UNIVERSITAT POLITÈCNICA DE VALÈNCIA

etsinf

Escola Tècnica Superior d'Enginyeria Informàtica

Escola Tècnica Superior d'Enginyeria Informàtica
Universitat Politècnica de València

Analysis, evaluation, measurements and implementation of network security systems and their critical points of failure during COVID-19

TREBALL FI DE GRAU

Grau en Enginyeria Informàtica

Autor: Adrián Olmedilla Belinchón

Tutor: Teresa del Montecarmelo Nachiondo Farinós

Curs 2022-2023

KTH ROYAL INSTITUTE
OF TECHNOLOGY

Degree Project in Information technology

First cycle, 15 credits

Analysis, evaluation, measurements and implementation of network security systems and their critical points of failure during COVID-19

ADRIÁN OLMEDILLA BELINCHÓN

Stockholm, Sweden, 2023

Analysis, evaluation, measurements and implementation of network security systems and their critical points of failure during COVID-19

ADRIÁN OLMEDILLA BELINCHÓN

Date: June 22, 2023

Supervisors: Hongyu Jin, Teresa del Montecarmelo Nachiondo Farinós
Examiner: Panagiotis Papadimitratos
School of Electrical Engineering and Computer Science
Swedish title: Analys, utvärdering, mätningar och implementering av nätverkssäkerhetssystem och deras kritiska felpunkter under COVID-19

Abstract

This study analyses the evolution of the COVID-19 pandemic from a cybersecurity perspective, highlighting the different types of cyber-attacks experienced that happened around the world. In addition, this thesis shows the different types of cyber-attacks produced due to the lack of security employed during the pandemic crisis and how were the reactions of the different organizations to solving the problem. Furthermore, there are different statistics and graphical tables that show the evolution and how it covered the main types of cyber-attacks by the majority of organizations. The analysis reveals a view of those different attacks that can show in various forms. How the cybercriminals leverage the different vulnerabilities of corporate networks in a never-explored perspective makes this review different from other present papers on the COVID-19 pandemic. In addition, the study manifests the different recommendations proposed by the different experts to avoid a similar situation in times of crisis, making that study a guide to avoid similar situations in the future. In fact, the information extracted from different specialized sources will be used to carry out an objective study.

Keywords

COVID-19, Cyber-attack, Internet security, Cybersecurity threats, Remote Work, Cybersecurity Awareness

Sammanfattning

Den här studien analyserar utvecklingen av covid-19-pandemin ur ett cybersäkerhetsperspektiv, och lyfter fram de olika typer av cyberattacker som upplevts runt om i världen. Dessutom visar denna avhandling de olika typerna av cyberattacker som skapats på grund av bristen på säkerhet som användes under pandemikrisen och hur de olika organisationerna reagerade på att lösa problemet. Dessutom finns det olika statistik och grafiska tabeller som visar utvecklingen och hur den täckte huvudtyperna av cyberattacker från majoriteten av organisationer. Analysen visar en syn på de olika attackerna som kan visa sig i olika former. Hur cyberbrottslingarna utnyttjar de olika sårbarheterna i företagsnätverk i ett aldrig utforskat perspektiv gör att denna recension skiljer sig från andra nuvarande artiklar om covid-19-pandemin. Dessutom visar studien de olika rekommendationerna som föreslagits av de olika experterna för att undvika en liknande situation i kristider, vilket gör den studien till en guide för att undvika liknande situationer i framtiden. Faktum är att informationen från olika specialiserade källor kommer att användas för att genomföra en objektiv studie.

Nyckelord

COVID-19, cyber-attack, Internetsäkerhet, Cybersäkerhetshot, Fjärrarbete, Cybersäkerhetsmedvetenhet

Resumen

Este estudio analiza la evolución de la pandemia de COVID-19 desde una perspectiva de ciberseguridad, destacando los diferentes tipos de ciberataques experimentados en todo el mundo. Además, esta tesis muestra los diferentes tipos de ciberataques producidos por la falta de seguridad empleada durante la crisis de la pandemia y cómo fueron las reacciones de las diferentes organizaciones ante la solución del problema. Además, existen diferentes estadísticas y tablas gráficas que muestran la evolución y cómo se cubrieron los principales tipos de ciberataques por parte de la mayoría de las organizaciones. El análisis revela una visión de esos diferentes ataques que pueden manifestarse de diversas formas. La forma en que los ciberdelincuentes aprovechan las diferentes vulnerabilidades de las redes corporativas en una perspectiva nunca explorada hace que esta revisión sea diferente de otros documentos actuales sobre la pandemia de COVID-19. Además, el estudio pone de manifiesto las diferentes recomendaciones propuestas por los diferentes expertos para evitar una situación similar en tiempos de crisis, convirtiendo dicho estudio en una guía para evitar situaciones similares en el futuro. De hecho, se utilizará la información extraída de diferentes fuentes especializadas para realizar un estudio objetivo.

Palabras claves

COVID-19, Ataque cibernético, Seguridad en Internet, Amenazas a la seguridad cibernética, Trabajo remoto, Concienciación sobre seguridad cibernética

Acknowledgments

A special thank you to my examiner Panagiotis, you are the reason why I chose and encouraged me to do that topic in my thesis; the course that you taught was very interesting and educational for me. I would like to thank my Spanish supervisor Teresa because the course you taught me in Spain was the main reason I decided to study networks. Sorry and thank you Hongyu for all the work I created for you. Thank you for always being there, answering questions, and coming up with suggestions.

Stockholm, June 2023
Adrián Olmedilla Belinchón

Contents

List of Figures

List of Tables

List of acronyms and abbreviations

2FA	Two-Factor Authentication
AI	Artificial Intelligence
BEC	Business Email Compromise
CISA	Certified Information Systems Auditor
DDoS	Distributed Denial of Service
DMARC	Domain-based Message Authentication, Reporting and Conformance
DRDoS	Distributed Reflection Denial of Service
ENISA	European Union Agency for Cybersecurity
FBI	Federal Bureau of Investigation
FTC	Federal Trade Commission
GDPR	General Data Protection Regulation
ICT	Information and Communication Technology
IoT	Internet of Things
IT	Information Technology
MFA	Mult-Factor Authentication
ML	Machine Learning
NIST	National Institute of Standards and Technology
PPE	Personal protective equipment
RDP	Remote Desktop Protocol
VPN	Virtual Private Network
WHO	World Health Organization

Chapter 1

Introduction

The World Health Organization (WHO) declared COVID-19 as a pandemic on 11 March 2020. The pandemic that resulted from the spread of COVID-19 quickly became a new crisis resulting in the mass quarantine of millions of citizens across numerous countries around the world [1]. This situation made people have to get used to the "new normal", creating considerable uncertainty, anxiety, and a drastic change regarding our way of life. In addition, so many countries decided to close non-primary services, accordingly, the majority of companies and governments had to virtualize the different types of work, and many workers have to learn to use digital technologies. Many organizations had to revamp their offices and were afraid because the employees did not have the resources and time to train them on working from home[2]. Moreover, the organizations solved this problem, so migrating many operations and services online for remote work was inevitable. Information and Communication Technology (ICT) took a central role in each activity, so as COVID-19 spread worldwide it led to a relevant threat to a technology-driven society [3].

1.1 Background

This work focuses on the intersection between the COVID-19 pandemic and cybersecurity, particularly the different types of cyber threats and attacks that have emerged in this context. It delves into how these threats have exploited corporate network vulnerabilities and impacted organizations and individuals globally. The thesis highlights the various ways in which these threats have been addressed and mitigated and analyzes the broader implications they may have for the future of cybersecurity and crisis management. Drawing on insights and recommendations from experts in the field, this work provides

a comprehensive analysis of the issues at hand and potential solutions and strategies for preventing similar situations from arising in the future.

1.2 Problem

In the wake of the recent global crisis, the reliance on and usage of the internet has surged to unprecedented levels, increasing susceptibility to cybercrime and cyberattacks [4]. In addition, the crisis provided attackers worldwide a significant opportunity to carry out various malicious activities and cyberattacks for financial gain and to advance their evil demands. This situation created:

- Financial losses: Many people fell victim to various cyber scams [5].
- Increased anxiety and stress: Cyberattacks can be highly distressing, and the COVID-19 pandemic has already caused significant anxiety and stress for many people.
- Disruption of essential services: Cyberattacks on healthcare systems, and attacks on other critical infrastructures, can disrupt essential services and have potentially life-threatening consequences [5].
- Damage to reputation and trust: Cyberattacks can damage the reputation and trust of companies, organizations, and individuals.
- Difficulty in adapting to remote work: Many people had to adapt quickly to remote work due to the pandemic, and cyberattacks targeting remote workers made this transition even more challenging.

Cybersecurity safeguards computer systems and networks against harmful attacks by individuals or groups with malicious intent. These attacks can lead to the unauthorized disclosure of information, theft of hardware, software, or data, and damage to computer systems. In addition, cybersecurity helps to prevent disruptions and misdirection of the services provided by computer systems and networks. Organizations and individuals can better protect their digital assets by implementing cybersecurity measures.[6]. Then, how was the evolution of cybersecurity doing COVID-19? Were they enough? So the idea is to solve the evolution of the cybersecurity employed during that period and how it worked. Later in the thesis, it will appear different solutions explained by experts to avoid those situations.

1.3 Purpose

The purpose of exploring the evolution of the COVID-19 pandemic from the perspective of cybersecurity is to shed light on cybersecurity's critical role in ensuring the resilience of individuals and organizations in times of crisis. By analyzing the impact of the pandemic on the cyber threat landscape and the types of attacks that have emerged, you can identify the key challenges that individuals and organizations face in securing their digital assets. Additionally, you can examine the strategies and solutions developed by cybersecurity experts to mitigate the risks and ensure business continuity. This analysis can inform policymakers and stakeholders of the importance of cybersecurity in crisis management and provide valuable insights for future crises.

1.4 Goals

The goal of this thesis is to

1. help different organizations around the world avoid similar situations.
2. better understand what happened during the relationship between cybersecurity and the COVID-19 pandemic.
3. try to motivate readers to be interested in cybersecurity.

1.5 Research methodology

The research question that the thesis will follow throughout the course will be: What is the current situation after the improvements in cybersecurity on the network introduced after the COVID-19 confinement? The thesis aims to explain the evolution of the COVID-19 pandemic from the point of view of the ICT, explaining from the beginning the most common attacks that were produced and caused many organizations lost much money. In addition, the thesis will include different statistics that allow the reader to understand the importance of cyber-attacks in our society. Additionally, digital service has led organizations to significant investments in administrative and technical countermeasures to prevent malicious cybersecurity accidents, so the thesis shows the organizations' reaction to countermeasures, checking how good the response was and its effectiveness. The idea is to check if the response

of the measures where wrong or not to see how it is possible to improve them. Finally, the thesis will include recommendations that it will be necessary for governments and organizations to be resilient and innovative in cybersecurity to avoid the future effects of the pandemic or similar crisis from the cybersecurity perspective based on the opinion of the experts.

1.6 Delimitation

Limitations of this thesis include the inability to cover all types of cyberattacks and their corresponding mitigations due to the expansive nature of the topic. Additionally, it should be noted that this thesis is primarily research-based and will not delve into implementation aspects. The focus is on investigating the intersection of cybersecurity and the COVID-19 pandemic, providing insights and analysis rather than practical implementation guidelines.

