

PREVIEW PREVIEW PREVIEW PREVIEW

HAKING

VOL. 18

NO. 05



EXPLORING THE DARK WEB

SLICING
THE ONION:
AN
INTRODUCTION
TO THE
ONION
ROUTING

AI AND
THE WAR
ON TRUST

EXPLORING
THE
DARK WEB:
UNVEILING
ITS **DUAL**
NATURE OF
GOOD AND

THE **SOCIAL**
DANGERS OF
THE DARK WEB

PREVIEW PREVIEW PREVIEW PREVIEW

EDITOR'S WORD

Dear Readers,

Enter the world of the Dark Web...

The vast expanse of the digital realm is much like the great oceans of our planet: we've explored only a fraction, with fathomless depths still concealed in mystery. Just below the Surface Web, which is the portion we navigate daily, lies the deepest, most enigmatic layer: the Dark Web. It's a term that often conjures images of shadowy figures, illicit activities, and digital rogues. But is it just that? Or is there more beneath the surface waiting to be discovered?

In this issue of Hakin9 Magazine, we're delving deep into the recesses of the Dark Web – not meaning to sensationalize, but to educate and inform. Our mission is to demystify the misconceptions, unravel the complexities, and shed light on how cybersecurity is intrinsically tied to this often misunderstood digital underworld. You will find articles on protecting your privacy online and the dual nature of the web.

We're very proud of this issue and without further ado... Delve in!

Helena Piorun and the **Hakin9** Editorial Team

HELENA.PIORUN@HAKIN9.ORG

EDITOR-IN-CHIEF
JOANNA KRETOWICZ
JOANNA.KRETOWICZ@HAKIN9.ORG

ASSOCIATE EDITOR
HELENA PIORUN
HELENA.PIORUN@HAKIN9.ORG

Cover Image
Wiktoría Bukowska

Technical Editors
Lee McKenziie

Cover Design
Wiktoría Bukowska

Reviewers
Daniel Boughton, Bev Robb, Momen Eldawakhly, Jose Manuel Orteg, Bhavin Makwana, FREREBEAU Laurent, Gabriel Carvalhaes, Doug Have, Justin Smith, Michal Jachim, Jay Kay, Paul Mellen, David von Vistauxx, Craig, Nadav Hashimshony, Javier Perez

04	EXPLORING THE DARK WEB: UNVEILING ITS DUAL NATURE OF GOOD AND EVIL
16	SLICING THE ONION: AN INTRODUCTION TO THE ONION ROUTING
26	THE BRING YOUR OWN DEVICE (BYOD) DILEMMA
34	AI AND THE WAR ON TRUST
42	CYBERATTACKS WITH THE USE OF AI
69	MULTI-FACTOR IDENTIFICATION AND AI TOOLS
78	INTRODUCTION TO DEFENSIVE AND OFFENSIVE AI IN CYBERSECURITY
92	HOW TO PROTECT YOURSELF ON THE DEEP WEB: TOOLS, EVALUATION, LEGALITY AND EXPECTATIONS
101	THE SOCIAL DANGERS OF THE DARK WEB
103	ARTYKULARTYKULARTYKULARTYKULARTYKULARTYKULARTYKULARTYKULARTYKUL

All trademarks, trade names, or logos mentioned or used are the property of their respective owners. The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.

Goce Stevanoski

Exploring the Dark Web: Unveiling its Dual Nature of Good and Evil

Freedom of speech is one of the fundamental human rights. It took a long time in human history to be developed to this stage of freedom and openness. With the advancement of the different technologies for communication and information dissemination, much research has had the vision that freedom of speech and open idea sharing will become more and more developed [1]. However, the new technologies don't always allow for free communications. Current technologies can limit the access to free communication and can impose surveillance on private communication [2].

The technology behind the Internet is leading to global interconnections and information availability. These technologies are making our life easier and more productive. We are able to exchange news information, currencies, social likes and dislikes, we can work over internet, even we can show our affection to some person. But this does not come without some price that has to be paid. The price is access to our privacy [3].

