Ransomware Vulnerabilities during a Pandemic

Carlos Garcia

Lusófona University, Porto - Portugal
a21901121@ mso365.ulp.pt

Abstract. Nowadays, our days are marked by the appearance of the coronavirus (covid-19), which has led the world health organization to decree a global pandemic. With this situation, several measures have been implemented to prevent the spread of the virus as much as possible.
These days, the concerns of organizations increased considerably because most of them were not prepared for this situation, and many of them had to make changes in the network to continue working and at the same time earn money, thus making their network more vulnerable to ransomware attacks.
Ransomware Vulnerabilities are concerns that all organizations should worry about because all can suffer attacks at any time. With the current pandemic situation, for hackers it is a great opportunity to attack weaker organizations, doing damage and profiting from the information obtained.
This paper will describe an introduction to the main threats in the area of IT security that occurred during the pandemic in general. This paper will also show whether or not there has been growth, during this time of the pandemic.

Keywords: Ransomware, Pandemic, Vulnerabilities, Covid-19, attacks.

1 Introduction

The security of an organization is only as strong as its weakest component. [1]

On March 11, 2020 [2] the world health organization had to declare a global pandemic state. Given the exponential growth of the virus, several countries have had to take certain measures to combat this sharp growth, which include the closure of countries, cities, and curfew measures.

With this new reality, organizations and people had to adapt to all these new measures taken quickly to be able to continue working. Given the speed of both organizations and people adapting, it has become easier for hackers to find more vulnerabilities and at the same time, new opportunities have arisen for them to attack more easily. All of this leads one to think that security is a rather important topic that is often forgotten until it is too late. So, the message must be shared with everyone, so that organizations and people can get the information they are missing as soon as possible.

In this paper, initially, the first chapter will analyze the main threats in the area of computer security that occurred during the pandemic in a general way with a brief definition of them. Also, the same chapter will analyze Ransomware Vulnerabilities during the covid-19 Pandemic with some examples of attacks during the pandemic.

After this chapter, we will focus specifically on Portugal, making a comparison before and during the pandemic showing some research results, which give us the idea of the state of ransomware in this country, showing some preventions and measures to be taken for future attacks.

2 Most common cyberthreats during the covid-19 pandemic

Since we have heard the word cybersecurity, it has had several definitions for it [4] being in constant evolution over time, but according to the author [5] cybersecurity is the prevention of damage caused by unauthorized use of hackers of electronic information and communication systems and their information that is stored, with the aim of ensuring confidentiality, integrity and availability.

Confidentiality means limiting access to and sharing the information in the system. Integrity means protecting the information from being altered or destroyed. Availability means keeping the system online for those who have access to it and unavailable for those who do not have access or have not logged into the system.

So, it is up to the engineers to try to keep everything secure and at the same time away from hackers.

Currently, there are 3 types of threats to cybersecurity, intentional, non-intentional and natural. Intentional attacks are considered the most serious since they are the result of malicious actions by other people involved. Non-intentional attacks are usually linked to all kinds of attacks caused by, for example, failing to protect certain equipment or even cutting a cable that is connected to something important. Natural attacks are all attacks where the human being is not directly involved, for example, earthquakes and tsunamis. [6] [24]

2.1 Prime Threats during covid-19 pandemic

Before the world was confronted by covid-19 there were already several cybersecurity challenges, because as time goes by technology changes and at the same time everything changes. Hackers need to adapt to new realities as well as engineers try to find ways to be more effective in less time and with more security.

With the emergence of covid-19, everything became more difficult as organizations and people had to come up with quick solutions to keep working.

According to ENISA [7], there are 8 main threats during the period April 2020 - July 2021

The 8 top threats during the reporting period
1. Ransomware
2. Malware
3. Cryptojacking
4. E-mail related threats
5. Threats against data
6. Threats against availability and integrity
7. Disinformation – misinformation
8. Non-malicious threats

Table 1. Most frequent crime based on the registration of denunciations to the Office Cybercrime, of the PGR, 2020 [15]

A brief explanation of the most common cyber threats

- Ransomware - encrypting files on an infected computer and holding the key to decrypt the files until the victim pays a ransom. During the period mentioned, this was the main threat. [3]
- Malware - software that is intended to perform an unauthorized process to install something like spyware, ransomware, virus, worms, which could lead to serious consequences [9]. It has always been considered among the threats with the highest risk, but lately, according to ENISA [7], it has gradually dropped.
- Cryptojacking - emerged in mid-September 2017, its function is to use a victim's computer components to mine virtual currency. [10]
- Threats against availability and integrity - DDoS (Distributed Denial of Service) is one of the most critical threats to IT systems. It aims to overload the system and cause it to shut down or reboot. [11]
- E-mail related threats – most common techniques used to attack e-mails include identity theft, phishing, virus and spam e-mails. [12]
- Threats against data - exposure to secret data can lead to manipulation, threats, defamation and ransomware. [7]
- Disinformation - misinformation - both aim at sharing false information with the goal of harming or even influencing in a negative way. [13]
- Non-malicious threats - most often it is human error that leads to the leak of important data by simple negligence and without malware or other external actions. [14]

2.2 Ransomware Vulnerabilities during covid-19 Pandemic

What exactly is ransomware? According to the authors [16], ransomware is a malicious attack in which attackers encrypt the data of an organization or person and demand a payment in exchange for returning the stolen data. In some circumstances, the attackers when stealing the information may ask in exchange for not disclosing the information to authorities, competitors, or the public.