1.7 Ethics, sustainability and societal impact

Cybercrime and cybersecurity are linked, giving rise to ethical considerations that have a societal impact [7]. Due to the pandemic, millions of workers have been forced to work online. However, new threats have emerged, leading governments to collect more personal data and information than ever before. These broader implications were intended to create a safer and more digital world that can be helpful during this period.

1.8 Structure of the thesis

The background will explain the evolution of the COVID-19 pandemic from the perspective of cybersecurity, including tracking the most relevant topics and examining the reactions to the attacks during COVID-19, as well as the speed of response. Chapter 3 will delve deeper into the types of attacks and Chapter 4 will discuss the different kinds of mitigations deployed. Finally, Chapter 5 will provide an overall conclusion and discuss future work.

Chapter 2

Evolution

This chapter provides the evolution of cybersecurity/cyberattacks during the COVID-19 pandemic. The background of the evolution is presented in Section 2.1. Section 2.2 provides an overview of the key cybersecurity concerns during the pandemic and Section 2.3 explains cyberattack responses. Finally, Section 2.4 debates future cybersecurity considerations, and section 2.5 summarizes the chapter.

2.1 Background

During times of crisis, it is common for an increase in cyberattacks. For instance, the war between Russia and Ukraine in 2022 resulted in cyber operations that provided benefits to Russia[8]. While the shift to a more digital world has brought many benefits, which has also created new opportunities for cybercriminals to exploit vulnerabilities and launch attacks. Cybercriminals use the COVID-19 crisis to steal passwords, data, or money directly [9].

The increase in the number of cyberattacks made many people's day-to-day lives more complicated. Cyber threats change, depending on users' behaviors and online trends to take advantage of them. The authors of these illegal activities have not left the occasion presented by the COVID-19 outbreak. These attacks include phishing scams, ransomware attacks, Distributed Denial of Service (DDoS) attacks, and other types of malware. The attacks have targeted various organizations, from hospitals and healthcare providers to government agencies and educational institutions [10].

The increasing number of cyberattacks is a growing concern in the digital age.

According to the data in the table below, reported cyberattacks have increased since 2016. In 2020, a total of 1872 data breaches were presenting a significant increase from the previous year [11].

S/n	Year	Compromises
1	2021	1,862
2	2020	1,872
3	2019	1,108
4	2018	1,175
5	2017	1,506
6	2016	1,088

Table 2.1: The trend of compromise between 2016 and 2021 (Table: fig. 2.1 in [11]).

In response to this surge in cyberattacks, governments and other organizations have implemented a variety of measures to strengthen their cybersecurity defenses. These include increased investment in cybersecurity infrastructure, improved training, and the development of new technologies to identify and prevent cyber threats.

A Cisco survey asking organizations to rank cybersecurity investment by importance during COVID-19 showed that the overall position of cybersecurity on defense, around 34% of the investment, including threat protection, risk assessment, and other defenses is the leading investment. In addition, it is the option chosen by 14 of the 21 markets surveyed [12].

Other priority investments highlighted by organizations include network access (24%), cloud security (22%), and user and device verification (20%). The percentages are general since it varies depending on the region. However, the classification is quite similar in the different areas. In figure 2.1, there is a table showing the results that were discussed before.

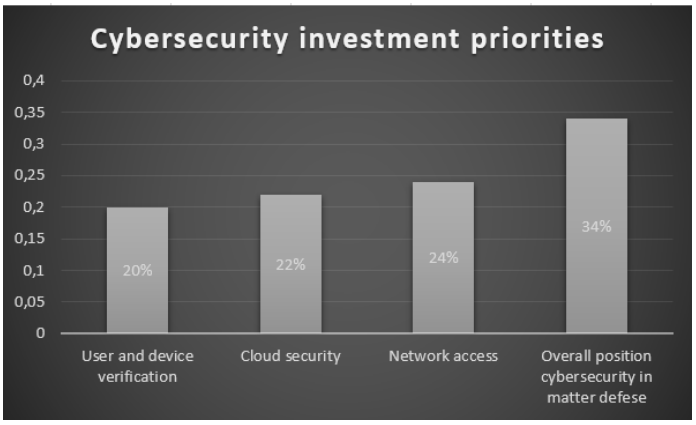

Figure 2.1: Distribution of organizational resources (Table: fig. 2.1 in [12]).

The COVID-19 pandemic has brought many challenges, however, it created chances to organizations to improve their security measures to avoid that types of problems again. In addition, organizations have been capable of reacting and protecting themselves and their users from cyberattacks. The following sections explore the various types of cyberattacks, the mitigation strategies implemented, and the solutions that experts in the field have proposed.

2.2 Key cybersecurity concerns during the pandemic

The evolution of technology has brought significant changes in our daily lives. From the power of the Internet that has enabled global communication to the efficiency and safety of transportation, access to food and healthcare, socialization, and productivity; Technology is essential today to live [13]. However, as we rely increasingly on technology, we also become increasingly vulnerable to cyberattacks.

In a pandemic crisis, it is crucial to prioritize public safety. However, we cannot ignore the possible privacy violation that may occur simultaneously [14]. Implementing social distancing and lockdown measures significantly changed people's daily routines, with remote work and e-learning becoming more prevalent. As a result, the internet has taken an increasingly important role in facilitating these activities [15].

The COVID-19 pandemic has forced many businesses, schools, and other organizations to transition to remote work and digital platforms at a rapid pace. While these changes have allowed for continued operations and some degree of normalcy, they have also opened up new opportunities for cyberattackers to exploit vulnerabilities in these new systems and networks. As a result, there has been a significant increase in cyberattacks as attackers look to take advantage of the pandemic and the accompanying surge in online activity.

During COVID-19, global organizations faced a substantial increase in cyber threats. Reports suggest that there has been an 81% rise in the number of organizations experiencing such threats. Moreover, during the peak season, a significant number of organizations, around 79% faced downtime due to cybersecurity risks [16]. Many sources have noted a substantial increase in the occurrence of scams and malware attacks since the beginning of the pandemic. Phishing attacks have increased to 667% since the end of February. Out of 467.825 spear-phishing email attacks about 9,116 of those detections were related to COVID-19 [17].

2.2.1 The timeline

During the pandemic period, there have been several types of cyberattacks. However, the main ones are:

- Phishing attacks: Phishing attacks have increased during the pandemic, with cyber criminals sending emails or text messages that appear to be from legitimate sources such as health organizations, banks, or government agencies.
- Malware attacks: Malware attacks have increased during the pandemic, with attacks using malware to steal sensitive data or gain access to systems.
- DDoS: DDoS attacks involve overwhelming a target system with traffic to take it offline. During the pandemic, DDoS attacks have been used to target online resources such as e-learning platforms and remote work tools.

These are just a few examples of the most common types of cyberattacks observed during the pandemic, as shown in Figure 2.2. It is important to note that the timeline is evolving and new types of attacks are emerging, so organizations need to adapt their strategies. In addition, these types of attacks

will be discussed in chapters 3 and 4.

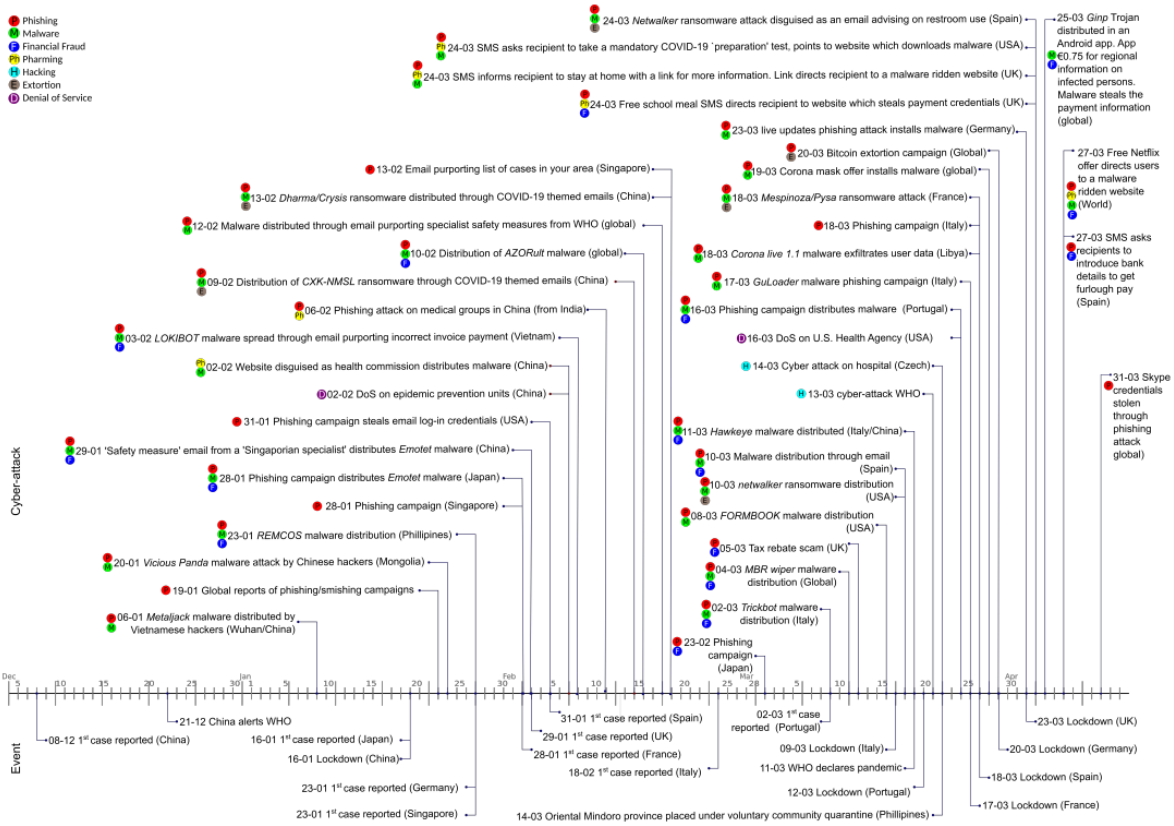

Figure 2.2: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic (Timeline: fig. 2.2 in [18]).

The timeline highlights several cyberattacks that have happened during the pandemic. One of the impressive attacks occurred on the 13th of March of 2020 when the WHO saw an increase in the number of cyberattacks directed at its staff [19].

On the 16 of March 2020, a DDoS attack was launched against the US Health Agency. The attackers were overwhelmed with millions of hits designed to slow or shut the page down. However, it was not successful. The attack did more than spread fear. Also, it showed the vulnerabilities of the health organizations that should improve to avoid similar situations [20].

These are some examples of the cyberattacks seen during the COVID-19 pandemic. As the pandemic continues, it is important to remain vigilant and take appropriate actions to safeguard sensitive information.

2.2.2 The impact of COVID-19 on the population's perception of cybersecurity

As governments worldwide have been working to contain the spread of COVID-19 and assist those affected by the pandemic, cybercriminals have been exploiting the situation by preying on people's anxiety [21].

Since the beginning of the COVID-19 pandemic, the general population is becoming more digitally connected. According to the McAfee survey, around 88% of Indian consumers feel that they are using more and more technology, and 86% have implemented more protection for their digital devices. [22]. To put it another way, almost half of the adults, specially 44%, now believe they are more susceptible to cybercrime than they were prior to the onset of the COVID-19 pandemic [23].

A good example of why there has been an increase in cases of awareness regarding cybersecurity is that 1 in 5 Norton consumers fell victim to a scam. As shown in Figure 2.3 of Norton consumers thought they were victims of scams.

