**ISTM 6206 Homework assignment 1 by Arsultan Nursapa**

The purpose of the assignment was to read approved article and write a paper that would provide a critical review of the article in which we would defend our position for or against the authors' tenets, assertions, and conclusions. Article that I chose to review is ISACA's Tech Brief on Darknet (http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/The-Darknet.aspx, 2018). Tech Brief series is designed to offer a high-level overview of an emerging or burgeoning technology for those unfamiliar or unaware of the subject.

For the purpose of a detailed analysis of this white paper, I have studied not only the articles and works to which the author of the paper referred but also additional information on the topic. I took great pleasure in reading them and all of them are listed in the References section.

In my opinion, the ability to express a position against an author of an article of such authoritative sources as NIST, ISACA or others requires at least more or less decent experience/knowledge in information security, and in particular on topic of discussion. Therefore, I consider a more correct position in my case to be only agreeing with the author of the white paper, giving some additional information and also expressing my understanding of the topic, which in no way claims to contradict the author's work. Thus, I present to your attention my view on the topic of Darknet in information security within the framework of the articles I have studied.

Darknet, sometimes called Dark Web or Deep Web, is part of the online shadow market. Darknet is a specialized group of sites where the identity of each user is hidden from the authorities, trackers and law enforcement agencies. Regular search engines and standard web browsers cannot see the Darknet pages. In essence, this is a private virtual space where people act anonymously to achieve their goals.

To work in Darknet the installation and use of special software is required. For this you need to be quite an experienced user. There are two options: I2P (Invisible Internet Project) protocol and TOR (The Onion Router) protocol.

The fact of having such an anonymous network like Darknet has both positive and negative ways to use it, which are:

Positive: Darknet serves as a haven for democracy and anti-corruption. Here whistleblowers can report corporate and government misconduct to the press, declassify corrupt practices that are hidden from the public, without fear of persecution. This network reigns complete freedom of speech and information. Darknet is also a place where people from despotic countries or oppressive religions can find like-minded people and even get help.

Negative: It acts as a black market, where you can buy or sell anything, any contraband, a stolen item or illegally obtained information. Drugs, weapons, stolen credit card numbers, illicit pornography, money laundering services, hacking services and even hiring hitmen.

On the other hand, there is one more way of using it which I am not able to address to any of the two ways mentioned above. Which is to use it for monitoring the negative aspects of the Darknet for the positive sake of information security. Information security specialists can monitor darknet activity to keep track of hackers activities and find out what content is usually monetized. Thus, practitioners may find out which assets of a company require additional protection. Companies can use a darknet to gather business intelligence, including information about competitors, employees, and leakage of confidential or proprietary corporate information. The white paper pays little attention to this topic, so I decided to add information that I personally find interesting as part of our ISTM 6206 course.

The author of the ISACA’s Tech brief on Darknet refers to an article (https://www.csoonline.com/article/3205924/data-breach/is-your-data-being-sold-on-the-dark-web.html?upd=1550683945143, 2018) where the role of information security specialists in monitoring the darknet and the results of conducted research are discussed in detail. This article in my opinion deserves more attention than it is given.

According to the article the dark side of the internet is actually not that big. Media often overestimates the size of the dark network, mixing everything that is not available to search engines, including corporate intranets and password-protected sites, such as online forums, banking sites, and email platforms. Scan of Tor network by the PunkSpider Web vulnerability scanner taken in 2015 found around 7 000 Tor sites, only 2 000 of which were active. Not all of these sites are run by criminals. When it comes to criminally oriented darknet sites, not all of them are of interest to information security specialists, but only 5%.

However, for most companies it would be better to let someone else do the monitoring. *"There are a lot of risks you run, from law enforcement and other perspectives, from interacting on the dark web"* - ThreatQuotient's Couch.

Nowadays, there are many specialized vendors of darknet site monitoring services. Specialists of these vendors are well trained and adapted to work in the darknet. They are embedded within hacking forums in order to gather and receive information hacking activities from the real members of such forums. These vendors develop techniques and tools for automated darknet mining, analyze gathered data and prepare detailed analysis.

One such analysis is referenced in the white paper - The 2017 DarkOwl Darknet Index: Reranking the Fortune 500 using Darknet Intelligence (DARKINT™). Although only one chart taken from it to the white paper, I find it of a big interest to me with regard to our course as it shows how much infosec is important nowadays.

DarkOwl has built a proprietary database of darknet content which is the most comprehensive one of its kind in the world, they claim. This database is automatically and continuously updated with between 10 to 15 million pages per day, from the Tor network alone. Darknet content is indexed and searchable in 47 languages for organizations wishing to monitor their data on the darknet.

For the analysis DarkOwl used their DarkOwl Vision database to rank all members of the Fortune 500 based on their darknet footprint.

The key takeaways from the analysis are:

* Every Fortune 500 company is exposed.
* Amazon leads the Index.
* Technology and telecommunications companies overall are the largest target
* Financial firms perform better than expected.
* Hacked valuable data = increased risk.
* Vigilance pays off.

Among these key takeaways the last in my opinion is the most important. Investing in cybersecurity provides tangible benefits on the Darknet index. Sectors that invested significant funds in infosec, in some cases have less impact and, consequently, lower index ratings.

“*Today, in an age where data loss is virtually inevitable, it is critical to look at the darknet as a key part of a complete cybersecurity program, enabling organizations to swiftly detect security gaps and mitigate damage prior to the misuse of data” - DarkOwl.*

Today, the presence of the darknet is a given, which for a number of political and social reasons cannot be refused. One way or another it is necessary to accept it and adapt to it. I consider the readiness to meet this reality and adapting to it in one of the mentioned above ways is a skill that would be highly appreciated in the near future*.*

There are many arguments against Darknet and on whether or not it should be banned, extinguished. In my opinion it should remain. Before starting this homework, I already had some experience with Darknet and Tor browser. I used TOR for visiting sites that are banned in my home country for political reasons. I also used it to express and interchange my opinion with others on some issues that happen in our country that in case of deanonymizing would be persecuted. Therefore, for me it was even more interesting to review this particular topic and to express my opinion on it not only from infosec view point, but also from my own personal view point. Such anonymity tools provide basic freedoms and rights at least online for many people that feel lack of it in the real world.

References:

1. Pagliery, Jose; “The Deep Web you don't know about,” CNN tech, 10 March 2014, http://money.cnn.com/2014/03/10/technology/deep-web/index.html
2. Guccione, D.; “What is the dark web? Why (and how) to visit this invisible part of the internet,” CSO, 19 January 2018, https://www.csoonline.com/article/3249765/data-breach/what-is-the-dark-web-is-it-illegal-and-should-you-ever-visit-the-dark-web.html
3. Jamieson, C.; “Understanding the Deep and Dark Web: mitigating risk and protecting your brand,” World Trademark Review, 18 May 2017, www.worldtrademarkreview.com/Intelligence/Anti-counterfeiting/2017/Industry-insight/Understanding-the-Deep-and-Dark-Web-mitigating-risk-and-protecting-your-brand
4. DarkOwl™, “Every company in the 2017 Fortune 500 is exposed on the darknet,” <https://www.darkowl.com/darknet-index-fortune-500/>
5. Gil, P.; “The Darknet: Black Market and Sanctuary” https://www.lifewire.com/darknet-black-market-2483129
6. Moore, D and Rid, T.; “Cryptopolitik and the Darknet.” Survival 58.1 (2016): 7–38.

<https://www.tandfonline.com/doi/citedby/10.1080/00396338.2016.1142085#tabMdule>