Ransomware Vulnerabilities During a Pandemic

Marco Querido a22002877

Lusófona University, Porto, Portugal
a22002877@mso365.ulp.pt

Abstract. With the growth of the covid-19 pandemic, the number of people browsing the internet rose drastically, giving them new ways to interact with each other or buy their favorite products, but that increase in activity lead to the increase of data flowing through the web, and consequentially the rise of online scams and cybercrime. Criminals and burglars around the world had a new market of potential victims to extort through existing methods, some of which are as easy as using external computer hardware.
This paper's goal is to give the reader an introduction on the main threats in IT security during the pandemic and their consequences to the people and the businesses. Secondly it'll specify about a case of ransomware, how it can start and analyze the spread of this type of malware throughout the world, comparing with earlier year's studies. Finally, it'll focus on the actual state of Portugal compared with Europe and the rest of the world by approaching some known security flaws and correction measures, fears, and ways to prevent worse case scenarios.

Keywords: malware, virus, phishing, hacker, ransomware, threats.

1 Introduction

The daily increase in covid-19 cases around the world has led many governments to take drastic measures to reduce the number of infections, such as the mandatory household lockdown. Deprived of physical social contact and frequent shopping trips, people started to interact with each other through social networks and other platforms, started working remotely and some even started shopping online. They also used some of their personal data in different contexts, from filling in forms for registration on digital platforms, accessing bank account management websites with credentials or even storing sensitive documents on their personal computers. Whenever people submit data, there is a responsibility on the part of who will keep this data, but also who fills it in, depending on confidentiality and access to it. [1]

All these changes have brough a new way of life, however associated threats arise, which jeopardize technological equipment and even human life. In the following chapters, the main threats felt this year in Europe and in 2020 in Portugal will be presented, talking specifically about one of these threats and presenting statistical data, as well as a practical case of an attack with an external device and finally presenting statistical data on cybersecurity in Portugal, comparing with other European countries, as well as ways of preventing and correcting security errors.

2 Main threats in IT during the pandemic

2.1 Major threats in Europe

The immense ocean that is the digital world is full of good and malicious users, the latter being a danger for those who do not dominate the internet. With the increase of fish in the ocean at the start of the pandemic, the number of potential targets for hackers increased, as many of the new users are largely very young children taking online classes, some of them using a computer for the first time, maybe their parent's computer due to digital inexperience and immaturity in having a personal computer. This technological innocence does not only apply to children, but to anyone without the slightest proximity to a computer and whoever has no notion of basic measures on how to safely browse the internet. Hackers can exploit this in simple ways or more elaborate ones, always using existing methods.

According to [2], the threat groups mentioned in the tables below had a greater impact at the European level during the pandemic:

Table 1. Prime threat groups identified by the ENISA Threat Landscape 2021 [2]

Name	Definition
Ransomware	A type of malicious attack where attackers encrypt a computer's or organization's data and demand payment to restore access.
Malware	Software or firmware intended to perform an unauthorized process that affects a system's confidentiality, integrity, or availability.
Cryptojacking	A type of cybercrime where a criminal secretly uses a victim's computing power to generate cryptocurrency.

Table 2. Prime threat groups identified by the ENISA Threat Landscape 2021 (continuation) [2]

Name	Definition
E-mail related threats	Threats that exploit weaknesses in the human psyche and in everyday habits, rather than technical vulnerabilities in information systems.
Threats against data	Encompasses data breaches/leaks. A data breach or data leak is the release of sensitive, confidential, or protected data to an untrusted environment.
Disinformation - misinformation	Spurred by the increased use of social media platforms and online media, as well as a result of the increase of people's online presence due to the COVID-19 pandemic, these threats are frequently used in hybrid attacks to reduce the overall perception of trust, a major proponent of cybersecurity.
Non-malicious threats	Threats where malicious intent is not apparent, mostly based on human errors and system misconfigurations, but they can also refer to physical disasters that target IT infrastructures.