As shown in the figure, most scams have fraudulent package notification links, 8%, usually, people click those links thinking they are legitimate links. However, it is a method to steal or control a computer. In addition, fake pages are another problem, they offer medical equipment or Personal protective equipment (PPE) that was different than advertised and never arrives or costs much more than the average market price.

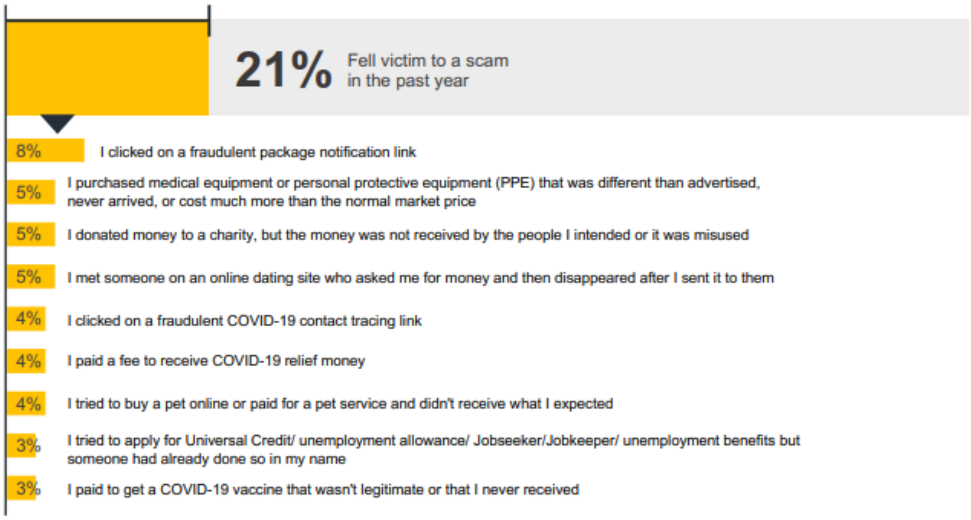

Figure 2.3: Scams Fallen Victim during COVID-19 Pandemic (Table: fig. 2.3 in [24]).

2.3 Response to the cyberattacks

Since the increment in cases of cyberattacks worldwide, governments and organizations have taken steps to protect themselves against these threats and minimize their impact.

For this reason, organizations must optimize cybersecurity measures to protect remote work environments and their digital resources [25]. This has involved not only updating existing security protocols but also developing new ones specifically tailored to the challenges of the pandemic. In many cases, the speed of digital evolution was faster than the adaptability of organizations [25].

In this section, we will explore how governments and organizations responded to cyberattacks during the pandemic, developing new policies, collaboration, information sharing, and adopting of technologies and training programs. While the landscape continues to evolve, these responses represent essential steps to a more secure digital future.

2.3.1 Government response

In today's society, the reliance on digital connectivity is more prevalent than ever before. Most people cannot imagine going without the Internet for even a

few hours. It is estimated that every second, approximately, 127 new devices are connected to the internet worldwide. Despite this, the risk of cyberattacks continues to rise, making governments create new measures to combat them. cybercrime [26].

One of the main responses from governments has been the increase in the funding for cybersecurity initiatives. For example, the Congress of the EEUU includes $650 million for Certified Information Systems Auditor (CISA)'s cybersecurity risk management programs [27]. Similarly, European Union Agency for Cybersecurity (ENISA) has had its budget increased yearly to nearly 22 million euros in 2020, five times more than it is initial budget [28]. This funding has been used to establish standard criteria and unify the national mechanism to award cybersecurity certification and conducts threat hunting and other response after an intrusion has been identified [28].

Another response from the government has been to establish cybersecurity regulations. As an illustration, the UK government launched a cybersecurity advisory report to disrupt or prevent malicious COVID-19-themed cyber activities [29]. The European Union also released a new framework for governance, management, and control of risks in the field of cybersecurity [30]. Furthermore, governments have also introduced legislation to enhance cybersecurity and protect against cybercrime. The South African government passed an Act (Act19 of 2020) to combat cyber threats [31].

Governments have also collaborated with international organizations, as it was previously mentioned, and other countries to address the cyber threat landscape. Countries such as the US, UK, Canada, Australia, and New Zealand formed the Five Eyes Alliance which monitors the electronic communications of citizens and foreign governments to prevent cyber threats [32].

Despite these measures, there are still concerns about the effectiveness of government responses to cyberattacks during the pandemic. For example, Americans reported 152,129 cases of coronavirus-related fraud, costing the population more than $97.39 million [33]. In addition, millions of employees had to work remotely, which created security breaches. Furthermore, there are concerns about the potential for government surveillance and privacy violations in the name of cybersecurity [34].

2.3.2 Company response

Companies have accelerated reliance on the technology of their customer and supply-chain interaction of their internal operations [35]. Due to the COVID-19 pandemic, companies have acknowledged using more resources for their digital initiatives. This has responded to the increased demand for remote working capabilities and digital services, and the risk of cyberattacks [35].

However, a recent study shows that many companies are still unable to afford an Information Technology (IT) disaster recovery plan the evident increase in IT funding, despite the evident rise in IT funding, as can be seen in the table. The table reveals that only 39% are capable of having a prepared and implemented plan, while 23% are working on the plan. On the other hand, the rest of the companies can't invest in the plan for different reasons. Specifically, 9% cited the lack of time, and 11% cited the lack of skill and 18% cited that they do not need a plan, perhaps because they assume they would not be the target of a cyberattack [36].

Plan and Reason	Percentage
Do not use a plan due to the lack of time to prepare it	9%
Do not use a plan due to the lack of internal skills to prepare it	11%
Do not use a plan because the companies do not need this kind of plan as we can respond on ad ad-hoc basis	18%
Has a plan that is implemented and prepared	39%
Working on a plan	23%

Table 2.2: IT disaster recovery plan.

A good example can be seen in a survey conducted by Kaspersky, 73% of employees were working from home and did not receive any cybersecurity training when they started working remotely[37]. In addition, part of the employees received malicious attacks [37].

One of the keys that the security and IT teams have been working on is on providing secure remote access to resources, apps, and data [38]. In consequence, companies had to increase their security measures. In a survey

conducted to identify the top security investment made during the pandemic, the most common response among companies was the implementation of Mult-Factor Authentication (MFA) which according to figure 2.4 has the highest investment rate, 20%. However, as you can see in the figure below, the survey depends on the different countries in which it is conducted (the survey was conducted in India (IN), Germany (DE), the United Kingdom (UK), and the United States (USA).

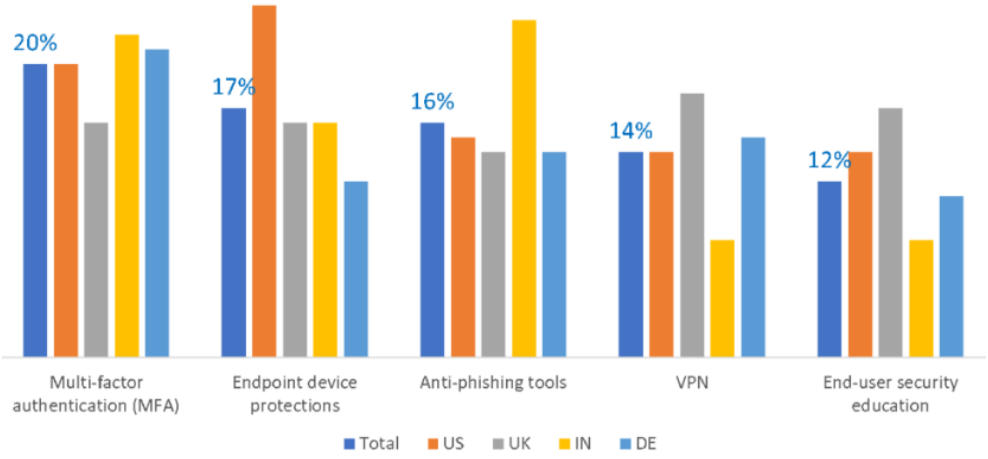

Figure 2.4: Top 5 cybersecurity Investments Since the Beginning of the Pandemic (Graphic: fig. 2.4 in [38]).

Another typical response to cyber threats is endpoint device protection which represents 17% of the investment of the companies as shown in Figure 2.4. These tools include firewalls, intrusion detection and prevention systems, and vulnerability scanners. However, while these tools can help companies, they are not foolproof.

Companies also rely on anti-phishing tools. During the pandemic, there has been a surge in phishing attacks that aim to trick people into taking sensitive information [39]. To counter this, companies have implemented anti-phishing tools. Anti-phishing tools consist of computer programs that attempt to identify phishing content [40]. According to a survey, one of the anti-phishing tools had an accuracy rate of over 90%, but it also had a false positive rate of 42%, because many anti-phishing browser tools only block websites that appear on a blacklist and take no further consideration[41].

Due to the pandemic, there has been a significant surge in Internet traffic, increasing up to 90% [42]. The technology adapted to access the Enterprises Intranet is Virtual Private Network (VPN), used by the majority of the companies (17% of the investment of companies in cybersecurity). A VPN connection hides the data online and protects it from outside access[43]. So far, 479 vulnerabilities have been revealed and public. Only the Top 28 vulnerabilities were y identified and exposed during 2020 [42]. However, it has some vulnerabilities because VPN cannot always be ”trusted” due to which companies are affected by a large number of data breaches around the globe [42].

Finally, the end-user security education will be explained in much more detail in subsection 2.3.3. Additionally, the evolution of cybersecurity to protect businesses against cybercriminals is increasing defenses against threats. However, as the threat continues to evolve, it will be critical to adapt to new challenges.

2.3.3 Individual response

A different response against cyberattacks is an individual response. Technology has evolved but has also increased the risk of cybercrimes. Cybersecurity is no longer just a concern for governments and companies.

A study made by Norton showed that 2 in 3 adults say that they are spending more time online than ever before, with a similar proportion saying they have taken more precautions online because of cybercrime concerns [24]. 74% of adults thought that remote work has made it much easier for hackers to take advantage of people and 62% found it difficult to determine if online information is from a credible source [24]. As a result, victims spent almost 7 hours resolving issues, and 47% were impacted financially [24].

Percentage	Ways to protect against online activities and Personal Information
48%	Made some or all of my passwords stronger
38%	Limited information shared on social media
29%	Used online parental controls on children's account or devices
27%	Stopped using public Wi-Fi
25%	Read the Terms & Conditions in full before installing or downloading a device or service
22%	Changed default privacy settings or devices
22%	Enabled multi-factor authentication
21%	Disabled third-party cookies in a browser
20%	Used an identity theft protection service
19%	Used something other than my full name for social media profiles
13%	Used a VPN to encrypt information sent to and from my devices
12%	Used anonymous payment methods
11%	Deleted a social media account
11%	Used a privacy monitoring service to find and remove my personal information online
11%	Used an encrypted email service
5%	Asked a company to see what personal information they have about me in their customer records
3%	Other
18%	I have not done nothing

Table 2.3: Steps done by the population to protect their online privacy (Global total) (Table: fig. 2.3 in [24]).

As shown in Table 2.3, Norton revealed that most people globally have taken steps to protect their online privacy. However, despite these efforts, cybercrime remains a significant concern, with 18% of the respondents reporting that they have not done anything. Additionally, part of the respondents had deployed solutions discussed in subsection 2.3.2, such as VPN (13%), MFA (22%).