From social media sites and advertising agencies to state sponsored intelligence agencies, everybody is aware that the internet is an ocean full of data, particularly corporate and private data. This greed for private and corporate data leads companies to develop tools and methods for gathering and storing the data for their specific purposes. State agencies are developing tools for intelligence activities that result in many cases of illegal activities on their own population [4], and social media and advertising agencies are gathering data for specific target marketing or reselling to other parties [3]. All these personal and corporate data can be used for influencing large population groups by indoctrinating them with selected news information [5] or for limiting their freedom of speech and, in many cases, even completely prohibit it.

This situation in the open internet shows the need for the introduction of a network that will provide better privacy online for regular users [6]. Developed in the mid-1990s as a project of US's Office of Naval Research (ONR) and DARPA agency, TOR Project successfully fulfilled this need. TOR, an abbreviation of "The Onion Router", was a project for implementing anonymity for the US intelligence agents that needed to be connected on the internet in any part of the world. With this project, the anonymity of the user is achieved by encrypting the data in an "application layer" multiple times. Further, this encrypted data is rerouted over many relay points, which are decrypting the data, a layer on each relay point (Figure 1). By this, on the destination side, the receiver does not know the source location. With this project, a special top level domain suffix was introduced, ".onion", that allows creating and hosting hidden web pages on the TOR network. All users and servers that are anonymously connected over TOR project are accessible over a specially created TOR Browser [7]. Because TOR network guarantees anonymity on the network, and as an opposite of the Clearnet (regular internet access over search engines), it was named Darknet or the Dark Web.