One of the currently most demanded payment methods is cryptocurrency because of its enhanced anonymity and the indistinguishability of transactions. [7]

The average ransom amount doubled over the last year, though small amounts of ransom are still popular with threat actors. They tend to be paid more easily and result in less public exposure for the threat actor. The higher demands also increased. Over just a few months, the highest demand made in 2020 more than doubled in 2021. [7]

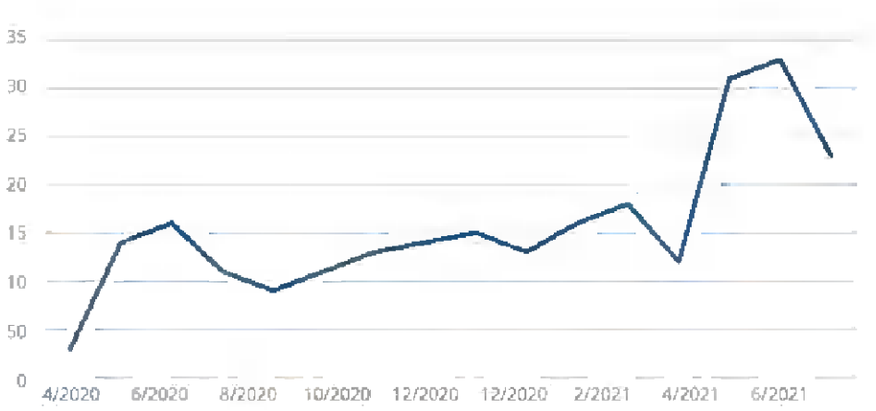

Fig. 1. Ransomware incidents observed by ENISA (April 2020-July 2021) [7]

By analyzing the chart, we can see that since the beginning of the pandemic there has been an increase in ransomware cases.

It is a mistake to assume that a specific industry is singled out and targeted by ransomware actors. Ransomware actors are indifferent to who pays them as long as they are getting paid. The distribution of industries is more a function of the median level of cyber resilience of the organizations and companies in that industry and the availability of cost effective methods to compromise them. [23]

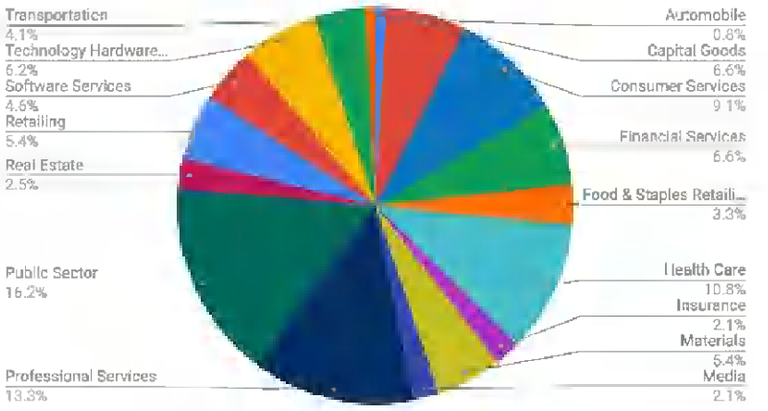

Fig. 2. Common Industries Targeted by Ransomware in Q2 2021 [23]

By analyzing the sector chart, we can see that the public sector suffers the most ransomware attacks followed by professional services.

During the time of the pandemic there were several ransomware attacks:

- In London, March 2020, the Maze ransomware group leaked the personal and medical data of thousands of former patients of a medical research company about covid-19 testing. [20]
- On June 1 2020, the University of California San Francisco (UCSF) working on the covid-19 vaccine fell victim to a ransomware attack in which it was forced to pay €995 thousand to cybercriminals called Netwalker.21. [19]
- In June 2020, in Canada, CryCryptor ransomware masquerades as COVID-19 contact tracking apps on Android devices. [21]
- In July 2021 in Spain, the fourth largest telecommunications company, MasMovil, fell victim to theft of customer information by the REvil ransomware group. [7]

3 A focus on Portugal before and during the covid-19 pandemic

According to Microsoft [17] [22] in March 2017 in Portugal malware was found on 8.3% of computers in Portugal, with Trojans identified on over 7.0%.