As depicted in Table 2.3, the population has increased it is protection against cyberattacks due to fear and advice. This situation generates an increase in the methods that the population uses to protect themselves. Around 98% of the population takes reactive steps after detecting unauthorized access.

The evolution of individual response to cybersecurity has also been influenced by new technologies such as Artificial Intelligence (AI) and the Internet of Things (IoT) [44] [45]. A study made by McKinsey found that 56% of all

respondents report AI adoption in at least one function, up from 50% in 2020 [46]. However, technology brings some risks and threats that need to be treated by different organizations to solve them.

2.4 Future cybersecurity consideration

Cybersecurity has always been dynamic, with new threats emerging. In addition, businesses are constantly investing in the latest technologies to run their businesses [47]. A recent made by McKinsey has shown, over the next three to five years, the three major cybersecurity trends will have significant implications for organizations [47].

2.4.1 The availability of data and information platforms that can be accessed on-demand

The increase in the population using technology is growing. This situation has created concern among experts, believing that the 60% of professionals in the financial sector want to ensure the security of the cloud [48]. Additionally, the marketplace for web-hosting services is expected to generate $183.18 billion by 2026 [47].

Cloud computing is the latest trend in distributed systems evolution, with its predecessor being the grid. Unlike traditional systems, cloud infrastructure is abstracted from the user, requiring no specialized knowledge or expertise [49]. As public cloud adoption continues accelerating, the cloud will be a concern. A survey made by Flexera shows that 90% of respondents who answered a question about COVID-19 expect cloud use to exceed plans due to the pandemic [50]. As seen in the image below, the use of the cloud has skyrocketed. Therefore, it is necessary to increase the cybersecurity of these systems, since when they are on the rise, vulnerabilities arise.

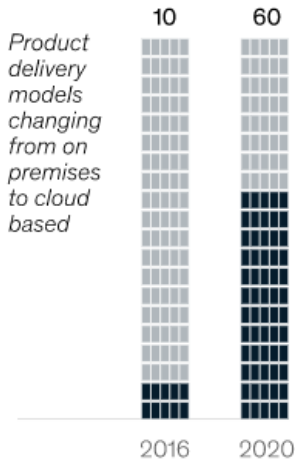

Figure 2.5: Security products delivered via the cloud, % of the total (Graphic: fig. 2.5 in [47]).

2.4.2 Emergence of sophisticated cyberattacks leveraging the new technologies

Hackers increasingly use advanced technologies such as AI and Machine Learning (ML) to launch more sophisticated and effective cyberattacks. These technologies allow hackers to identify opportunities to access sensitive data, vulnerable applications, devices, and networks to scale their social engineering attacks [51].

2.4.3 Regulatory landscape and resource shortages

A growing number of organizations face a shortage of cybersecurity talent and expertise. The demand for cybersecurity professionals has increased with the rapid proliferation of digital technologies, but many companies have struggled to keep up with the pace of change [47]. As a result, companies are finding it challenging to identify and manage digital risks. Cyber risk management has not evolved at the same pace as digital transformations, leading to a growing gap between cybersecurity capabilities and the risks that organizations face.

2.5 Summary

In conclusion, as the world becomes increasingly digitized, the importance of cybersecurity continues to grow. Going forward, cybersecurity will need to adapt to an evolving threat landscape. To respond to these threats, organizations must prioritize cybersecurity and invest in creating a cybersecurity posture that includes risk management strategies, enhanced detection and response capabilities, and a well-trained, educated workforce.

The COVID-19 pandemic has highlighted the need for organizations to be resilient and adaptable to new and unforeseen challenges. Key cybersecurity concerns during the pandemic include the rapid shift to remote work, increased reliance on cloud services, and the rise of pandemic-themed cyberattacks. Moving forward, organizations must continue to prioritize cybersecurity and build resilient infrastructures that can withstand unexpected challenges.

In general, COVID-19 has significantly impacted cybersecurity, making organizations aware of the new change they must adapt to. As the world becomes more connected and dependent on digital technologies, there is a need to ensure that digital data and systems.

Chapter 3

Types of cyberattacks during the pandemic

The chapter aims to provide an overview of the various types of cyberattacks that have become more prevalent during the COVID-19 pandemic. It aims to increase awareness of the threats individuals and organizations face in the current environment. This chapter deals with the main types of cyberattacks seen in Figure 2.2, phishing attacks in section 3.1, malware attacks in section 3.2, DDoS attacks in section 3.3 and the summary in section 3.4.

3.1 Phishing attack

Since the beginning of the COVID-19 pandemic, different organizations have suffered from cyberattacks, generating costs worldwide, costing companies $110B for protecting against cyberattacks [52]. However, investigations by Federal Bureau of Investigation (FBI) in the US estimated the cost of phishing attacks $1.8B in 2020, up from $1.7B in 2019 [52]. Recent cyberattacks have become more sophisticated, requiring advanced detection techniques to match the pace of attackers.

3.1.1 Definition

Phishing is an act of fraud where attackers attempt to acquire sensitive data such as login credentials, credit card numbers, and other personal information by posing as a trustworthy entity [53]. By masquerading as a reputable source with an enticing request to trick them into divulging sensitive information [53].

Figure 3.1 is a good example of a phishing attack where the attacker sends an email to the victim who will be redirected to a similar page or similar page to a verified web page to enter personal data.

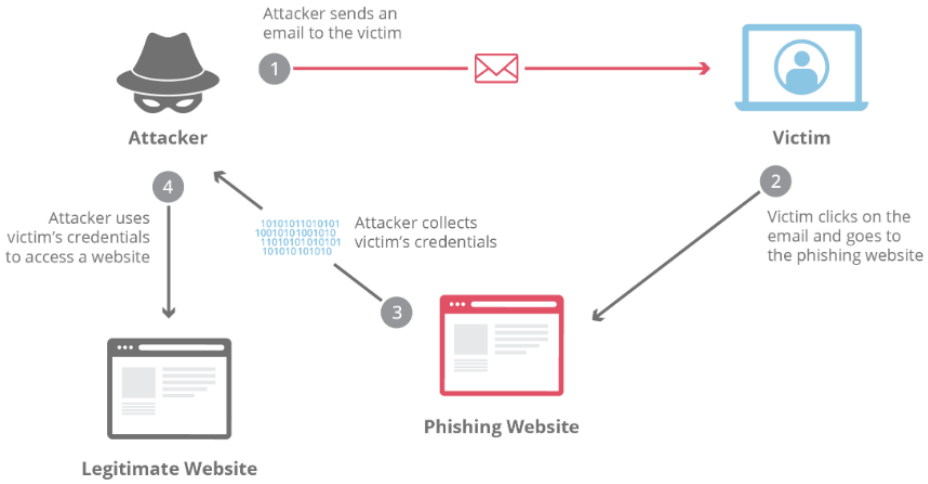

Figure 3.1: Phishing attack example (Scheme: fig. 3.1 in [53]).

3.1.2 Tactics

During the COVID-19 pandemic, phishing attacks were the most carried out, representing 59% of all cyberattacks during the pandemic, according to Interpol [54]. For example, a survey conducted by Barracuda Networks found an increase in phishing attacks in the region of 600% in March 2020 concerning the previous month [55].

The analysis below shows that phishing has common tactics when carrying out these cyberattacks. Among these, we can see those shown in the following subsections.

3.1.2.1 Spoofed emails and websites

Spoofed emails and websites are a common tactic used in cyberattacks, particularly in phishing attacks. Email spoofing tricks users into thinking a message came from a person or entity they either know or can trust and website spoofing is the same, however instead of forging an email, they simulate a real

website [56].

The most common technique used in spoofed emails and websites was the use of domain impersonation [52]. During the COVID-19 pandemic, phishing attacks involved impersonating government organizations, the WHO, the US Centre for Disease Control and Prevention... [52]. In March 2020, a statistical report published by Palo Alto researchers revealed that a significant number of new domain titles and registrations related to COVID-19 were created, totaling 116,357 since the beginning of the pandemic. The report showed that out of all these domains, 2% were found to be clearly malicious, while 34% were categorized as high-risk [52].

3.1.2.2 Social engineering

Social engineering refers to all techniques aimed at talking a target into revealing specific information or performing a specific action for illegitimate reasons [57]. Although it can be confused with fake emails and websites, they cannot be considered the same, since social engineering consists of psychological manipulation while spoofing is the technical part when launching attacks. Social engineering in phishing is dedicated to many people in the way of spam, while Business Email Compromise (BEC) focuses on the target victim.

According to a survey made by NordVPN, 84% of Americans have experienced some form of social engineering although only 54% have heard of the term ”social engineering” [58], however more and more studies and surveys reported that 84% of cyberattacks are conducted by social engineers with high success rate [59].

3.1.2.3 Malicious attachments and links

Malicious attachments and links are a common tactic cybercriminals use to distribute malware, ransomware, and other malicious software [60]. A survey conducted by Proofpoint found that 90% of cyberattacks start with an email, so cyberattacks require some form of human interaction to be successful, especially those malicious email attachments and links that are a common means of attack [56]. This will be explained in more detail in section 3.2.

In Figure 3.2, it is possible to see all the paths to carry out a phishing attack, including the spoofed website or malicious attachments.

Figure 3.2: A complete explanation of the phishing attack (Scheme: fig. 3.2 in [60]).

3.1.3 BEC attack

One of the types of phishing attacks that were highlighted in Figure 2.2 is the BEC attack. The COVID-19 pandemic caused a shift from traditional office environments to remote work-from-home settings, leading to an increase in BEC attacks. According to the 2020 Internet Crime Report from the FBI, 19,369 reported BEC complaints resulted, resulting in a total loss of $1.8 billion [61]. BEC attacks increased by 14% in 2020 due to the massive cyberattack surge prompted by the COVID-19 issue and worldwide lockdown measures [11].

3.1.3.1 Definition

BEC is a cybercrime tactic email to deceive individuals into revealing confidential information or sending money. The perpetrator impersonates a trustworthy figure, often requesting payment for a fictitious bill or requesting sensitive data for use in a future scam [62].

Specifically, BEC victims are typically executives or someone holding a position tied to finances. The purpose of BEC campaign is to be focused on the

target while causing the most significant impact on the infrastructure. Unlike regular phishing attacks that send out a large amount of spam to a large group of people [63].

3.1.3.2 Attack method

1. **Spoofing emails**
   About half of all BEC attacks are carried out by cybercriminals who spoof an individual's identity. These attackers target employees, who are more likely to click on malicious links if they see a familiar name or other relevant identifiers related to their job. The attackers use a variety of phishing techniques, including using the names of the company (68%), names of specific individuals (66%), and the names of bosses or managers (53%) to carry out their attacks [64].

2. **Phishing emails**
   Symantec research suggests that throughout 2020, 1 in every 4,200 emails was a phishing email. The vast majority of phishing attacks, 96%, arrive by email. Another 3% are carried out through malicious websites, while just 1% occur via phone [65]. Steer noted that 68% of people trust emails from friends or coworkers [61].

3. **BEC**
   During 2020, the IC3 noticed a surge in BEC complaints linked to exploiting stolen identities and converting funds into cryptocurrency. These variations typically involve an unsuspecting victim who falls prey to a non-BEC scam, such as romance scams, tech support scams or extortion [66]. The victim provides some form of identification to the scammer, which is then utilized to open a bank account to receive stolen BEC funds. After that, the funds are transferred to a cryptocurrency account [66].