These threat categories include threats and types of attacks that exist and are also referred to in the published document. As the main objective of hackers is monetary extortion, it is natural that there is a predominance of attacks with this objective, such as attacks by ransomware or phishing (in the sense of stealing personal data for money extortion), as well as data breaches. With the growth of cryptocurrency, there is also a trend towards the production of this currency through cryptojacking (using the victim's computing power to generate cryptocurrency). There was also a preponderance of DDoS (Distributed Denial of Service) attacks, and with the growth of new technologies a new branch of attacks of this nature, linked to ransomware, RDoS (Ransom Denial of Service).

2.2 Major threats in Portugal

In Portugal, the National Cybersecurity Center (CNCS) reports the following threats as being 5 of the threats with the most incidents registered in 2020:

- Phishing/Smishing;
- Malware infections;
- Malware distribution;

- Unprivileged account commitment;
- Unauthorized access.

The peaks represented in the graph in fig. 1 may be related to the months of greatest social isolation decreed during that year. The relevance of these threats is explained by fears about the pandemic and the effects it had on the population, who, prevented from leaving their homes during periods of social isolation, started to carry out more transactions through online services, being more vulnerable to malware attacks and phishing. [3]

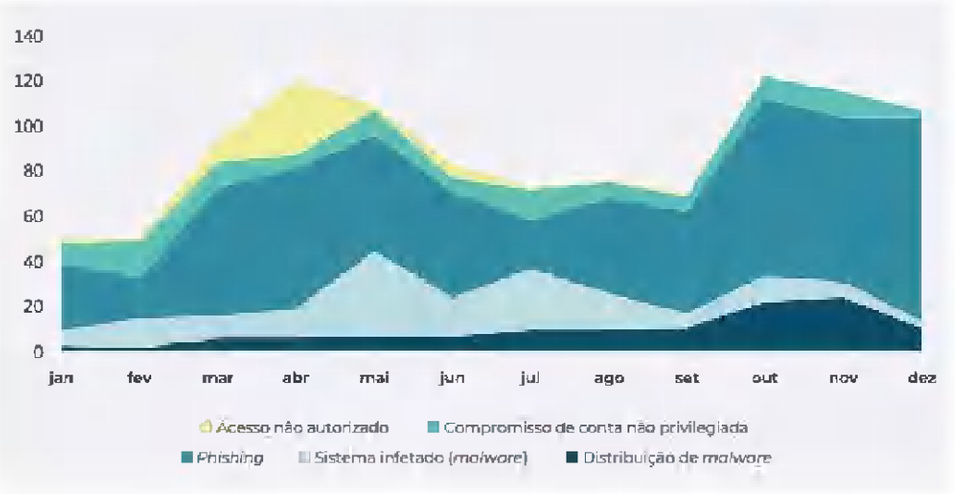

Fig. 1. Incidents by type recorded by CERT.pt,2020 (C/V)-Top 5, by month [3]

Phishing/Smishing are types of attacks that use a combination of social engineering and deception to persuade the victims into revealing personal and sensitive data like credentials, addresses or credit card details. The attack usually takes the form of spam mail, malicious websites, email messages, or instant messages (Smishing), appearing to be from a legitimate source such as a bank, or a social network. The attackers often use scare tactics or urgent requests to entice recipients to respond, and these fraudulent messages are usually not personalized and may share similar generic properties. [4]
Account compromise attacks are carried out using password databases available online and/or using brute-force mechanisms. [5]

These threats can have effects on people and companies, such as permanent loss of sensitive data, financial losses in the order of thousands of euros, loss of computer equipment, technological damage, psychological damage, etc.

3 Ransomware

With the increase of people browsing the internet, it is inevitable that there will be an increase in computer attacks, because for the less experienced in the area, just a click on a wrong link is enough to download a software that we think is legitimate and execute it, just to see all the information on our computer compromised due to a ransomware program.