The same study also says that in March 2017 Portugal had a high percentage of 73% of computers with security software enabled. Also, in the same study, we can see that ransomware is well below when compared to the other.

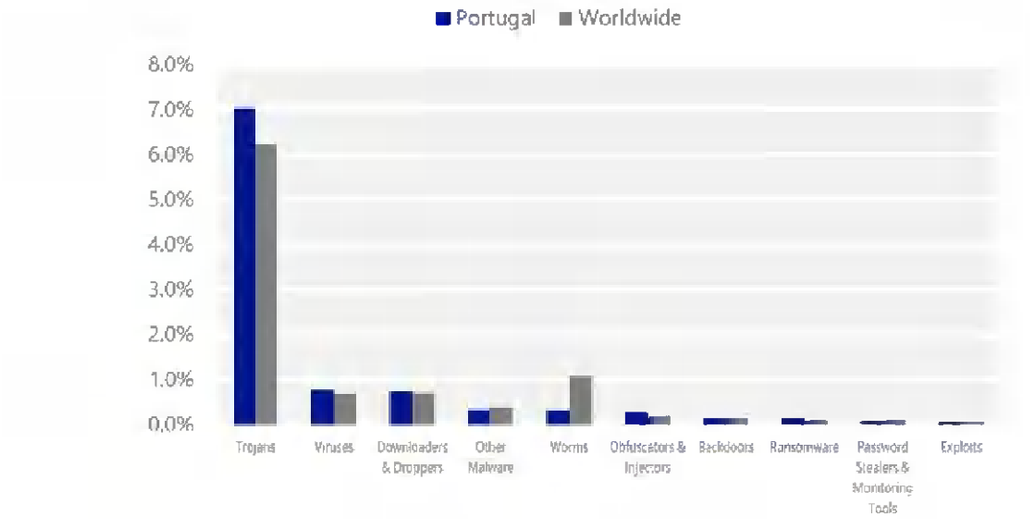

Fig. 3. Percentage of malware in the amount of analyzed Computers in Portugal as of March 2017 [17] [22]

6

The same document also shows that in the European Union (EU), Portugal was in 3rd place in the number of major cybercrime victims among EU countries.

	% OF POPULATION WHO HAVE EXPERIENCED CYBERCRIME	ANNUAL AVERAGE MALWARE ENCOUNTER RATE	CYBERCRIME VICTIMHOOD RATING
1. ROMANIA	18%	28%	23%
2. NETHERLANDS	27%	14%	21%
3. PORTUGAL	15%	24%	20%
4. POLAND	16%	23%	20%
5. ITALY	17%	21%	19%

Fig. 4. Top victims of cybercrime among EU countries [17] [22]

According to the data provided in the CNCS 2021 risk and conflict report [8], we can see that the most frequent crime was fraud in the use of the MBWAY payment application, followed by phishing and ransomware. Also, CNCS counts with the cooperation of different enterprises like NATO, ENISA, the European Commission, and others. It also partners with the project "No More Ransom", that vouches to stop criminal activities connected to Ransomware. [22]

1º Fraud in the use of the MBWAY payment application
2º Phishing
3º Ransomware
4º CEO fraud
5º Online scams
6º Scams with relationships and with cryptocurrencies
7º Scams with fake web pages
8º Private data and image sharing
9º Stalking e sextortion
10º Hate speech
11º Copyright infringement

Table 2. Most frequent crime based on the registration of denunciations to the Office Cybercrime, of the PGR, 2020 [8]

During this time of the pandemic, the energy company EDP in April 2020, was the victim of a ransomware attack in which the Ragnarok group demanded €9.5 million where it threatened data disclosure. The same group also threatened to release 10TB of information containing private customer and financial information. [7]

Proposals for preventing ransomware attacks, according to ENISA: [7]

- Implementation of secure and redundant backup strategies;
- Implementation and auditing of identity and access management (least-privilege and separation of duties);
- Training and raising the awareness of users (including privileged users);
- Separation of development and production environments;
- Information sharing on incidents with authorities and the industry;
- Restricting access to known ransomware sites;
- Identities and credentials should be issued, managed, verified, revoked, and audited for authorized devices, users, and processes;
- Access permissions and authorizations should be managed, incorporating the principles of least privilege and separation of duties;
- Use of security products or services that block access to known ransomware sites;
- Report any attack or attempted attack to the authorities and help restrict its spread;
- Systems' monitoring for fast identification of infections;
- Ransomware response and recovery plans should be tested periodically to ensure that risk and response assumptions and processes are current with respect to the evolving ransomware threats;
- Keeping up with recent ransomware trends, developments and proposals for prevention.