4. **Social engineering**
   According to ISACA's State of Cybersecurity reports, social engineering was identified as the leading threat to organizations between 2016 and 2018. In this period, 48% of large companies and 32% of companies of all sizes have experienced at least 25 social engineering attacks. Among large companies, 30% have reported a per-incident cost of over $100,000 [67]. Currently, social engineering is used in 98% of all cyberattacks, costing companies an average of $130,000 through money theft or data destruction [68].

Figure 3.3 explain in detail the steps to the above steps:

Figure 3.3: BEC attack pattern (Scheme: fig. 3.3 in [69]).

3.2 Malware based-attack

The 2021 SonicWall Cyber Threat Report has revealed a significant increase in malware attacks. The report states that over the course of 2020, there were more than 18.5 million COVID-themed malware attacks, with the number of attacks exceeding 4 million in April alone [70].

The COVID-19 pandemic led to a global surge in malware incidents, increasing the likelihood of an organization being targeted by malware attacks to over 35%. However, by December of that year, the odds had decreased to approximately 21% [71].

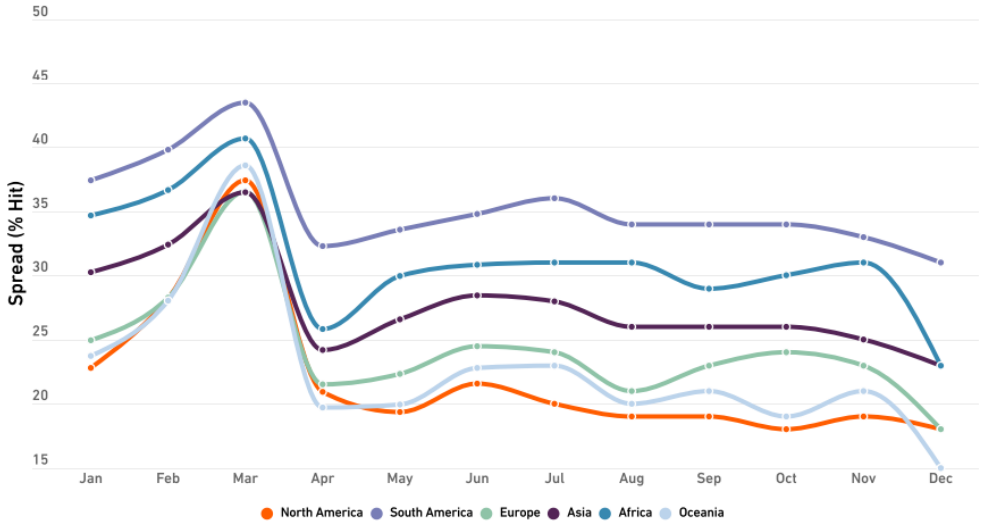

Figure 3.4: 2020 Global Malware Spread Trend (Graphic: fig. 3.4 in [71]).

3.2.1 Definition

Malware is any type of software designed to cause harm or damage to computer systems or networks. Malware can include viruses, Trojans, worms, spyware, and other types of malicious code. In this report, we differentiate between malware and software since their objectives and methods tend to differ, although it is known that ransomware is a type of software (malware).

3.2.2 Common delivery methods

- Email attachment and link: Previously explained on 3.1.2.3.
- Drive-by downloads: Occur when a victim visits a compromised website that downloads malware onto their computer without their knowledge [72].
- Software vulnerabilities: Attackers exploit weaknesses in software programs to gain access to systems and install malware.
- Infected USB drives: The malware is then installed onto the victim's system when the USB drive is connected.

- Remote Desktop Protocol (RDP): This protocol is used to access remote desktops. Attackers can use stolen credentials or weak passwords to gain access and deploy ransomware.
- Exploit Kits: Software tools that attackers use to take advantage of vulnerabilities in outdated software. Ransomware can be delivered through exploit kits that are hidden on websites or distributed through spam emails.

3.2.3 Ransomware

COVID-19 has brought about two significant concerns about ransomware. The first one is the incorporation of ransomware into phishing attacks, as discussed in 3.1. In June 2020, the group behind one particular ransomware strain sent out over one million phishing emails to infect US organizations [73]. This resulted in several high-profile ransomware attacks, with the largest payout of $40 million in Bitcoin reported by CNA Financial in March 2021 [74].

The second COVID-19-related concern is attacks against COVID research firms, firms manufacturing the vaccine, and healthcare facilities [73]. The COVID-19 pandemic has exacerbated this trend, making these organizations even more vulnerable to attacks [73]. According to Healthcare IT News, the annual number of ransomware attacks doubled from 43 in 2016 to 91 in 2021. Of these attacks, 44.4% targeted healthcare facilities, disrupting the delivery of crucial healthcare services [75]. Additionally, 8.6% of the attacks led to operational disruptions lasting over two weeks.

3.2.3.1 Definition

Ransomware is malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files until a ransom is paid [74]. When the ransom has not been paid, some firms have seen their data auctioned on the dark web site with prices ranging from $5,000 to over $20 million [73]. The type of ransomware attacks have different phases, however, the modern ransomware attack is explained in Figure 3.5.

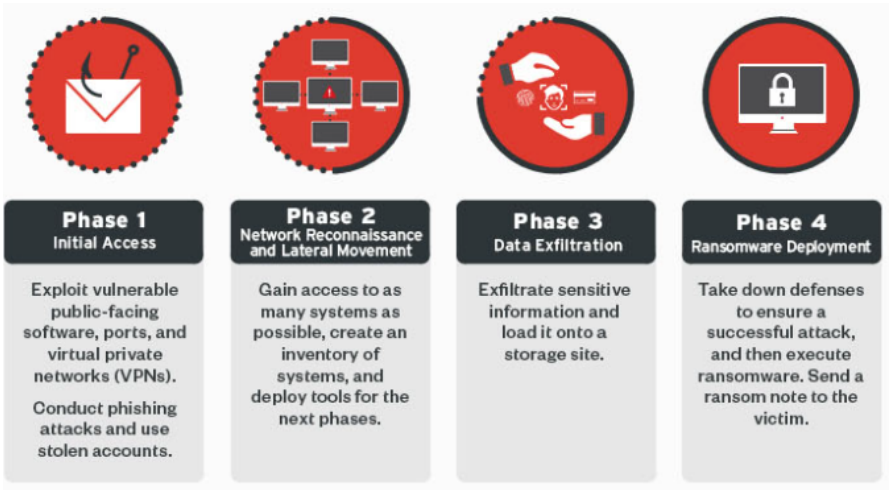

Figure 3.5: General Phases of a modern ransomware attack (Scheme: fig. 3.5 in [74]).

3.2.4 Main types of malware

Based on Figure 2.2 there are mentioned several types of malware that were involved in cyberattacks during the pandemic, however, the highlighted are:

3.2.4.1 Emotet

It is a banking Trojan first identified in 2014 [76]. It is typically spread through spam emails containing malicious attachments or links. During the COVID-19 pandemic, Emotet was used on notifications made by fake disability welfare providers and public health centers. In addition, the device infected with Emotet malware can deploy ransomware. The malware can also drop other types of malware that steal user credentials, browser history, and sensitive documents. The harvested data can then be used to send spam to other email accounts [77].

According to CheckPoint, Emotet was the most detected malware in January 2020, impacting 13% of organizations globally [78]. It was used mainly by cybercriminals, using recognized institutions such as WHO, health centers, and governments where they sent an email with information in Word or Excel about security measures, after accessing this file they downloaded the Emotet malware. An example of this malware can be seen in Figure 3.6.

Figure 3.6: First Emotet COVID-19 lure used on 29 January 2020 (Screenshot: fig. 3.6 in [79]).

3.2.4.2 TrickBot

TrickBot is a banking Trojan that has been active since 2016. It has evolved over the years to become a malware strain that can perform various of malicious activities, including launching phishing attacks and delivering ransomware payloads.

Similarly, as shown in Figure 3.6, TrickBot takes advantage of COVID-19-themed lures, preying on people's fears. For example, in 2020 TrickBot targeted hospitals and healthcare centers, launching a wave of ransomware in which the ransoms were paid to the TrickBot group [80].

3.2.4.3 Ryuk

Ryuk is a type of ransomware such as TrickBot that locks files or systems and holds them hostage for ransom and is used in targeted attacks [81].

A variant of the old Hermes ransomware, Ryuk tops the list of the most dangerous ransomware attacks. In CrowdStrike's Global Threat Report 2020, Ryuk accounts for three of the top ten ransom demands of the year. 5.3 million, 9.9 million, and 12.5 million dollars. Ryuk has successfully attacked industries and companies around the world. Hackers call the practice of attacking large companies "big game" [82].

When a system is infected with Ryuk, it shuts down 180 services and 40 processors because they prevent Ryuk infection. Then all important files are encrypted with 256-bit AES. In addition, you can do it remotely, and at the end, they leave you a note with text similar to the one in the figure 3.7 [82].

Figure 3.7: Ransomware Note.

3.2.4.4 NetWalker

NetWalker is a strain of ransomware, created in 2019. At a basic level, NetWalker operates similarly to many other types of ransomware, gaining

access through phishing emails and then stealing and encrypting important data to demand a significant ransom in exchange for it being released.[83]. There is a detailed explanation in Figure 3.8.

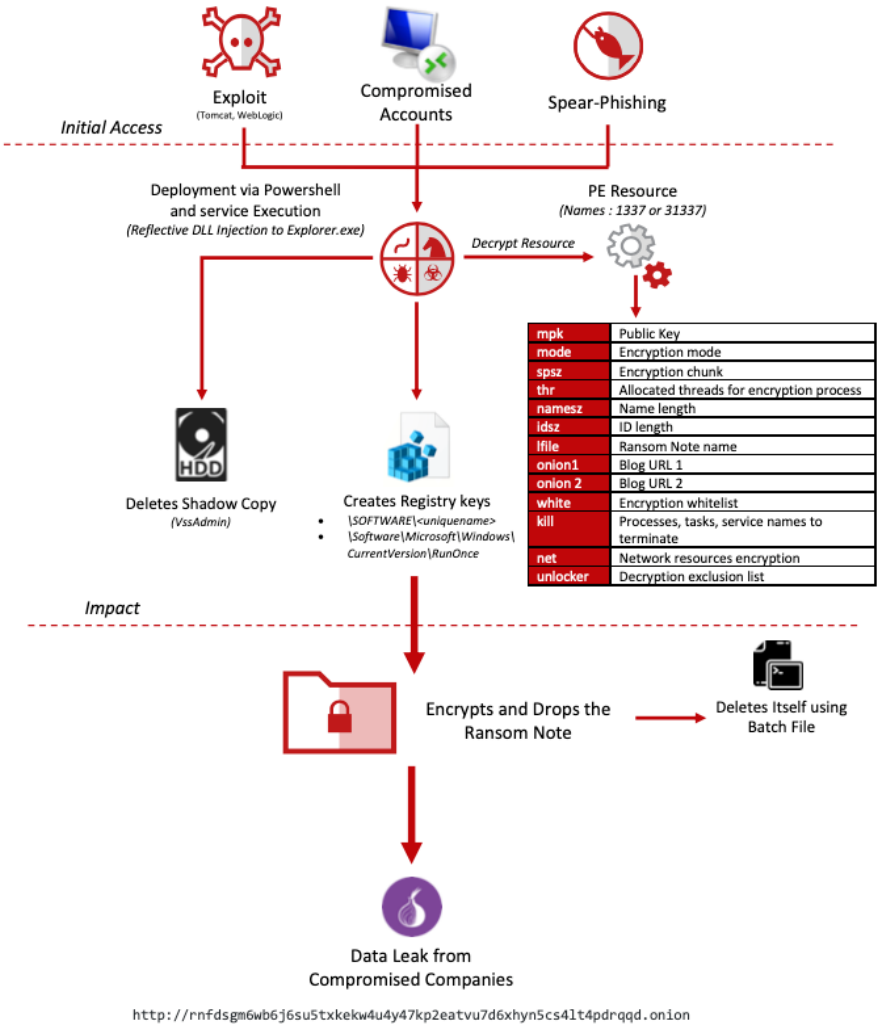

Figure 3.8: NetWalker behavior (Scheme: fig. 3.8 in [84]).