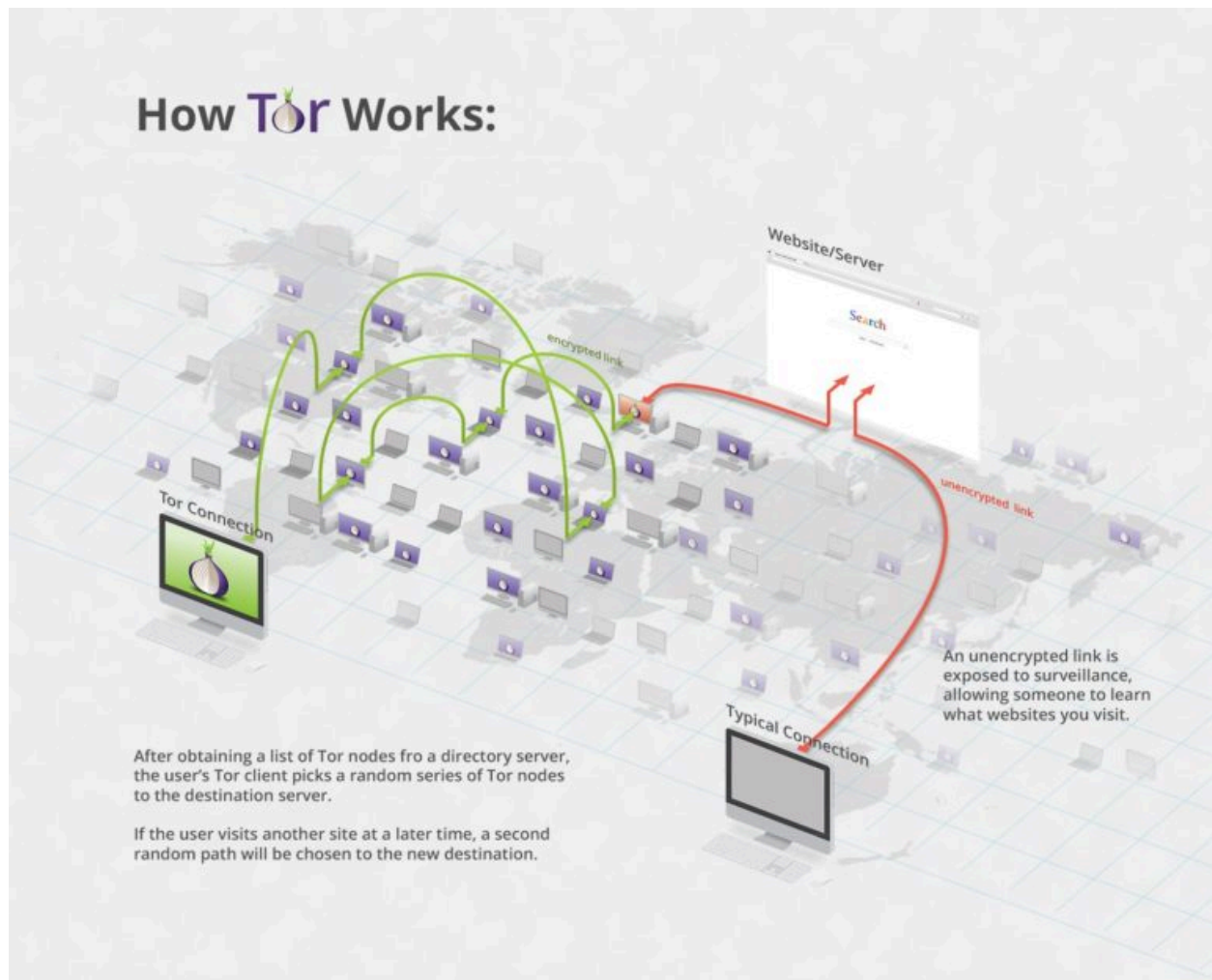


Figure 1: How TOR works.

Source of the image: <https://www.extremetech.com/internet/279391-indie-isp-offering-tor-enabled-sim-cards/>

This successful implementation of anonymity over the Internet revealed many other aspects for utilization of the Dark Web. The aspects can be presented as good and evil sides of the Dark Web.

The good side of the Dark Web

On the good side, anonymous interaction on the internet can help different social rights activists, people that are under a totalitarian regime, threatened journalists and bloggers. Nowadays, the Dark Web has become a digital space that enables regaining the right for freedom of speech in censorship circumstances.

This network allows whistleblowers to expose all kind of violations and stay anonymous. There are news agencies that have their own presence on the Dark Web where whistleblowers can securely drop their digital material. Daily newspapers, like the British, The Guardian (Figure 2) and the US, New York Times (Figure 3), are only some of the news agencies that have secure drop on the Dark Web. This practice gives them an opportunity to obtain relevant information without revealing the source, which is very important in investigative journalism [8].