3.1 Definition and case studies

Ransomware is simply a type of malware, used for illicit purposes, with the aim of encrypting all the information on a computer's hard drive, with the victim being coerced into paying a ransom (hence the name) to see this information decrypted. Usually, the victim is intimidated and put under pressure by a false countdown which, when finished, allegedly will erase all the data on the computer, which further motivates the victim to make the payment, often made in bitcoin or another type of cryptocurrency.

Malicious software can appear on a victim's computer by (and more often) downloading files from unsafe or dubious websites whose link was wrongly clicked and acts as soon as it is executed. This type of malware can have a significant impact depending on the amount of data on the attacked computer and the owner of the computer, and for a student, for example, it may not have such a big impact, while for a company it could mean the loss of thousands of euros.

A study by CERT [6] shows that from 2019 to 2021 and observing data for the first half of each year, there has been an increase in the record of incidents, with a total of 378 incidents being identified in 2019, 689 in 2020 and 847 in 2021. The greater number of incidents in the months of April 2020 and February 2021 lead to greater social confinement, possibly associated with greater proximity to technological means.

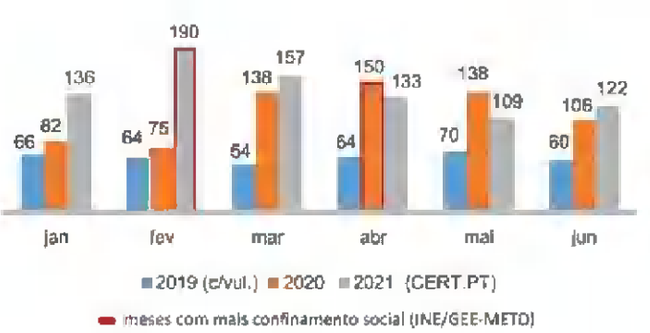

Fig. 2. Number of incidents registered by CERT.PT, on the first semester of 2019, 2020 and 2021, and peaks of social confinement [6]

Looking at information about ransomware attacks, Blackfog collected data from monthly ransomware attacks that occurred this year all over the world, compared it to data collected in 2020 and noticed that from January to August there was always an increase trend in attacks, while which from September to November decreased. If we add up all the attacks from both years and compare, we can conclude that between 2020 and 2021 the number of attacks increased from 250 to 259. A case very close to Portugal, collected by the company for the study is that of Spain, which in March saw the SEPE (Servicio Publico de Empleo Estatal) affected by a distributed ransomware attack. [7]