According to McAfee, the individuals behind the Netwalker ransomware obtained a staggering sum of $25 million in ransom payments from the beginning of March to the end of July. This is a significant amount of money, particularly when many industries struggle to survive due to lockdowns and economic downturns. McAfee's report suggests that Netwalker is profiting at the expense of legitimate companies already struggling to stay afloat [85].

In a report, the FBI noted that the number of NetWalker attacks on healthcare providers had increased during the pandemic, with the attackers [86]. The FBI also noted that the NetWalker group had successfully exported significant sums of money from their victims, with one victim reportedly paying a ransom of $4.5 million [86].

3.3 DDoS attack

DDoS attacks are more significant than ever. According to research made by Imperva in 2020, network DDoS traffic has increased by 24% [87]. Additionally, there is an increase of 41% in the total number of DDoS packets and a 21% increase in DDoS attack duration. This attack can produce downtime in organizations, costing up to $100k [87].

3.3.1 Definition

A DDoS attack is a type of cyberattack that involves overwhelming a targeted server, service, or network with a massive flood of internet traffic. This attack aims to disrupt the normal traffic flow and render the target inaccessible to legitimate users [88].

3.3.2 DDoS on Health Agencies

The United States Health and Human Services Department's website has been hitting several times during the COVID-19 pandemic. Criminals have been taking advantage of the situation of the people to block access to the website and create fear and confusion, as well as slowing down progress on the COVID-19 vaccine with the idea of being able to demand a ransom to unlock access to the website [89].

According to a Neustar report, DDoS attacks experimented with a 151% increase in number compared to the same period in 2019 [90]. The 2021 Global DNS Threat Report showed that the average cost per attack in healthcare increased to $862,630, a rise of 12% from 2020 and the sharpest increase seen by any industry [91].

3.3.3 Common types of DDoS attacks

- Volumetric Attack: Floods the target with a high volume of traffic, overwhelming its bandwidth capacity.
- TCP State-Exhaustion Attack: Exploits the stateful nature of the TCP protocol to exhaust resources on the target, such as connection tables or session state tables.
- Application Layer Attack: Targets the web application layer, overwhelming the server with requests that appear to be legitimate.
- Protocol Attack: Exploits weaknesses in network protocols, such as Ping of Death attacks or SYN floods.
- Reflective Attack: Leverages a third-party server to amplify the attack traffic, making it harder to trace the source.
- Distributed Reflection Denial of Service (DRDoS): Similar to reflective attacks, but using multiple reflecting servers to amplify the attack traffic.
- Amplification Attack: Sends a small amount of traffic to a vulnerable server that responds with a much larger amount of traffic, which is then directed at the target.
- IoT-Based Attack: Uses compromised IoT devices, such as smart cameras or routers, to launch coordinated attacks.
- Mobile Attacks: Targets mobile devices and exploits their vulnerabilities to overwhelm servers and networks.

3.4 Summary

2020 witnessed a surge in cyberattacks, with cybercriminals exploiting the pandemic to launch more attacks. Phishing attacks have become the most popular, with scammers using COVID-19 themes to deceive people. To make the attacks more powerful, cybercriminals take advantage of malware, particularly ransomware, which has led to significant financial losses for victims, as discussed in subsection 3.2.4. Moreover, due to the increased demand for online services, the number of DDoS attacks has risen, with victims forced to pay ransom to restore their services.

These attacks have become more sophisticated and can be combined in different ways to make them more successful and undetectable. Therefore, it is crucial to remain vigilant and implement countermeasures to protect against these threats.

Chapter 4

Mitigations deployed to counter cyberattacks during the pandemic

As discussed in the previous chapter, organizations around the words have had to deploy new strategies and technologies to mitigate the risks of cyberattacks during the pandemic, caused by the change in how people work and live. This chapter will focus on the mitigations implemented to counter the most prevalent types of cyberattacks during the pandemic. In addition, it will discuss the effectiveness of these mitigations, including statistics and surveys conducted to analyze their success. It is necessary to understand those measures to develop future effective cybersecurity strategies.

The countermeasures to phishing are in 4.1, DDoS in 4.3, and malware in 4.2.

4.1 Phishing attack

Phishing and BEC are often grouped because they use social engineering tactics to trick individuals. Due to the similarities in the attack method and mitigations, it has been decided to cover these two topics under the same section.

4.1.1 Employee training and awareness programs

Cybercriminals found new opportunities to launch attacks when the work began to be carried out remotely. However, different organizations realized their shortcomings and trained their employees to make them aware of this type of cyberattack.

According to a survey conducted by ISACA, 52% of organizations indicated that employees were their most significant weakness in IT security [92]. In another report by Proofpoint, only 53% of respondents could correctly identify the definition of the term 'phishing' in a multiple-choice matrix, down from 63% last year, a 16% year-over-year decrease [93]. Additionally, the failure rate in phishing simulations remained stable at 11% year-on-year [93].

Employee training and awareness programs focus on educating employees about common cyber threats such as phishing attacks. They also teach employees about how to recognize and report suspicious activity, as well as how to safely handle sensitive information.

However, the effectiveness of employee training programs can vary based on the quality and frequency of the training. Overall, time given to training was slow, with 80% of respondents saying their organizations only offered two hours or less per year, according to Proofpoint survey [94].

Nowadays, 98% of organizations have a training program but only 56% train everyone in the organization, and 35% run phishing simulations [94]. In summary, employee training and awareness programs have proven effective mitigation strategies for countering cyberattacks during the pandemic.

4.1.1.1 General rules

According to WHO during the COVID-19 pandemic, most phishing attacks include suspicious information that claims to request information or click on a link or domain. In that way they use the victim to download malware [95]. To avoid that there are simple rules:

1. Check their email address.
2. Check the link before you click.
3. Be careful when providing personal information.

4. Do not rush or feel under pressure.

5. If you gave information do not panic and change the credentials of all sites.

6. If you see a scam, report it

Using those recommendations among all the recommendations that can be taught is possible to avoid a significant amount of problems.

4.1.2 Best Practices for computer security measures

The best security measures that can help to prevent phishing attacks are Two-Factor Authentication (2FA) and email blocking and filtering. It is important to note that these are just two of many possible security measures that can be implemented. Keeping software up-to-date and using strong, unique passwords is crucial to protecting yourself.

4.1.2.1 Two-factor authentication

2FA is a security process where users provide two different authentication factors to verify themselves [96]. The use of 2FA has been found to be an effective mitigation strategy against cyberattacks [96].

A report conducted in 2020 by Last Pass reported that 57% of organizations use MFA [97]. Additionally, the report found that 2FA is useful, as seen with Google, where the Google authentication shows that MFA provides up to 100% protection from automated cyberattacks.

2FA showed to be effective because 61%of people reuse the same password across multiple accounts [98]. In view of such data, companies such as Google made an obligation 2FA for 150 million Google users in 2021, showing a 50% decline in compromised accounts [99].

However, the FBI said that 2FA does not mean that it is enough, still it is necessary to:

1. Make it unique to your life but something not easily guessed.

2. Use a different one for each online account, write it down and store it safely away from the computer.

3. Change it several times a year.

In conclusion, 2FA is an effective defense mechanism against phishing attacks. Requiring a second authentication factor makes it much harder for attackers to access sensitive information even if they have obtained the user's password through a phishing email.

4.1.2.2 Email filtering and blocking

Email filtering and blocking are common mitigation measures deployed by organizations to prevent cyberattacks. According to a report by Mimecast, email blocking tools such as Domain-based Message Authentication, Reporting and Conformance (DMARC) are aware by 97% of respondents of the survey, however only 28% use DMARC [100]. These data are alarming because the number of scams is increasing and large companies like Gmail use filters that block 100 million phishing attacks [101].

In 2020, according to a report by SecureList, anti-phishing was able to block 434,898,635 attempts at redirecting users to phishing web pages and 184,435,643 were dangerous emails with malicious attachments [102].

Overall, this measure can prevent malicious emails from reaching users' inboxes. However, this is not infallible and can still miss some advanced or targeted attacks.

4.1.3 Laws and regulations

Phishing has been an important topic of concern between governments due to the crisis of scams during the COVID-19 pandemic. In response, governments have been working to strengthen their laws and regulations.

Federal Trade Commission (FTC) has warned about COVID-19-related phishing scams to report suspicious emails in the United States [103]. The agency has also taken action against companies that do that type of practice.

TheGeneral Data Protection Regulation (GDPR) has played a crucial role in the fight against phishing attacks in Europe. The GDPR mandates that companies implement appropriate technical and organizational measures to safeguard personal data from unauthorized access. Moreover, it grants individuals the right to access their personal data and request its deletion or

correction [104].

In addition, there are broader laws to cybersecurity that can also use to combat phishing. For example, the Computer Fraud and Abuse Act prohibits unauthorized access to computers and networks [105]. In the United Kingdom, criminalized unauthorized access to computer systems [106].

4.2 Malware-based attack

4.2.1 Employee training and awareness

Mitigations for malware attacks are essential today, especially during the COVID-19 pandemic when many employees work remotely. With the rise in remote work, employees must be trained to identify and avoid malware attacks.

According to a survey conducted by Proofpoint, users alerted their security teams to more than 350,000 credential phishing emails, and nearly 40,000 emails with malware payloads [93]. In addition, only 63% of the respondents said they recognized the definition of malware [93].

The same survey highlights the effectiveness of employee training and awareness in mitigating the risk of malware attacks. It found that security awareness training programs are covered in 43% of the programs and had a 60% lower click rate on phishing emails compared to those that did not provide training [107].

4.2.1.1 Guidance for being prepared

Among the many guides and recommendations that we can find on the internet, it is worth highlighting the one made by the National Cyber Security Center that recommends:

1. **Make regular backups**
2. **Prevent malware from being delivered and spreading to devices**
    - Filtering to only allow file types you would expect to receive.
    - Blocking websites that are known to be malicious.
    - Actively inspecting the content.

- Using signatures to block known malicious code.

3. **Prevent malware from running on devices**
   The measures required will vary for each device type, OS, and version, but you should generally use device-level security features.

4. **Prepare for an incident**

The list of recommendations explains the main type of recommendations giving information for more it is recommended to look on the web [108].

4.2.2 Best practices for computer security measures

To ensure the security of computer systems, it is essential to adopt best practices such as regular software updates, strong passwords, and network segmentation. Among these measures, network segmentation and endpoint security solutions are particularly important for mitigating the risk of malware attacks. This subsection will focus on the importance of these measures and guide on how to implement them effectively.