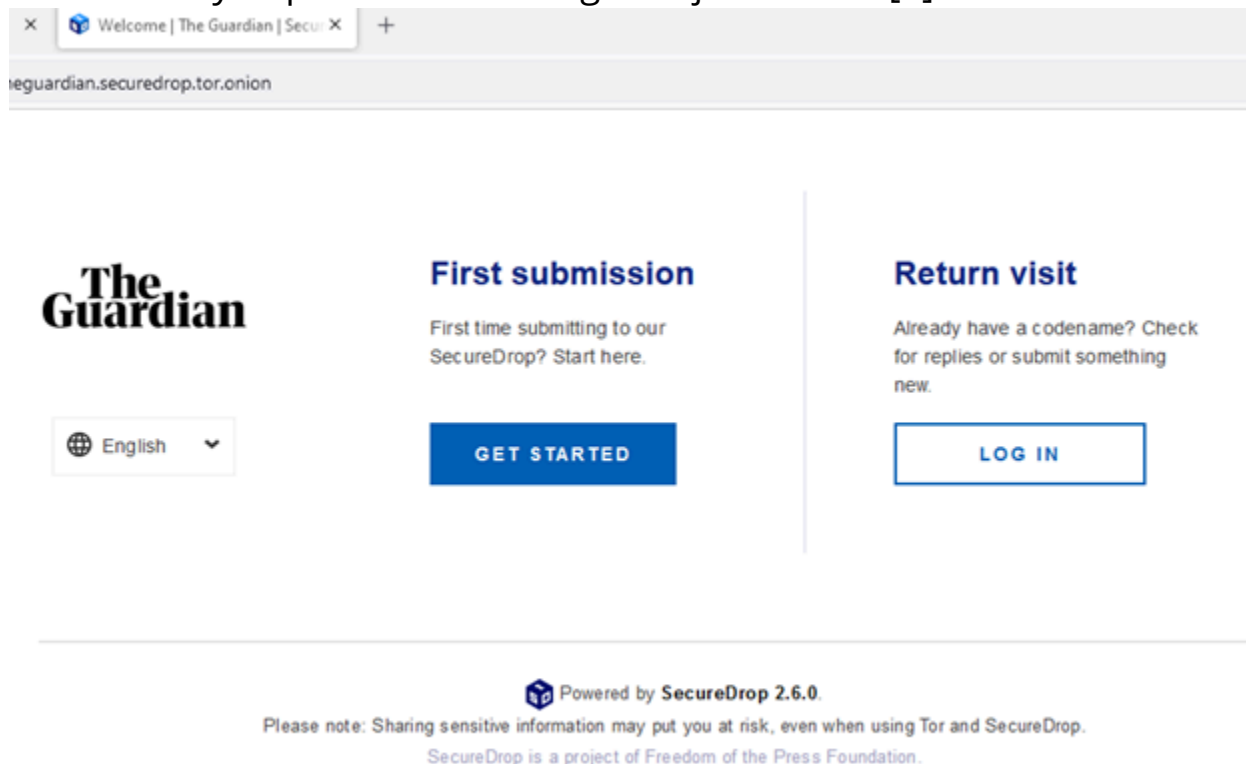


Figure 2: The secure drop on the Dark Web of British daily newspaper

The Guardian URL: <http://theguardian.securedrop.tor.onion/>

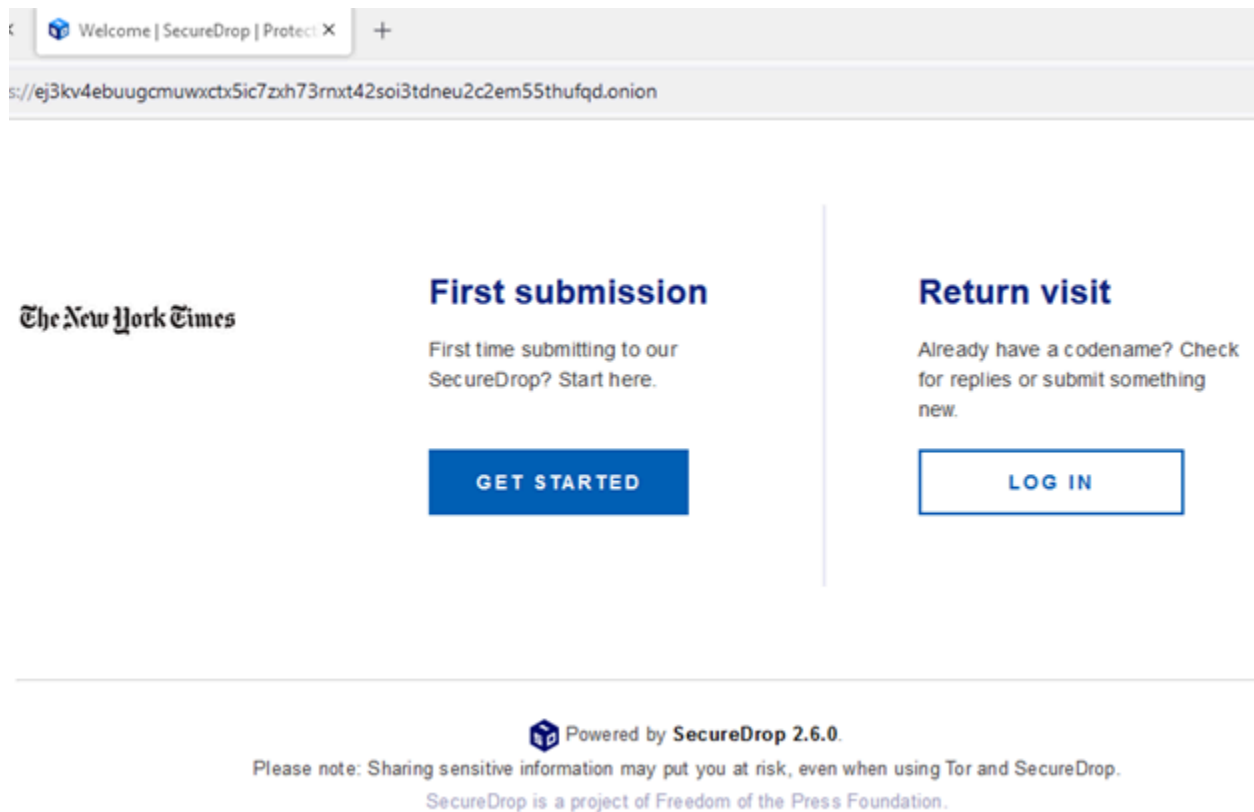


Figure 3: The secure drop on the Dark Web of US daily newspaper

The New York Times, URL: <https://ej3kv4ebuugcmuwxctx5ic7zxh73rnxt42soi3tdneu2c2em55thufqd.onion/>