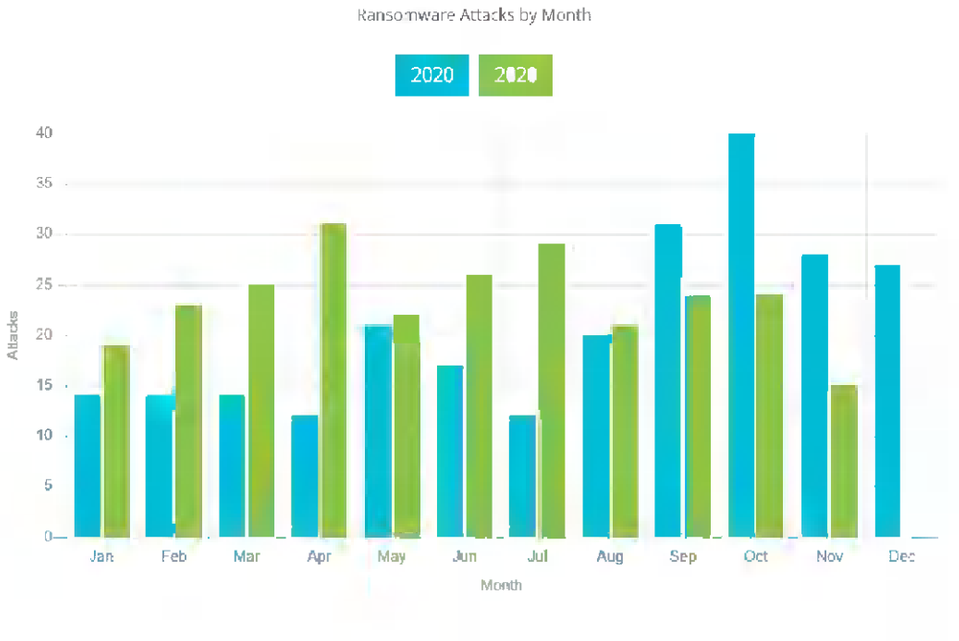

Fig. 3. Ransomware attacks by month [7]

An attack of this nature can be carried out inside a company by an employee who has unknowingly downloaded ransomware masquerading as a legitimate program, or if the employee has malicious intents, they may deliberately spread the ransomware across the company's network.

3.2 Practical Example

Having physical access to the computer, the employee can, using a usb rubber ducky, download the malware. The rubber ducky is a device in the form of a usb pen,

recognized by the system as an external keyboard, being immediately accepted, and which runs automatic scripts written via keyboard keystrokes, in the form of payloads. [8] This allows those who have rubber duckies to run all sorts of scripts. In the case of ransomware, we can create a script that disables the Windows native anti-virus through administrator privileges and then download the malware from an online repository and run it. [9]

```
#!/bin/bash
#
# Title:         Disable D3f3nd3r (Rubber Ducky)
# Description:   This Payload disables Windows Defender using Powershell, Works also for the Hak5
#                Rubber Ducky or any HID device that supports Quacking.
# Author:        REDD of Private-Locker
# Version:       1.0
# Category:      Disable Security
# Target:        Windows
#
# Source:        https://gist.githubusercontent.com/PrivateLocker/6711c4fe88eae75774284bd6efc377dc/raw/30c9a50a3dd
#

Q WIN R
Q STRING "powershell -NoP -NonI -W Hidden -Exec Bypass -c \"Start-Process cmd -A '/t:4f'-Verb runAs\""
Q LEFTARROW;
Q ENTER;
Q STRING "powershell -ExecutionPolicy Bypass -c \"IEX (New-Object Net.WebClient).DownloadString('https://gist.githu
Q ENTER;
sleep 1;
Q STRING "exit";
Q ENTER;
```

Fig. 4. Windows Defender deactivation payload [10]

The code shown in fig. 4 is an example of a script that can be created in ducky script language that allows you to carry out part of what was previously said, seen and discussed for educational purposes only. A second piece of code would fetch the software from an online repository and run it on the computer. [10]

4 Portugal compared to the world

In recent years cases of cyber-attacks have been reported through the media around the world. One of the loudest names in 2017 was WannaCry, a ransomware that affected several British hospitals and paralyzed the country's healthcare services for hours. [11] The aim of the attack would possibly be just extortion of money through malware, but another way of attacking could involve, for example, life support medical equipment,

putting the lives of patients at risk [12]. But it wasn't just the UK that felt the damage from the virus.

4.1 Ransomware cases in Portugal

According to [13] the company Anubisnetworks estimates that in Portugal 12,000 computers were infected with WannaCry, data provided by those responsible for stopping the virus. Most computers would be connected to the area of telecommunications and the internet, which makes sense as those are areas with a high number of electronic devices.

A recent case of ransomware attack, according to the ENISA Threat Landscape, in April 2020 was the company EDP, threatened with exposure of 10TB of personal data and company financial information by hacker group Ragnarok, which demanded 10.9 million dollars (corresponding to 9.5 million euros) for the data not to be exposed. [14].

