PRACTITIONERS' BROAD VIEW

THE DARK WEB – A USEFUL TOOL FOR THE OPEN SOURCE INTELLIGENCE GATHERING (OSINT) AND A CHALLENGE FOR THE SECURITY SECTOR

GIS Representative*

Abstract:

The spread of the global network (the Internet) throughout the public has completely changed and simplified the means of communication, exchanging information and the working process. It has become a useful tool for specialists represented in almost all fields, as it allows them to quickly search, verify and share information. The Internet has greatly simplified and increased the effectiveness of the working process of the Government Agencies, including those that are represented in the security sector. Nevertheless, it also created new challenges which can pose a threat to ordinary citizens, different groups, organizations and Governments. Countries were forced to adapt and integrate new ways of working in order to prevent and counteract novel security threats. Some divisions represented in the security sector had to completely transform in order to combat new challenges.

Due to the fact that the law enforcement agencies are able to fight cybercrime in the "Surface Network", the "criminal world" of the Internet has shifted to a completely different Internet space – The Dark Web, where it tries to bypass the law without leaving any trace by using a variety of available software, thus creating a serious threat for the Global Community.

Keywords: *global network, dark web, security, OSINT.*

Introduction

Kaspersky Lab blog state that "the Internet is sizable with millions of web pages, databases, and servers all running 24 hours a day. But the so-called "visible" Internet (aka *surface web* or *open web*) that most of us use on a daily basis and can be found using search

* Georgian Intelligence Service (GIS).

engines like Google and Yahoo – makes up under 5% of the total internet and is considered to be only the 'tip of the iceberg'." As for the Internet that is unreachable (or reachable through special software) for ordinary citizens, also known as "Deep Web" and "Dark Web", it accounts for up to 95% of the whole Internet Space (Kaspersky Lab blog; McAfee blog; Norton blog). Most people often use the term "Deep Web" when talking about the "Dark Web", but they both differ in nature.

"The Deep Web is part of the World Wide Web whose contents are not indexed by standard web search-engines (e.g. Google, Yandex, and Bing) and makes it hard for the law enforcement agencies and ordinary people to search for the specific websites." (Karpersky Lab blog) The opposite term is "surface web", which is readily available to the general public and searchable with standard web search engines.

The Dark web refers to sites that are not indexed and can only be accessed via specialized software (e.g. TOR, I2P, and Freenet). Significantly smaller than the tiny surface web, the dark web is considered a part of the deep web. The specialized software helps the Internet user to access the unreachable web by hiding his/her IP address, thus ensuring anonymity.

"Even if the cover of the dark web often keeps law enforcement at bay, basic tools can enable anyone to engage dark web services without much difficulty. Basic internet literacy, a computer, and access to the internet are enough for any sufficiently motivated individual to begin supplying or purchasing illicit goods on the Dark Web." (Karpersky Lab blog)

The Deep Web

The deep web accounts for approximately 90% of all websites and is considered to be "much larger than the surface web. In fact, this hidden web is so large that it is impossible to discover exactly how many pages or websites are active at any one time." (McAfee blog) According to some sources, the Deep Web holds approximately 7.5 petabytes – about 400-500 times bigger than the Surface web. As already mentioned, the content of the Deep Web is not indexed by standard web search-engines, which makes it hard for internet users to directly access its contents. "While many news outlets use 'deep web'

and 'dark web' in the same context, in fact, Dark Web is the part of the Deep Web, which is mostly legal and safe. Some of the largest parts of the deep web include":

- "Databases: both publicly and privately protected file collections that are not connected to other areas of the web, only to be searched within the database itself."
- "Intranets: internal networks for enterprises, governments, educational facilities and groups of individuals used to communicate privately and control aspects within their organizations."
    - The user should know the direct link of the non-indexed website he/she wants to access. However, the given resource may require the visitor to enter a password, which must either be created during registration, or received directly from the owner or a member of the website.
    - Access to the content is decided by the Admin, who sets the list of IP addresses of computer users with access to the website.

Some of the Deep web sites "may be concealed behind passwords or other security walls, while others simply tell search engines to not "crawl" them." Without visible links, these pages are more hidden for various reasons. Their "hidden" content is generally cleaner and safer. Everything from blog posts in-review and pending web page redesigns, to the pages you access when you bank online.

Dark Web

Like the "Deep Web", the Dark Web's content is also not indexed by standard web search-engines and, in order to access it, the Internet users must install special software, such as TOR, I2P, and Freenet, which also ensures their anonymity. "Dark Web can be small peer-to-peer or friend-to-friend networks, as well as large networks like Tor and I2P operated by organizations and individuals. The Tor network focuses on providing anonymous access to the Internet and I2P specializes in anonymous hosting of websites." (Karpersky Lab blog)

It is possible to identify the owners of non-indexed websites located in the Deep Web with the help of different technical means (e.g. it is possible to determine who buys, who visits and to whom the website domain is registered), but this is impossible in the case of the "Dark Web", due to the fact that it was created by using the TOR / I2p / Freenet network. The Dark Web websites do not share the same principles of naming their domain like the Surface websites (e.g. bbc.com, facebook.com, google.com). The Dark Web domain consists of various characters (numbers, letters, etc.) and ends with .onion or .i2p (similar to the surface web: .com, .ru, .com.uk). It is not possible to access websites ending in .onion or .i2p through normal browsers as they are not part of the DNS system. Onion websites are only perceived by Onion servers.