All over the world, many activist groups need secure communication lines to coordinate their activities. The Dark Web provides this kind of service. Here are some examples that show the usefulness of the Dark Web infrastructure for these activists groups:



Figure 4: People protesting against internet censorship during Arab Spring Uprising – Egypt

Source: <https://johnpostill.wordpress.com/2011/02/10/egypt-uprising-different-media-ensembles-at-different-stages/>

- In the Arab Spring uprising in 2011, many governments across the Arab world implemented internet censorship and mass communication surveillance on their own population. People, especially in Egypt, had used TOR browser to avoid the governmental censorship and maintain secure communication and information sharing [9].

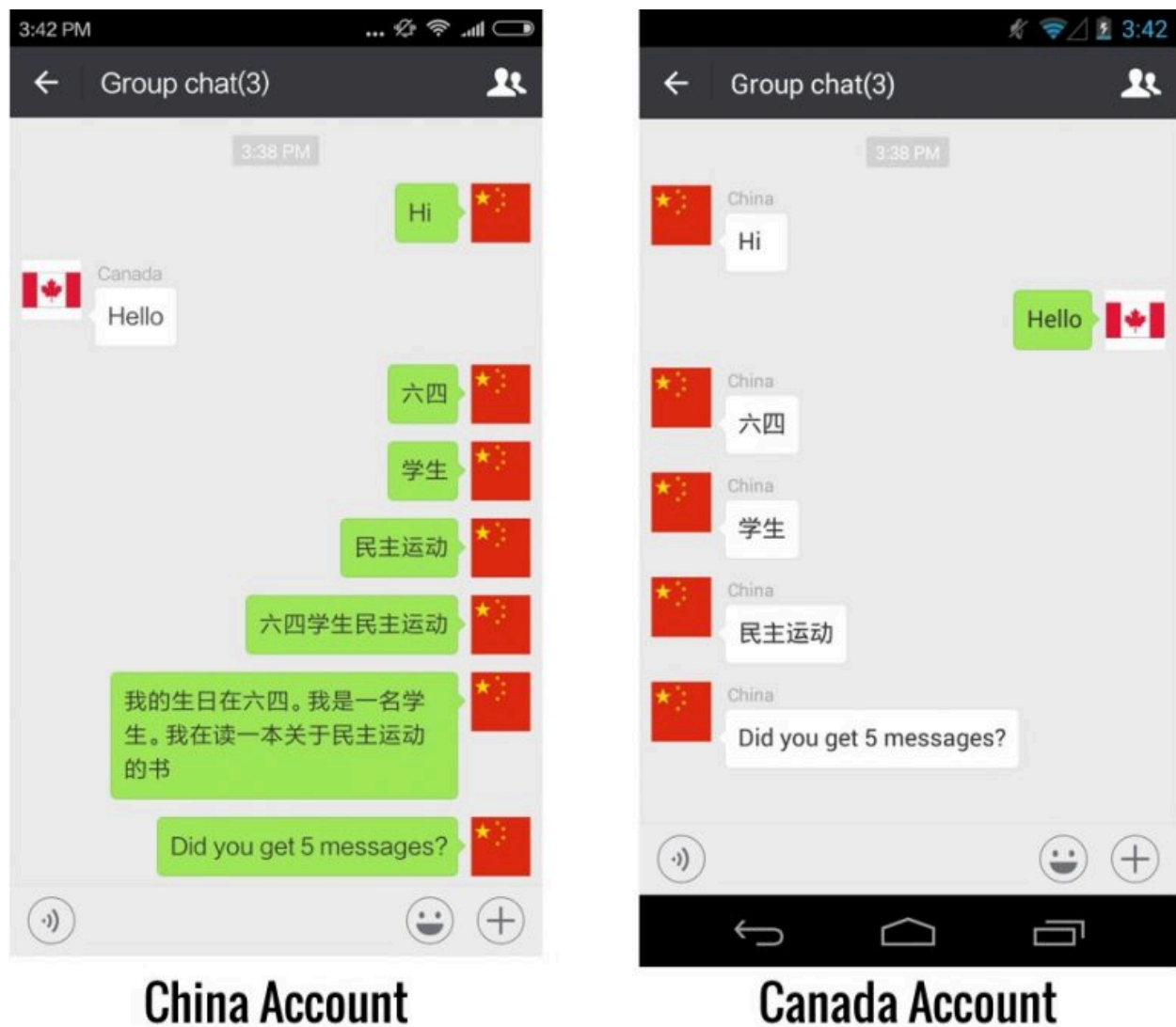


Figure 5: Comparison of one conversation over same network in censorship environment

Source: <https://www.hongkongfp.com/2016/12/01/one-app-two-systems-wechat-censorship-researchers-find/>

- During the mass protest in Hong Kong, the “Umbrella Revolution” in 2014, the government blocked communication over the mobile internet (Figure 5). Their intention was to block the coordination between the protestors and scale down their activity. The protestors continued their communication and coordination over FireChat messenger service, a decentralized network service [10].

While many people are assuming that the Dark Web is an unnecessary part of the internet, filed with evil and threats, the examples above

show that its existence is truly needed. The good side of the Dark Web represents an essential weapon in the fight for freedom and democracy.

The evil side of the Dark Web

On the other hand, the Dark Web infrastructure has its own evil side. This network became a space for various criminal activities and odd behavior online. The added anonymity brought out the worst in the people's behaviors, represented by the creation of markets that are selling illegal items and services.