4.2.2.1 Network segmentation

As seen in 4.3 network segmentation is used to restrict the propagation of the attacks across the network. Furthermore, network segmentation improves the general vision of the network, making it easier to detect and respond to potential attacks.

4.2.2.2 Endpoint security solutions

Endpoint security solutions are the practice of securing endpoints or entry points of end-user devices from being exploited by malicious attacks [109].

In a research report from Malwarebytes, over 68% of firms suffered one or more damaging endpoint attacks that compromised valuable information, and 60% of endpoints of those organizations had endpoints harbor hidden threats, like Trojans, rootkits and backdoors [110].

According to Statista, the market 2020 of endpoint security software has been increasing with time, in 2019 was $7.459 million, and in 2020 was $8.212 million [111].

To sum up, endpoint security solutions have proven to be effective mitigations and as remote work continues to be part of our lives, endpoint security will be important to avoid cyberattacks.

4.2.3 Laws and regulations

Malware can pose a serious threat to organizations and individuals, with the potential to cause disruption and financial loss. To help mitigate these risks, several laws and regulations have been put in place during the COVID-19 pandemic to prevent malware attacks.

One regulation issued by the National Cyber Security Center of the United Kingdom in the European Union is a guideline with appropriate techniques and measures to protect data. In subsection 4.2.1 there is a guidance to those recommendations [108].

In the United States, the National Institute of Standards and Technology (NIST) issued an alert about an increase in malware/ransomware attacks targeting remote workers during the pandemic. CISA recommends implementing different defenses such as endpoint detection or updating software [112].

To sum up, laws and regulations are important to mitigate the risk of malware attacks. Organizations should follow the guidance provided.

4.3 DDoS attack

4.3.1 Employee training and awareness

Employee training and awareness is a critical aspect of DDoS mitigation. There is no specific training for avoiding DDoS attacks. However, there is a list of recommendations that should be taken in mind to prevent attacks. It can be seen in the sub-subsection 4.3.1.1.

4.3.1.1 General recommendations

From 2020 to 2021, there were different recommendations to avoid DDoS attacks [113]. According to a report of Odata, the recommendations that everyone should pay attention to prevent DDoS are:

- Document your plan: Develop an action plan, consisting of a set of best practices to be adopted in case of attacks. Responding quickly to incidents is essential to choose the right path and reducing damages.
- Do not underestimate attacks: Many attackers launch small volumes of requests just to test the system before doing something more significant. Therefore, it's important to constantly monitor and double your attention when such action occurs. It could be a sign of something worse.
- Avoid relying solely on traffic monitoring: Often, it's not possible to distinguish whether it's good or bad traffic. So, this analysis is not enough to detect attacks.
- Invest in the multiplicity of resources: Having an Intrusion Prevention System (IPS) or integrated firewall is insufficient. Attackers usually find gaps in some of them. That's why building a solid plan is important. There are some examples in subsection 4.3.2.
- Internet Service Providers: Many providers offer DDoS attack protection plans. For example, the advantage of having a Remote Data Center is that the operation is already entirely based on security. That is, specialized technicians control these aspects.

4.3.2 Best Practices for computer security measures

In the cybersecurity world, many strategies and tools are available for protecting computer systems. In this section, we will focus on three specific techniques: network segmentation, load balancing, and traffic filtering and blocking which were used during the COVID-19 pandemic. While there are certainly other approaches to mitigate DDoS, we will delve into these three in more detail due to their proven effectiveness

4.3.2.1 Network segmentation

Network segmentation is a security technique that divides a network into smaller, with each segment having its security controls [114]. The idea is to mitigate DDoS, in a way that it is impossible to send a large volume of traffic to overload a simple network. In that way is necessary to limit the attack.

As reported in a survey by HelpNet Security in 2021, 96% of organizations claim to be implementing segmentation in their networks, yet only 2% of

those organizations are segmenting all six mission-critical asset classes [115]. However, segmentation is an IT approach that separates critical areas of the network and this can often prove labor-intensive, implying that 82% of respondents think that is a huge task [115].

According to the findings of the previous survey, 92% of respondents believe that implementing network segmentation has prevented cyberattacks, further, it identifies external attacks spreading more quickly (49%) and internal attacks (44%) [115]. Despite this, the respondents claim that the segmentation is used across two or fewer mission-critical areas [115].

Overall, network segmentation is useful against DDoS attacks. The statistics show that many organizations have recognized network segmentation's value and implemented it as part of their security strategy.

4.3.2.2 Load balancing

Load balancing effectively divides incoming network traffic flow among a collection of backend servers.

Based on the F5 report between January 2020 and March 2021, DDoS attacks increased by 55% and are becoming more complex [116]. Load balancing has shown to be useful against DDoS, it adds resiliency by rerouting live traffic from one server to another.

Additionally, load balancing can be used with other security measures. The combination of load balancing and other security measures can provide a strong defense against cyberattacks.

4.3.2.3 Traffic filtering and blocking

Traffic filtering and blocking are used as common ways to defend against malicious traffic on the Internet. The purpose of these measurements is to prevent malicious traffic from reaching the organization or the network.

According to the TrustRadius report, this can be reflected in the global network security firewall market, where the market size was $3.364 billion in 2020 [117]. The same report found that 30% of companies have more than 100 firewalls set up on their network.

Finally, traffic filtering and blocking can protect the user by blocking high-risk sites, spam, and malicious websites, that is why the organizations adopt it. However, it does not teach the users hows to use the internet responsibly.

4.3.3 Laws and regulations

Governments and regulatory bodies have implemented laws and regulations to mitigate the risk of DDoS attacks during this period.

One regulation is the CISA Telework Essential Toolkit, which provides guidelines for remote workers on protecting their devices and network from cyber threats. The toolkit included advice on making frequent backups to protect themselves from prolonged disruption or enterprise cybersecurity control to avoid disruption from outside the network [118].

In addition, the United States Department of Health and Human Services issued guidance for healthcare organizations on cybersecurity during the COVID-19 pandemic [119]. The guidance emphasizes the importance of maintaining a robust cybersecurity program for being prepared for DDoS attacks. The United States Department of Health and Human Services recommends using intrusion detection and prevention systems and having a response plan [119].

In summary, laws and regulations implemented during the COVID-19 pandemic aim to mitigate the risk of DDoS attacks by providing guidelines for remote workers, highlighting the importance of maintaining a robust cybersecurity program and ensuring access to digital services.

4.3.4 Summary

A comprehensive cybersecurity approach is important for any organization in today's digital landscape. Cyber threats such as DDoS, malware, and phishing attacks are evolving and becoming more sophisticated, highlighting the importance of using different security measures.

Implementing security solutions such as those previously mentioned in this chapter helps protect us against various types of attacks. However, relying on a single solution is not enough.

In addition, to have multiple security measures is important to follow laws and regulations related to cybersecurity because the governments have the methods and the best guides regarding the use of technologies for organizations and individuals helping them and providing them with information on how to defend themselves.

Furthermore, employee training and awareness programs keep employees informed and educated about cyber threats. This training can include best practices for them, helping to reduce the risk of a cyberattack.

Chapter 5

Conclusions and Future work

5.1 Conclusions

In this thesis, I explore the evolution of security systems during the COVID-19 pandemic. Based on the information from the different reports, surveys, conferences, and sites across the Internet, the main types of attacks launched are DDoS, malware, ransomware, phishing, and BEC attacks and their mitigations implemented by the different organizations. Finally, we discussed the different recommendations given by experts.

The thesis fulfills the research question, defining the evolution of cybersecurity during COVID-19 and how people were learning how to countermeasure the different attacks. Despite all the breaches created by cybercriminals, organizations have learned how to prevent those attacks. However, they need to remain vigilant and keep evolving their cybersecurity system to avoid similar situations.

The thesis has enabled me to gain new knowledge about the security system, reminding the importance of the security system in our day-to-day. Furthermore, I learned new techniques to avoid cyberattacks on my personal computer. My suggestion to all the people working in that area is to invest in cybersecurity because it is an evolving field that always requires improving our knowledge about it.

5.2 Limitations

The thesis had different limitations that were hard to decide how to solve. First of all, the COVID-19 pandemic was a long period that had a lot of different attacks and mitigations, so it was hard to decide which ones were the most important and which mitigations the organizations used during that period. Secondly, different organizations deployed the mitigations, so it was necessary to choose the main ones. Finally, the recommendations made by the experts were so many, then I select the ones that are the best to avoid the majority of the attacks and recommended by the majority.

5.3 Future work

Due to the scope of the research, only some of the initial goals have been met. This section will focus on some of the remaining issues that should be addressed in future work. The thesis just talks about the main attacks and mitigations, so it would be a good idea to try to explain more about the attacks and mitigations, giving more technical examples. Furthermore, it can give a visual example of those attacks to show how they work. Additionally, it would do a more detailed explanation of the evolution of security systems during COVID-19, trying to go into more specific details that could not be shown.

5.4 Reflections

One of the most significant findings is the amount of money lost due to cyberattacks, the thesis contributes to the organizations giving accurate data on the different amounts of money that can be lost, and also providing, recommendations to avoid it. On the other hand, cybercriminals are causing the average person to lose a large amount of money, generating consequences only to get economic benefits or recognition.

References

[1] "Coronavirus disease (covid-19) - world health organization," *World Health Organization*, Sep. 2020. [Online]. Available: https://www.who.int/emergencies/diseases/novel-coronavirus-2019

[2] M. K. J. D. P. Muhammad Kashif, Aziz-Ur-Rehman, "A surge in cyber-crime during covid-19," *Indonesian Journal of Social And Environmental Issues*, vol. 1, pp. 48–52, August 2020. doi: 10.47540/ijsei.vli2.22. [Online]. Available: https://www.ojs.literacyinstitute.org/index.php/ijsei/article/view/22/38

[3] "It risk and resilience-cybersecurity response to covid-19," *IEEE Xplore*, vol. 22, pp. 4–10, may 2020. doi: 10.1109/MITP.2020.2988330. [Online]. Available: https://ieeexplore.ieee.org/document/9098180/figures

[4] M. Y. X. L. Y. H. Q. Isaac Chin Eian, Lim Ka Yong and F. Z, "Cyber attacks in the era of covid-19 and possible solution domains," *Preprints.org*, September 2020. doi: 10.20944/preprints202009.0630.v1. [Online]. Available: https://www.preprints.org/manuscript/202009.0630/v1

[5] A. Cook, "Covid-19: Companies and verticals at risk for cyber attacks." [Online]. Available: https://www.digitalshadows.com/blog-and-research/covid-19-companies-and-verticals-at-risk-for-cyber-attacks/

[6] "Computer security," feb 2023. [Online]. Available: https://en.wikipedia.org/wiki/Computer_security

[7] M. P. R. K. Aleksandra Pawlicka, Michał Choraś, "A $ 10 million question and other cybersecurity-related ethical dilemmas amid the covid-19 pandemic," *ScienceDirect*, vol. 64, no. 6, pp. 729–734, November 2021. doi: 10.1016/j.bushor.2021.07.010. [Online].