To understand the panorama of Portugal compared to other European countries, a study was carried out by ESET to classify European countries with the best cybersecurity. 24 countries were specifically approached, one of them being Portugal. Each country was rated with a score on different factors, such as the percentage of malicious software discovered on devices in the last three years, the percentage of victims of identity theft in the last three years, or even the commitment to cybersecurity. In the end, after combining all the factors, each country is assigned a result from 0 to 10, which says how safe it is in case of an attack, and this result is called the European Cybersecurity Index. As of June 2021, Portugal is ranked 1st in Europe in terms of cybersecurity, with an index of 8.21 in the ranking. This ranking portrays the work of national entities in cooperation with international organizations for the prevention and combat of cybercrime, as well as the results of the implementation of legislation, measures, and techniques for the prevention of cybercrime in the country. [15]

9

1	Portugal	42	0.758	11%	3%	2%	1%	5	8.21
2	Lithuania	60	0.908	23%	6%	2%	1%	4	7.99
3	Slovakia	62	0.729	17%	5%	3%	3%	3	7.21
4	Greece	59	0.527	18%	5%	1%	2%	4	7.03
5	Spain	21	0.896	20%	5%	4%	5%	4	6.82
6	Estonia	63	0.905	32%	14%	4%	4%	5	6.75
7	Latvia	61	0.748	25%	13%	3%	6%	4	6.20
8	Finland	22	0.856	34%	9%	6%	3%	5	6.09
9	Denmark	34	0.852	31%	9%	11%	2%	5	6.08
10	Slovenia	68	0.701	32%	9%	4%	4%	3	6.05
11	Italy	51	0.837	23%	10%	8%	8%	4	5.93
12	Germany	9	0.849	37%	10%	5%	6%	7	5.89
13	Poland	15	0.815	23%	7%	6%	6%	4	5.87
14	Croatia	55	0.84	26%	12%	9%	10%	5	5.66
15	Hungary	56	0.812	24%	12%	10%	12%	6	5.61

Fig. 5. European cybersecurity score, according to different factors (top 15 countries) [15]

Within the scope of this paper, a small survey was carried out among 160 people in Portugal, with the aim of understanding technological habits and internet care during confinement by respondents. [16] The first two questions aim to collect the biographical data of the respondents, with 63.1% being female and 36.9% male, mostly in the range from 45 to 54 years old (26.2%), followed by the range from 18 to 24 years old (23.8%) and from 35 to 44 years old (22.5%). The survey was divided into two sections, the first one that aims to collect data on the digital habits of respondents, whose data show some aspects like the large majority, 83,1%, feeling a greater need for a computer or a mobile device to carry out everyday activities, or on average 47,5% of the respondents spent more than 6 hours a day using that equipment. Combining this last percentage with the fact that more than 75% of respondents have a personal computer or mobile device, used to work, or use social networks, proves a prolonged daily use of technologies and the internet, increasing exposure to threats already talked about. To understand the degree of exposure of respondents to certain threats, the second section focuses on questions that try to understand the use of simple security measures, such as the use or not of the same password for more than one user account, to which 68.1% responded that

they share some between accounts. 46.3% of respondents also answered that they never change the passwords they use. These two factors together allow us to deduce that if a data breach occurs, users will be more vulnerable to attacks by login attempts if the platforms do not incorporate two-factor authentication. Another example focuses on whether they use an ad blocker or not, to which more than half of respondents said they do not use it, and only 28.1% pay attention to hyperlinks on websites. Combined, these factors demonstrate that there is a high risk of users being exposed to malware, more specifically adware. One aspect of the study to highlight is that 60% of respondents regularly update the software on their devices.

4.2 Corrective and prevention measures

There are vulnerabilities that can be corrected, by each one of us, to reduce as much as possible the risk of computer attacks, with preventive measures that can be adopted for that. ENISA [17] presents on its website tips for users to ensure some online security for remote work, some of which are:

- Using company computers, where possible. As far as possible do not mix work and leisure on the same device;
- Connect to the internet via secure networks, avoid open/free networks;
- Avoid the exchange of sensitive company information through possibly insecure connections;
- As far as possible use corporate Intranet resources to share working files;
- Pay attention to emails about the pandemic, as they may be phishing attempts or scams;
- Data at rest should be encrypted;
- Antivirus / Antimalware should be installed and updated;
- The system needs to be updated regularly;
- Locking the computer screen if working in a shared space;
- Do not share the virtual meeting URL's on social media or other public channels.