The Dark Web as an "island of lawlessness" [11] became part of the cyber space where criminal activities are spreading and advancing. At the beginning, the criminal activities were focused in different dark forums where hackers and criminals were exchanging tools and ideas about how to commit fraud to make money. Later, this evolved into the creation of special marketplaces (Dream Market, Wallstreet Market) for selling drugs, fake ID documents, weapons, credit cards and different services, such as financial frauds, DDoS services, renting hackers and even renting hitmen (Figure 6).

Dream Market
Ichudifyeqm4ldjj.onion
 Established 2013

Shop Messages: 0 n0rm0ne

Bitcoin (BTC) 0.00

0

Logout

Browse by category

- Drugs 85160
 - Barbiturates 50
 - Benzos 4199
 - Cannabis 28049
 - Dissociatives 3113
 - Ecstasy 10973
 - Opioids 5550
 - Prescription 5282
 - Psychedelics 6352
 - RCs 690
 - Steroids 3875
 - Stimulants 13448
 - Weight loss 179
- Digital Goods 63039
- Drugs 85160
- Drugs Paraphernalia 465
- Services 6094
- Other 8300

Exchange

BTC	1.0
mBTC	1000.0
BCH	28.6
USD	3691.3
EUR	3252.7
GBP	2924.2
CAD	4983.1

Drugs (85178)

Filter

Ships to Ships from Escrow Category Cryptocurrency

Price - Searchtext Sort by Vendor

Apply filter

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 ... 2653 2654 2655 2656 2657 2658 2659 2660 2661 2662

TIP JAR

B0.001084
 Mrpunctual (340) (4.87★)
 US → US

ESCROW

Order

1,5gr Pure Amfetamine Speed Sulfate!

B0.00879
 HeroMeister (1) (5.00★)
 EU → EU

ESCROW

Order

100G COCAINE

B1.598
 JonSnow (520) (4.93★)
 DE → DE, EU

ESCROW

Order

1G 90% PURE FLAKE COLOMBIAN COCAINE [SUPER HQ]

B0.0284
 Supermalt2 (50) (4.91★)
 GB → EU

ESCROW

Order

Figure 6: The front page of Dark Web Market place on 20th January 2019.

