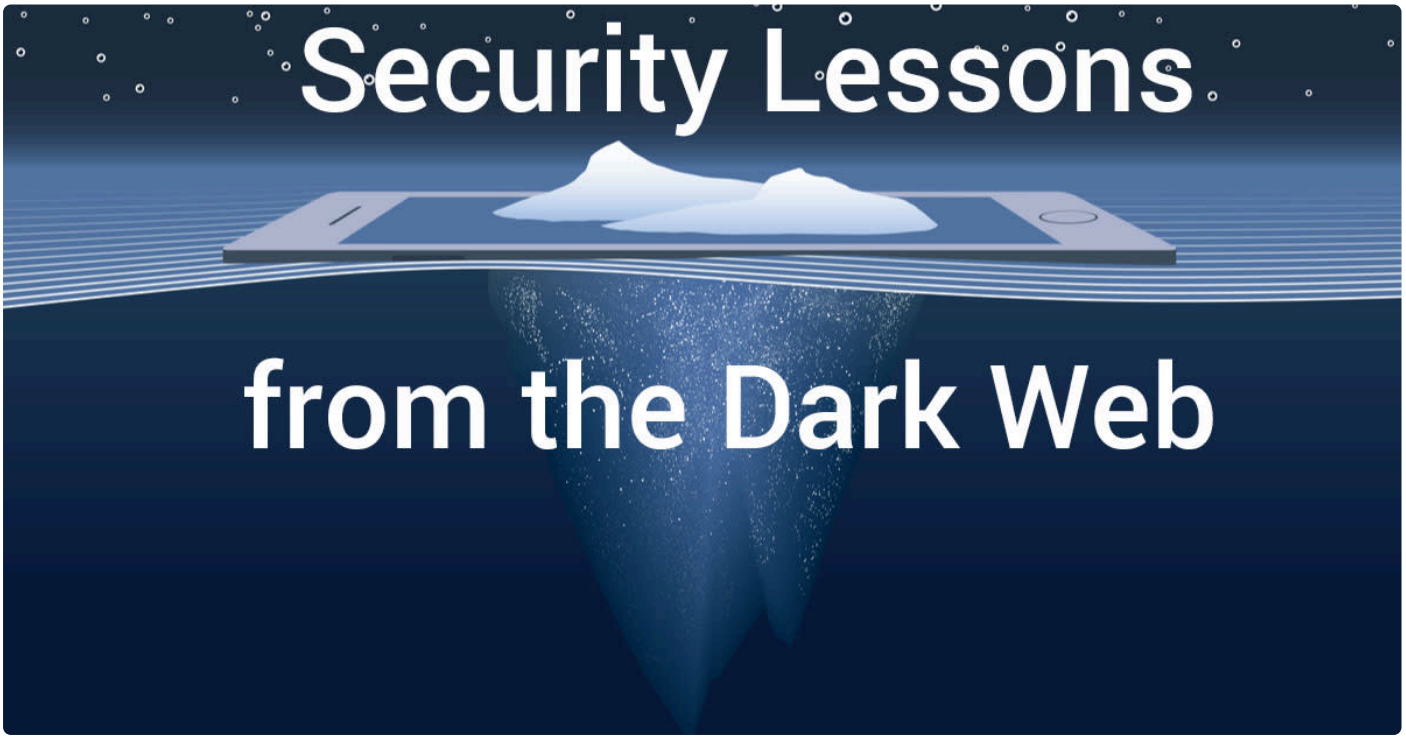
Security lessons from the Dark Web

Ewa Anna Szyszka · 2020-10-05



Most of us associate the dark web with criminal activities. Its the Internet's dark alley, where one can find spoofed documents, acquire illicit goods and get access to illegal content. However, this exact same place can serve as an excellent source of security knowledge and privacy lessons in the digital world. It is essential to distinguish between the so-called **Deep Web** and **Dark Web**. In this article, we will focus on the Dark Web, which is only a small part of the Deep Web.

What is the "Deep web"?

Deep Web can be defined as any content that cannot be accessed by crawlers like Google. Those are all the websites that you are unable to see by using search engines such as Google, Yandex, or NAVER. That means if, for example, you are taking a video course online and you need to log in into it in order to access the content, the content that is secured by the password belongs to the Deep Web, as it is not accessible from the search engine's viewpoint.

What is the "Dark web"?