5 Conclusion

There was a growing trend and a greater preference for attacks aimed at extorting money from companies and individuals, with hackers using already existing methods, but also more sophisticated and technologically advanced methods.
Malware and ransomware are among the most evident threats in recent years and today, ransomware being a cryptographic method that puts heavy pressure on victims to pay the ransom. This method is relatively simple to perform within a company, by a malicious employee, using external devices such as a usb pen or a usb rubber ducky.

There has been a growth at a European level in the register of incidents about cyber-threats over the last few years, especially this year, when many companies opted for teleworking and saw their working methods changed. However, we can prove through the study referred to in the previous chapter that Portugal is considered the country with the best European ranking in terms of cybersecurity, in relation to other European countries, and having a small local notion through the survey also mentioned.

As a future continuation of this paper, a study could be made to forecast the continuation of trend growth or an unexpected decrease in threats for the next year, in Europe and the rest of the world, as well as the influence of the appreciation or depreciation of certain cryptocurrencies in cyber-attacks.

References

1. Fernandes, L., "Data Security and Privacy in Times of Pandemic", (2021).
2. ENISA, ENISA Threat Landscape, pp. 9-11, (2021).
3. Centro Nacional de CiberSegurança, https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriocibersegurança-cncs.pdf, pp 33-34, last accessed 2021/12/16
4. ENISA, https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/phishing-spear-phishing, last accessed 2021/12/16
5. Centro Nacional de CiberSegurança, https://www.cncs.gov.pt/pt/relatorio-riscos-conflitos-2020-ameacas-prospetivas/, last accessed 2021/12/16
6. Boletim Observatório de Cibersegurança, https://www.cncs.gov.pt/docs/boletim-observatorio-setembro2021-1.pdf, last accessed 2021/12/03.
7. Blackfog, https://www.blackfog.com/the-state-of-ransomware-in-2021/, last accessed 2021/12/03.
8. Hack5, https://hak5.org/products/usb-rubber-ducky-deluxe, last accessed 2021/12/04.
9. NullByte, https://null-byte.wonderhowto.com/how-to/use-usb-rubber-ducky-disable-antivirus-software-install-ransomware-0180418/, last accessed 2021/12/04.
10. REDD, https://forums.hak5.org/topic/50868-payload-disabled3f3nd3r/, last visited 2021/12/04.
11. Russell Brandom, https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin, last visited 2021/12/04.
12. Moreira, A., "The Benefits and Risks of Privacy and Security in the Era of Digital Health: Health National Service (SNS) of Portugal", (2019).
13. Visao, https://visao.sapo.pt/exameinformatica/noticias-ei/internet/2017-05-15-wannacry-12-mil-computadores-infetados-em-portugal/, last visited 2021/12/07
14. ENISA, ENISA Threat Landscape, pp. 98-99, (2021).
15. ESET, https://www.eset.com/uk/about/newsroom/blog/european-cybersecurity-index-2021/, last accessed 2021/12/10.
16. Google Forms, https://docs.google.com/forms/d/1fWYUjBmGVArzA62LylT5bwcZqpdIQnc06oc7O8yvJb8/edit#responses, last accessed 2021/12/09
17. ENISA, https://www.enisa.europa.eu/tips-for-cybersecurity-when-working-from-home, last accessed 2021/12/07