Partial blame for the evolution of these marketplaces can be attributed to the introduction of digital cryptocurrency, Bitcoin, to the world. Bitcoin is an unregulated currency with the technical capability to be anonymously exchanged between different people on the Dark Web [12]. The bitcoin ledger is available to the public, so all transactions are public, but the accounts are not linked to any person on the web.

Nowadays, the Dark Web evil side is not only a black marketplace, it also became the cyber space where sexual and sadistic predators found their own ground. These predators use hidden web forums to exchange videos and images of their victims so that later they can blackmail them into carrying out depraved sexual and physical acts. The trial in 2018 of convicted British citizen Matthew Falder, a former post-doctoral researcher in geophysics at the University of Birmingham, has clearly shown the cruelty and effects of these behaviors [13]. Faced

with blackmailing from this predator, at least three traumatized victims attempted to take their own lives.

This evil side of the Dark Web is very popular among the cybercriminal communities but is condemned in the law enforcement agencies and the public over the internet. Numerous governments and international organizations are actively engaged in efforts to identify and apprehend criminals and predators who operate behind the veil of anonymity on the Dark Web.

The occurrence of the Dark Web on the world stage became a counterbalance to the Clearnet, as in everyday life, where many other aspects always have their own opposite side. The technology revolution will always bring new and innovative ways to improve people's lives, but almost always, it will bring an opposite effect or side effect to the community where we live. These opposite or even side effects may not always be good and in correlation with human development. That is why the new findings must perceive the benefits to the communities and attempt to predict the evil aspects to the same community.

REFERENCES

[1] Andrew L. Shapiro , Richard C. Leone, (1999) *The Control Revolution: How the Internet is Putting Individuals in Charge and Changing the World We Know*, Perseus Books, Cambridge, MA.

[2] Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W. & Rivest, R. L. (2015). Keys under doormats: mandating insecurity by requiring government access to all data and communications. *Journal of Cybersecurity*, 1(1), 69-79.

[3] Geoffrey A. Fowler (2018). What if we paid for Facebook — instead of letting it spy on us for free? URL: https://www.washingtonpost.com/news/the-switch/wp/2018/04/05/what-if-we-paid-for-facebook-instead-of-letting-it-spy-on-us-for-free/?noredirect=on&utm_term=.e57df468f3f6 / Accessed on 13.08.2023.

- [4] Greenwald, G. (2014). No place to hide: Edward Snowden, the NSA, and the US surveillance state. Macmillan.
- [5] Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 election. *Journal of Economic Perspectives*, 31(2), 211-36.
- [6] Erlandsson, F., Boldt, M., & Johnson, H. (2012, September). Privacy threats related to user profiling in online social networks. In *Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Conference on Social Computing (SocialCom)* (pp. 838-842). IEEE.
- [7] Tor: Overview, URL: <https://www.torproject.org/about/overview.html.en> / Accessed on 13.08.2023.
- [8] Voorhoof, D. (2005). The protection of journalistic sources under fire? Ghent University.
- [9] Ingmar Zahorsky, (01 August 2011). Tor, Anonymity, and the Arab Spring: An Interview with Jacob Appelbaum, The Peace and Conflict Monitor – University for Peace, URL: <https://ideasforpeace.org/content/tor-anonymity-and-the-arab-spring-an-interview-with-jacob-appelbaum/> Accessed on 13.08.2023.
- [10] Bland, A. F. (2014). The messaging app that's powering the Hong Kong protests. *The Guardian*, URL: <https://www.theguardian.com/world/2014/sep/29/firechat-messaging-app-powering-hong-kong-protests> / Accessed on 13.08.2023.
- [11] Wendorf D., Plass-Fleßenkämper B. (August 2018). Redeeming the darknet in five examples. Goethe-Institut. URL: <https://www.goethe.de/ins/nz/en/kul/mag/21343933.html>, Accessed on 13.08.2023.
- [12] Grinberg, R. (2012). Bitcoin: An innovative alternative digital currency. *Hastings Sci. & Tech. LJ*, 4, 159.
- [13] Davies C. (19 February 2018). 'Sadistic' paedophile Matthew Falder jailed for 32 years. *The Guardian*, URL: <https://www.theguardian.com/>

technology/2018/feb/19/dark-web-paedophile-matthew-falder-jailed-for-32-years, Accessed on 13.08.2023.