On the other hand, the dark web is the content on the Internet that one can access using only specific browsers such as Tor or I2P. There are two crucial lessons ahead of us

(1) Layering, which looks at the onion routing and how the principle can be used in the clear web and **(2) Communication**, which looks at vulnerabilities of onion routing and traditional search engines and how they can communicate more securely on the Internet despite those vulnerabilities.

Lesson 1: Layering

The Tor browser enables users to access both the clear web and the dark web. The dark web sites are secured using the so-called **onion routing**, which is the extension that the websites on the darknet have instead of the traditional **.com**.

As illustrated below, the onion routing is designed so that instead of the client and server communicating directly with each other, the message is routed via a circuit.

The client has the keys to all nodes in the circuit and encodes the message using all of those keys. Then the message is passed from one node to another, and each node has only two pieces of information: with which key the layer should be decoded and to which node the message should be passed next. As the message passes through the onion network, each encryption layer is peeled off, and the message finally reaches the server.

The server does not know how many nodes there are in the circuit. Onion routing has some issues, which we will investigate closer in the next sections. However, the principle of layering can be well implemented in the clear web as well.

Many parties might be interested in eavesdropping and listening to what you have to say on the web. The principle of layering can be used to shield your privacy.

Just like the layers in the onion routing, one can use several layers of security as well. For example, connecting to the network via a VPN, which hides your computer's identity. You connect to a server with a VPN IP address, not the IP address our internet service provider has assigned. You can use **firewalls**, scanning the incoming traffic for listed websites, and on top of an antivirus and a proxy.

The onion routing also encrypts the messages sent via the insecure network. In the clear web, encryption should be a priority, especially when dealing with sensitive data. As a user, we should see any network that we are using as potentially insecure.

Security protocols such as TLS aim at providing more secure connections and tie the identity of an enterprise with one or more websites. However, there exists an extensive market for selling such certificates on the dark web. While handling sensitive data one should always act as if the network was insecure. Thus one should use different layers of security.

Lesson 2: End-2-end encryption

In the age of Deep Learning, one should be particularly careful about online presence and online communication. Despite higher anonymity on the dark web, it is possible to reveal your identity using deep learning techniques. For example, author identification analyses the writing style of a text and predicts if it was written by a particular person.

> The I2P Invisible Internet Project aims at addressing some of the vulnerabilities of Tor

Over time however the Tor browser revealed multiple vulnerabilities to attacks such as entry point surveillance, time analysis, and fingerprinting. There was a need for an even more secure browser. To provide even better online security and secure the anonymity of communication, the I2P Invisible Internet Project was created, that aimed at addressing some of the vulnerabilities of Tor.

I2P, unlike Tor, uses *garlic routing*, which relies on bundles of various messages that are encrypted together and sent across the network. An important lesson for the clear web user is that just like in the dark web, the websites' owners might be interested in investigating and analysing who is visiting their websites. Companies in the non-dark world are interested in acquiring your data to be able to sell it to marketers or use it for their own advertising purposes.

Garlic routing was a substantial improvement on the onion routing, as it focused on end-2-end encryption and decentralization. In the context of clear web communication, encryption protocols such as PGP can be used to encrypt messages containing sensitive information and ensure that we are using the end-2-end communication principle. No other third party is taking part in the communication. PGP makes used of a public key to encrypt the messages (for instance, your email), and your recipient would use a private key to decrypt it.

We should remember that the internet protocol by design does not offer the best anonymity solutions or protections of our data and communication on the web. As entrepreneurs, institutions, and individuals on the web, we should always protect ourselves against data breaches by layering multiple security techniques on top of each other. And we should carefully monitor how we connect to the Internet and via which channels we are communicating. In case of dealing with sensitive data, it's best to always see the network connection as insecure.

Sources

https://github.com/Attacks-on-Tor/Attacks-on-Tor
https://www.researchgate.net/publication/220117871_Security_of_Computer_Systems_and_Networks_Book_Preview
https://henryjacksonsociety.org/publications/terror-in-the-dark-how-terrorists-use-encryption-the-darknet-and-cryptocurrencies/
https://www.researchgate.net/publication/333651442_Terror_in_the_Deep_and_Dark_Web

Image: Shutterstock / C. Fish Images

This article was published on the Search Guard blog: https://search-guard.com/blog/security-lessons-dark-web/
Search Guard is Security and Alerting for Elasticsearch and Kibana — search-guard.com · Start a free trial