As already mentioned, the software used to access the Dark Web allows users to surf the Internet anonymously by avoiding the Government institutions and without leaving traces. This creates a ground for journalists, bloggers, various opposition groups, or followers of certain ideologies to use the Dark Web as a platform to exchange information, discuss various issues and express their opinions freely. Likewise, free e-libraries and banned literature are also available for the web users. However, the Dark Web is actively used by individuals who are involved in criminal activities.

The Dark Web is mostly used for drug trafficking and there are many websites that offer users a vast variety of drugs. The most well-known website that was used as a platform to sell drugs and other illegal products was – The Silk Road (known as the Amazon.com of the Dark Web). The Website was shut down by the US Federal Bureau of Investigation in 2013, but it didn't solve the problem; if anything, it made it even worse as it led to the creation of many other websites with similar content.

Buying drugs is not the main interest for most Dark Web users. "Customers" have access to the illegal trade of classified information and weaponry. They can also view/order sadistic videos and child pornography in exchange for crypto currency, purchase personal information about individuals (passwords to various accounts, information on bank debit cards etc.), organize a terror attack, hire

hackers and hitmen for various tasks and order fake documents. The users carry out the aforementioned illegal activities through various websites, forums, online stores and social networks. There are speculations that there are websites related to the so-called "Islamic State", through which young people around the world are recruited and become part of organized terrorist attacks.

The Dark Web can be used by certain groups driven by anti-state interests and might be directly/indirectly controlled by other states; if necessary, other states can also aid the members of the covert group with financial support (with crypto currencies) and, if needed, provide them with an action plan and advice. The Dark Web might also be used as a communication platform by opposition forces against the government (e.g. the opposition Tor during the Arab spring)

The law enforcement agencies throughout the world are actively involved in the Dark Web (also Global Web) monitoring process in order to: identify individuals involved in criminal activities; detect a leak of classified/personal information and take measures to delete it; identify dissident groups working for other states.

Although detecting threats in the Web might seem complicated, law enforcement agencies are still able to successfully identify illegal activities through the joint efforts of OSINT, SIGINT and HUMINT units (Easttom, 2018; Froomkin, 2015, Kumar and Rosenbach, 2019).

Dark web as a source for OSINT gathering

"Open Source Intelligence (OSINT) gathering and a proper understanding of the Dark Web are the first step in combating the Internet's dark spaces. With an understanding of how to use open source encrypted anonymity services safely, organizations can explore OSINT sources – which include web-based communities, user-generated content, social-networking sites, wikis, blogs and news sources – to investigate potential threats or analyse relevant information for business purposes." (McAfee blog) As already mentioned, the Dark Web has become a platform for journalists, anti-state-minded citizens, dissidents and public officials with harmful intentions to share/leak various types of information. Web users will often come across classified documents belonging to private companies

and Governments, which were obtained as a result of cyber-attacks carried out by hackers on the servers of the aforementioned institutions. It should be noted that there have been many cases of leaked classified information which negatively impacted some states and defiled their reputation. Searching for the leaked documents is considered to be one of the main interests of OSINT gathering and many of the obtained papers are valuable for their contents.

Cases of leaked information on the Dark Web

Databases of the agencies of different countries containing information about citizens have been repeatedly leaked into the Dark Web.

WikiLeaks. A website that publishes classified documents provided by anonymous sources and hackers. The information posted on the website has not once received international attention and even caused diplomatic scandal. Access to WikiLeaks is also possible with ordinary browsers (Chrome, Opera, Firefox), although most of the documents posted on the website are available only on the Dark Web version of WikiLeaks

In 2019, hackers leaked data on 267 million users of the social network Facebook, which contained information about their identities, dates of birth, addresses and Facebook IDs. The leak mainly affected the Facebook users living in the US;

In 2019, hackers obtained information on nearly 620 million users registered on 16 popular websites which, in addition to identities and other personal data, contained user accounts, passwords and Debit Card information.

In 2020, information on 500,000 users (including accounts and passwords) of the video-telephony software program ZOOM was made available on the Dark Web. Information on most of the accounts was for sale (approx. 1 US cent per account) but some pieces were provided for free.