4 Conclusion

In the last decade, technology has evolved dramatically, and in order to be constantly updated, we need to search for secure and at the same time fast information. Given this exponential evolution and the difficulty of adapting to new technologies, engineers and hackers are in a constant battle, some solving problems and solutions, others looking for weaknesses where they can act to steal data and make money with it.

With the emergence of the pandemic and the new measures imposed by governments, the solutions had to be done quickly without much worry, which damaged the security of companies and people, and at the same time, the hackers used this to their advantage.

So, when this is over, it is important to carry out as many studies as possible on the whole situation, thus making it possible to improve the actions to be taken in case there is another event with the same dimension.

Safety comes first!

References

1. Contch, N.; Royer, M, "The Rise in Cybercrime and the Dynamics of Exploiting the Human Vulnerability Factor", International Journal of Computer (IJC), Volume 20, Number 1 (2016).

2. Declaration of pandemic situation by WHO, https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020, last accessed 13/11/2021.
3. "What is Ransomware? A Guide to the Global Cyberattack´s Scary Method", https://www.wired.com/2017/05/hacker-lexicon-guide-ransomware-scary-hack-thats-risc/ , last accessed 2021/11/29.
4. Nicole M Tucker, "Cybersecurity: Deciding the Effectiveness of the U.S.Comprehensive Initiative, pp.1-2 (2015).
5. Cavalcanti, C., "Cyberdefense: Challenges and comparative legislation between Brazil and Portugal", p.6 (2017).
6. Jore, S.H. "The Conceptual and Scientific Demarcation of Security in Contrast to Safety", pp.2-5 (2019).
7. ENISA Threat Landscape 2021, October 2021. From April 2020 - July 2021.
8. "Relatório Risco e Conflitos 2021", https://www.cnes.gov.pt/pt/observatorio/#relatorios (2021), Last Access 2021/12/01.
9. "What are the Most Common Cyberattacks?", Cisco Security, Retrieved From: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html#~how-cyber-attacks-work, Last Access 2021/12/01.
10. "What is Cryptojacking? Prevention and Detection Tips", Varonis, Retrieved From: https://www.varonis.com/blog/cryptojacking/, Last Access 2021/12/03.
11. "Types of Cybercrime", Panda Security Mediacenter, Retrieved From: https://www.pandasecurity.com/en/mediacenter/panda-security/types-of-cybercrime/, Last Access 2021/12/04.
12. "Types of email attacks and the damage they can cause", CloudSecureTech, Retrieved From: https://www.cloudsecuretech.com/types-of-email-attacks-and-the-damage-they-can-cause/, Last Access 2021/12/04.
13. "Digital misinformation/disinformation and children", UNICEF, Retrieved From: https://www.unicef.org/globalinsight/stories/digital-misinformation-disinformation-and-children, Last Access 2021/12/07.
14. "Unintentional Insider Threats: The Non-Malicious Within", Software Engineering Institute, Retrieved From: https://insights.sei.cmu.edu/blog/unintentional-insider-threats-the-non-malicious-within/, Last Access 2021/12/07.
15. "Threat Landscape", ENSINA, Retrieved From: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends?tab=details, Last Access: 2021/12/09.
16. B, Willian C., S, Karen., F, William., S, Murugiah., "Cybersecurity Framework Profile for Ransomware Risk Management", NIST Preliminary Draft NISTIR 8374, pp. 1-2 (2021).
17. Barros, G., "A Cibersegurança em Portugal", Temas Económicos, Number 56, Gabinete de Estratégia e Estudos, Ministério da Economia, pp. 5-6 (2018).
18. "Vulnerabilities and Exploits", ENISA, Retrieved From: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/vulnerabilities-and-exploits, Last Access 2021/12/09.
19. "How hackers extorted $1.14m from University of California, San Francisco", https://www.bbc.com/news/technology-53214783, Last Access 2021/12/09
20. "Cyber gangsters hit UK medical firm poised for work on coronavirus with Maze ransomware attack", https://www.computerweekly.com/news/252480425/Cyber-gangsters-hit-UK-medical-research-lorganisation-poised-for-work-on-Coronavirus, Last Access 2021/12/09
21. "New ransomware masquerades as covid-19 contact-tracing app on you Android device", https://www.zdnet.com/article/new-crycryptor-ransomware-masquerades-as-covid-19-contact-tracing-app-on-your-device/, Lass Access 2021/12/09

22. Silva, J., “Cybersecurity and Cybercrimes in Portugal”, Digital Privacy and Security Conference, pp.6-7 (2019)
23. “Q2 Ransom Payment Amounts Decline as Ransomware becomes a National Security Priority”, https://www.coveware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-national-security-priority, Last Access 2021/12/15
24. Pinto, D., “Portugal cyberthreats Review: Targeted Health institution”, Digital Privacy and Security Conference, pp.2 (2020)