package, which has been designed specifically for the Dark Web, but it also contains a chatting mechanism as well. What is nice about this is that after you have copied and pasted any content, it gets automatically encrypted; and your content of your Email/Chat message can also be protected with any type of password that you choose to create (of course, if it is long with alphanumeric values, the better it will be). An example of this is illustrated below:



(SOURCE: 1).

The Difficulties That Law Enforcement Has On The Dark Web

In our last whitepaper, we also examined some of the difficulties that law enforcement and digital forensics experts face when trying to collect evidence, especially those of a latent nature. But given just how things have been evolving from the standpoint of technology, especially driven by the COVID19 pandemic, collecting this evidence has not only become even more difficult, but even more time consuming as well. The end result of all of this is that it now takes a much longer time to bring a perpetrator to justice.

This is further substantiated by a recent study that was conducted by the RAND Corporation and the Police Executive Research Forum. Their findings include the following:

- The very small pieces of digital evidence such as Bitcoins, are very difficult to track down. But they are needed, as they can be linked to other, much larger pieces of latent evidence.

- Because the Cyberattacker now uses a myriad of sophisticated tools when they are in the Dark Web, it is very difficult for experts to build a comprehensive profile on them.

- Trying to prove the authenticity of digital evidence that is "anonymized" can prove to be a very laborious process, with no guarantees that it would be admissible in a court of law, even if the most minute trace of legitimacy can be ascertained.

- As mentioned, just about everything on the Dark Web is encrypted to some degree or another. As a result, this is makes that much more difficult to capture any digital evidence on a real time basis. The only way this can be done is by actually "jailbreaking" into the physical RAM of the server that is hosting a targeted website in order to collect this kind of evidence, and yet maintaining its integrity at the same time.

- It is very difficult for digital forensics investigators and law enforcement officials to actually break into a particular device in order to collect evidence. This is best exemplified by Apple and the FBI. On a number of instances, the FBI could bot break into the security features of the iPhone, and Apple refused to cooperate and help in this regard. Their claim was that it would invade upon not only the privacy rights of the individual in question but would also give their trade secrets when it came to their Encryption Algorithms.

- The various marketplaces on the Dark Web in which illicit transactions are very often hardened. Thus, it makes it even that much more difficult to collect any latent pieces of digital evidence.

- Once one piece of digital evidence has been found, it is often difficult to find other pieces that relate to it, thus making it even harder to build a case against an alleged perpetrator.

- The use of Cryptocurrencies often hinders the process of tracking down the Cyberattacker. For example, they could use the Bitcoin in one marketplace, but yet use an entirely different one in another marketplace.

Conclusions

Overall, this whitepaper has examined some of the places that you can visit once you have successfully penetrated into the Dark Web, and the difficulties when it comes to collecting digital evidence down there. The bottom line is that visiting the Dark Web is technically not illegal. But what you down there, even if it seems legal to you, can still get you in trouble either being caught by law enforcement, or even having your own identity stolen and that being used to launch subsequent Identity Theft attacks against you.

Also, no matter how sophisticated or intelligent the Cyberattacker may claim to be, there is always some sort of evidence left behind, even if it is the most miniscule in nature. At Exterro, we offer a range of products to help the law enforcement and digital forensics community in this regard.

Contact us today for more information!

Sources

1) https://vpnoverview.com/privacy/anonymous-browsing/dark-web-websites-worth-visiting/
2) "Identifying Law Enforcement Needs for Conducting Criminal Investigations Involving Evidence on the Dark Web", by the RAND Corporation.