Examples of Dark Web websites that can be used for OSINT gathering

The information and websites on the Dark Web can be accessed through search engines designed specifically for the web, although most websites require the knowledge of their direct links. There are many websites that provide a long list of various websites, although the data may be obsolete because the websites on the Internet are not stable - they are often deleted by various law enforcement agencies (if the website is illegal), or by the owners themselves. There are many sources that are considered interesting for OSINT gathering, including some of the websites given below:

Tor Facebook (facebookcorewwwi.onion)

- Facebook created a special address for users to access its website securely with an end-to-end encryption. Ideally, this means that Tor users, some of whom may be using the software to circumvent government censorship or restrictions of the internet in places such as China or Iran, will be able to use Facebook reliably and without worrying about leaking their personal information. It is reported, that TOR Facebook is being used by over 1 million people monthly.

The Hub

- It is considered to be the largest discussion forum on the dark web focused on dark net market, reviews, crypto currency and cyber security. The forum gives its users access to a variety of groups of interest. According to the recommendations provided by Internet users, in order to get acquainted with the Dark Web, you must join The Hub.

Sci-Hub

- A large database of scientific papers from around the world that was obtained and uploaded by hackers. Anyone can read and download papers prepared by scientific institutes.

ProPublica

- An investigative journalism outlet which has a presence on the surface web but also a dark web link. This way, visitors of the website can remain anonymous if they want to. This could come in handy for people living under oppressive

regimes, for instance. After all, ProPublica doesn't shy away from covering controversial topics, such as child labour and corrupt politicians. ProPublica publishes news stories in both English and Spanish.

SecureDrop

- A place where whistle-blowers and journalists meet. The dark web is one of the only ways for whistle-blowers to share their information while being certain they won't be tracked down. Whistle-blowers often have damaging information about a company or government and try to share this with journalists. If they do so, on the surface web, they'll likely be traced and, in some cases, punished. SecureDrop is an .onion website that protects the privacy of whistle-blowers and journalists all over the world. Many important publishers and news organizations have realized the power of anonymous whistle-blowers on the dark web and have set up their own SecureDrop URL. Some notable examples include: Forbes: http://t5pv5o4t6jyjilp6.onion/; The Financial Times: http://xdm7flvwt3uvsrrd.onion/; and Reuters: http:// smb7p276iht3i2fj.onion/

Conclusions

As already mentioned, the use of illicit Internet is on the rise and the Dark Web has become a platform for criminal activity, where users roam freely and get involved into various illegal deeds. Although law enforcement agencies have witnessed a steady expansion of dark web activities, they largely lack quantitative data to inform effective responses and solutions to dark web activities.

The Dark web activity crosses national borders. The cross-jurisdictional nature of the dark web makes it essential that investigators collaborate across agencies. Therefore, the law enforcement agencies of various countries must cooperate in order to counter the incoming threats more effectively and in time. Constant communication, sharing information and personal experiences between the partner organizations will play a vital role in this regard.

Specialists states that: "The 'dark web' is an internet shadow world where the good and the bad co-exist. On the good side, the dark web provides anonymous, secure communication channels to shield classified government activity and protect reform agents such as human rights activists and journalists opposed by oppressive foreign regimes. On the bad side, the dark web has emerged as an important hub of criminal commerce, a fully functional marketplace where hidden customers can buy from hidden sellers with relative confidence, often with customer ratings available, just as on the public-facing web."

References:

1. Easttom, Chuck, (2018). "Conducting Investigations on the Dark Web", *Journal of Information Warfare*, vol. 17, Issue 4. Available on https://www.jinfowar.com/journal/volume-17-issue-4/conducting-investigations-dark-web

2. Froomkin, Dan. (September 11, 2015). *FBI Director Claims Tor and the "Dark Web" won't let criminals hide from his agents.* Available on https://theintercept.com/2015/09/10/comey-asserts-tors-dark-web-longer-dark-fbi/

3. Kaspersky Lab Blog. (n.d.). *What is the Deep and Dark Web?*, Available on https://www.kaspersky.com/resource-center/threats/deep-web

4. Kumar, Aditi, Rosenbach, Eric. (September 2019). "*The Truth about the Dark Web.* Intended to protect dissidents, it has also cloaked illegal activity", *Finance & Development*, International Monetary Fund, Vol. 56, No. 3. Available on https://www.imf.org/external/pubs/ft/fandd/2019/09/pdf/the-truth-about-the-dark-web-kumar.pdf

5. McAfee Blog. (August 24, 2015). *The Mysterious, Ominous Dark Web: A Primer for the Rest of Us.* Available on https://www.mcafee.com/blogs/internet-security/what-the-dark-web-is/

6. Norton Blog (n.d.). *The emerging threats. What is the dark web?* Available on https://uk.norton.com/internetsecurity-emerging-threats-what-is-the-dark-web.html

7. Leigh, David, Harding, Luke. (2011). *WikiLeaks: Inside Julian Assange's War on Secrecy*, London: Guardian Books.

8. Tor Project website. Sponsors. Available on https://www.torproject.org/about/sponsors/