References

1. Mwila, K. (2018, August). *The Deep Web*. Research Gate. Retrieved December 13, 2021, from https://www.researchgate.net/publication/335336010_The_Deep_Web
2. Varma, C. (2018, April 19). *CISO Guide: Surface Web, Deep Web and Dark Web - Are they different?* CISO Platform. Retrieved December 10, 2021, from https://www.cisoplatform.com/profiles/blogs/surface-web-deep-web-and-dark-web-are-they-different
3. Varma, C. (2018, April 19). *CISO Guide: Surface Web, Deep Web and Dark Web - Are they different?* CISO Platform. Retrieved December 10, 2021, from https://www.cisoplatform.com/profiles/blogs/surface-web-deep-web-and-dark-web-are-they-different
4. Finklea, K. (2017, March 10). *Dark Web*. Congressional Research Service. Retrieved December 10, 2021, from https://a51.nl/sites/default/files/pdf/R44101%20(1).pdf
5. Varma, C. (2018, April 19). *CISO Guide: Surface Web, Deep Web and Dark Web - Are they different?* CISO Platform. Retrieved December 10, 2021, from https://www.cisoplatform.com/profiles/blogs/surface-web-deep-web-and-dark-web-are-they-different
6. Finklea, K. (2017, March 10). *Dark Web*. Congressional Research Service. Retrieved December 10, 2021, from https://a51.nl/sites/default/files/pdf/R44101%20(1).pdf
7. Varma, C. (2018, April 19). *CISO Guide: Surface Web, Deep Web and Dark Web - Are they different?* CISO Platform. Retrieved December 10, 2021, from https://www.cisoplatform.com/profiles/blogs/surface-web-deep-web-and-dark-web-are-they-different
8. Finklea, K. (2017, March 10). *Dark Web*. Congressional Research Service. Retrieved December 10, 2021, from https://a51.nl/sites/default/files/pdf/R44101%20(1).pdf
9. Varma, C. (2018, April 19). *CISO Guide: Surface Web, Deep Web and Dark Web - Are they different?* CISO Platform. Retrieved December 10, 2021, from https://www.cisoplatform.com/profiles/blogs/surface-web-deep-web-and-dark-web-are-they-different
10. Finklea, K. (2017, March 10). *Dark Web*. Congressional Research Service. Retrieved December 10, 2021, from https://a51.nl/sites/default/files/pdf/R44101%20(1).pdf
11. Gehl, R. (2014, October 15). *Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network* [Graph]. Sage Journals. https://journals.sagepub.com/doi/full/10.1177/1461444814554900
12. Buxton, J., & Bingham, T. (2015, January). *The Rise and Challenge of Dark Net Drug Markets*. Global Drug Policy Observatory. Retrieved December 10, 2021, from https://core.ac.uk/download/pdf/34722885.pdf
13. Branwen, G. (2011, July 11). *Silk Road 1: Theory & Practice*. Gwern.Net. Retrieved December 10, 2021, from https://www.gwern.net/Silk-Road
14. Branwen, G. (2011, July 11). *Silk Road 1: Theory & Practice*. Gwern.Net. Retrieved December 10, 2021, from https://www.gwern.net/Silk-Road
15. Love, D. (2013, March 6). *There's A Secret Internet For Drug Dealers, Assassins, And Pedophiles* [Photograph]. Insider. https://www.businessinsider.com/tor-silk-road-deep-web-2013-3
16. Urquhart, A. (2016, November). *The Inefficiency of Bitcoin*. https://eprints.soton.ac.uk/400597/1/Bitcoin%2520efficiency%2520R%2526R.docx
17. Chen, H. (2011). Dark Web: Exploring and Data Mining the Dark Side of the Web (Integrated Series in Information Systems, 30) (2012th ed.). Springer.
18. Chertoff, M. (2017). A public policy perspective of the Dark Web. *Journal of Cyber Policy*, *2*(1), 26–38. https://doi.org/10.1080/23738871.2017.1298643
19. Jardine, E. (2015). *The Dark Web Dilemma: Tor, Anonymity and Online Policing*. Elsevier BV. https://doi.org/10.2139/ssrn.2667711