Available: https://www.sciencedirect.com/science/article/pii/S0007681321001336

[8] J. A. Lewis, "Cyber war and ukraine." [Online]. Available: https://www.csis.org/analysis/cyber-war-and-ukraine

[9] "Cyber crime." [Online]. Available: https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime#:~:text=Cyber

[10] "Ciberamenazas relacionadas con la covid-19." [Online]. Available: https://www.interpol.int/es/Delitos/Ciberdelincuencia/Ciberamenazas-relacionadas-con-la-COVID-19

[11] O. I. A. Moatsum Alawida, Abiodun Esther Omolara, "A deeper look into cybersecurity issues in the wake of covid-19: A survey," *ScienceDirect*, vol. 34, no. 10, pp. 8176–88 206, November 2022. doi: 10.1016/j.jksuci.2022.08.003. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1319157822002762

[12] "Informe el futuro del trabajo remoto seguro," *cisco*, 2021. [Online]. Available: https://www.cisco.com/c/dam/global/es_mx/products/pdfs/future-of-secure-remote-work-report.pdf

[13] J. Turner, "The 7 main ways technology impacts your daily life." [Online]. Available: https://tech.co/vpn/main-ways-technology-impacts-daily-life#:~:text=Technology.

[14] "Balancing personal privacy and public safety during covid-19: The case of south korea," *IEEE*, vol. 8, pp. 171 325–171 333. doi: 10.1109/ACCESS.2020.3025971. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9203800

[15] "Campus traffic and e-learning during covid-19 pandemic," vol. 176. doi: 10.1016/j.comnet.2020.107290. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128620306046

[16] A. Dolezal, "Cyber threats have increased 81% since global pandemic." [Online]. Available: https://www.businesswire.com/news/home/20211108005775/en/Cyber-Threats-Have-Increased-81-Since-Global-Pandemic

[17] F. Shi, "Threat spotlight: Coronavirus-related phishing," Mar. 2020. [Online]. Available: https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/

[18] J. R. C. N. A. E. G. E. C. M. Harjinder Singh Lallie, Lynsay A. Shepherds and X. Bellekens, "Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic." [Online]. Available: https://kar.kent.ac.uk/86976/1/Cyber_Security_in_the_Age_of_COVID_19.pdf

[19] "Who reports fivefold increase in cyber attacks, urges vigilance," *WHO*. [Online]. Available: https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance

[20] S. Morrison, "What we know about the health department website cyberattack." [Online]. Available: https://www.vox.com/recode/2020/3/16/21181825/health-human-services-coronavirus-website-ddos-cyber-attack

[21] L. Grustniy, "The great lockdown: How covid-19 has affected cybersecurity," *Kaspersky daily*, Mar. 2021. [Online]. Available: https://www.kaspersky.com/blog/pandemic-year-in-infosec/39123/

[22] D. K. Bhavani, "Beware coronavirus-themed cyber-attacks, urges mcafee." [Online]. Available: https://www.thehindu.com/sci-tech/technology/internet/mcafee-2021-consumer-mindset-report-covid19-cybersecurity-internet-habits-india/article34699465.ece

[23] "115 cybersecurity statistics and trends you need to know in 2021." [Online]. Available: https://us.norton.com/blog/emerging-threats/cyberthreat-trends-cybersecurity-threat-review#

[24] T. H. Poll, "2021 norton cyber safety insights report global results," *Norton*, May 2021. [Online]. Available: https://now.symassets.com/content/dam/norton/campaign/NortonReport/2021/2021_NortonLifeLock_Cyber_Safety_Insights_Report_Global_Results.pdf

[25] "Aumento de ciberataques con la pandemic: ¿cuál es la situacion actual." [Online]. Available: https://www.ikusi.com/mx/blog/aumento-de-ciberataques-con-la-pandemia-cual-es-la-situacion-actual/

[26] M. N. Ankit Fadia and J. Noble, "Follow the leaders: How governments can combat intensifying cybersecurity risks," *McKinseyCompany*, Sep. 2020.

[27] G. Sands, "Millions in covid relief funding to be used for federal cybersecurity efforts," *CNN*, March 2021. [Online]. Available: https:

//edition.cnn.com/2021/03/10/politics/millions-covid-relief-funding-cybersecurity/index.html

[28] Álvaro Merino, "Enisa: The cornerstone of the eu's cybersecurity strategy," *European Data Journalism Network*, December 2021. [Online]. Available: https://www.europeandatajournalism.eu/eng/News/Data-news/ENISA-The-cornerstone-of-the-EU-s-cybersecurity-strategy#:~:text=As.

[29] "Advisory: Covid-19 exploited by malicious cyber actors," *National Cyber Security Center*, April 2020. [Online]. Available: https://www.ncsc.gov.uk/news/covid-19-exploited-by-cyber-actors-advisory

[30] "Nuevas normas para aumentar la ciberseguridad y la seguridad de la información en las instituciones, órganos, organismos y agencias de la ue," *European Commission*, March 2020. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/es/ip_22_1866

[31] "Cybercrimes act 19 of 2020 (english / afrikaans)," June 2020. [Online]. Available: https://www.gov.za/documents/cybercrimes-act-19-2020-1-jun-2021-0000

[32] "How the five eyes alliance fuels global surveillance," *NordVPN*, Jun 2022. [Online]. Available: https://nordvpn.com/es/blog/five-eyes-alliance/

[33] E. G., "Over 150,000 covid-related fraud reports submitted to the us government ytd," *AtlasVPN*, August 2020.

[34] T. Sharma and M. Bashir, "Use of apps in the covid-19 response and the loss of privacy protection," *nature medicine*, May 2020.

[35] "How covid-19 has pushed companies over the technology tipping point and transformed business forever," October 2020. [Online]. Available: https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever#/

[36] "Cyber-resilience during a crisis." [Online]. Available: https://www.kaspersky.com/blog/smb-cyber-resilience-report-2022/

[37] "Homeworkers wait for protection: 73% of employees have not received remote working cybersecurity guidance," *Kaspersky*, May

2020. [Online]. Available: https://www.kaspersky.com/about/press-releases/2020_homeworkers-wait-for-protection-73-of-employees

[38] A. Conway, "New data from microsoft shows how the pandemic is accelerating the digital transformation of cyber-security," *Microsoft*, August 2020. [Online]. Available: https://www.microsoft.com/en-us/security/blog/2020/08/19/microsoft-shows-pandemic-accelerating-transformation-cyber-security/

[39] "Phising." [Online]. Available: https://en.wikipedia.org/wiki/Phishing

[40] "Anti-phising software." [Online]. Available: https://en.wikipedia.org/wiki/Anti-phishing_software

[41] M. A. Alex Sumner, Xiaohong Yuan and M. McBride, "Examining factors impacting the effectiveness of anti-phishing trainings," *Journal of Computer Information Systems*, vol. 62, pp. 975–997, August. doi: 10.1080/08874417.2021.1955638. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/08874417.2021.1955638

[42] R. Bansode and A. Girdhar, "Common vulnerabilities exposed in vpn – a survey," *IOPScience*, October 2020. doi: 10.1088/1742-6596/1714/1/012045. [Online]. Available: https://iopscience.iop.org/article/10.1088/1742-6596/1714/1/012045/meta

[43] "¿qué es una vpn y cómo funciona?" [Online]. Available: https://www.kaspersky.es/resource-center/definitions/what-is-a-vpn

[44] M. E. Bonfanti, "Artificial intelligence and cybersecurity: a promising but uncertain future," December 2020. [Online]. Available: https://www.realinstitutoelcano.org/en/analyses/artificial-intelligence-and-cybersecurity-a-promising-but-uncertain-future/

[45] "Iot security challenges and problems." [Online]. Available: https://www.balbix.com/insights/addressing-iot-security-challenges/

[46] "The state of ai in 2021." [Online]. Available: https://www.mckinsey.com/capabilities/quantumblack/our-insights/global-survey-the-state-of-ai-in-2021

[47] "Cybersecurity trends: Looking over the horizon." [Online]. Available: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon

[48] "With the right security outcomes, your business thrives." [Online]. Available: https://www.withsecure.com/en/expertise/campaigns/with-or-without?gclid=CjwKCAiAjPyfBhBMEiwAB2CCIr4MWgaqiYKunwpcX6oajK_gCx_86u_2iBIWcIhXBwrv6dIlcQB6ZBoCreAQAvD_BwE

[49] M. R. P. Rabi Prasad Padhy and S. C. Satapathy, "Cloud computing: Security issues and research challenges," *International Journal of Computer Science and Information Technology Security*, vol. 1, no. 2, pp. 136–146, 2011. [Online]. Available: https://d1wqtxts1xzle7.cloudfront.net/43674121/cloud_computing_avee-libre.pdf?1457852189=&response-content-disposition=inline%3B+filename%3DCloud_Computing_Security_Issues_and_Rese.pdf&Expires=1678640314&Signature=JLTB-WIkqYPKONPftHP5MjW6q3TYZ06k7-KSMma1iOMfrEegdVIiXpRX-cFF8HGEmbSWpn1WNffWcxURjOzR77eyyl175I1Ty6~yXti8wUnWj6I7Cezre89VgmW92CQxPRpg2Bd455jy3VTUpVLOLLWBEVgmDOF2qe0a89H8gGN-Rf8DRFMi0IeSJvUVb24k2dycGOkW1Z77HdDjalMyXcUq7nGKre8mspcBq1JPCF8aU~HuZxo7Z0JwmoQD3bG9GBTEti5Ri-FoBAiG0QwvAR0wzlrchF3Q-XK28lCukbvsWsBia0HdT1fX-6p5KFpBQwlyKApitXZJ2qrG7inzlw__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

[50] "Flexera releases 2021 state of the cloud report," March 2021. [Online]. Available: https://www.flexera.com/about-us/press-center/flexera-releases-2021-state-of-the-cloud-report

[51] "How artificial intelligence is used for cyber security attacks." [Online]. Available: https://fraudwatch.com/how-artificial-intelligence-is-used-for-cyber-security-attacks/

[52] S. C. Ali F. Al-Qahtani, "The covid-19 academic: A survey of phishing attacks and their countermeasures during covid-19," *The Institution of Engineering and Technology*, vol. 16, no. 5, pp. 324–345, July 2022. doi: 10.1049/ise2.12073. [Online]. Available: https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/ise2.12073

[53] "What is a phishing attack?" [Online]. Available: https://www.cloudflare.com/learning/access-management/phishing-attack/

[54] "Interpol report shows an alarming rate of cyberattacks during covid-19," August 2020. [Online]. Available: https://www.interpol.int/New

s-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

[55] F. Shi, "Threat spotlight: Coronavirus-related phishing," March 2020. [Online]. Available: https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/

[56] "What is email spoofing?" [Online]. Available: https://www.proofpoint.com/us/threat-reference/email-spoofing#:~:text=Email%20spoofing%20is%20a%20technique,users%20take%20at%20face%20value.

[57] "What is "social engineering"?" [Online]. Available: https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering

[58] S. Sjouwerman, "The extent of social engineering," August. [Online]. Available: https://blog.knowbe4.com/the-extent-of-social-engineering

[59] F. Salahdine and N. Kaabouch, "Social engineering attacks: A survey," *MDPI*, vol. 11, no. 4, April 2019. doi: 10.3390/fi11040089. [Online]. Available: https://www.mdpi.com/1999-5903/11/4/89

[60] K. R. R. Venkatesha Sushruth and B. R. Chandavarkar, "Social engineering attacks during the covid-19 pandemic," *Springer Link*, February 2021. doi: 10.1007/s42979-020-00443-1

[61] C. P.Dutcher, "Pandemic phishing: Business email compromise during covid-19," Master's thesis, Utica University, May 2022. [Online]. Available: https://www.proquest.com/openview/19782fe66d0c2950850fb6f9e233d04f/1?pq-origsite=gscholar&cbl=18750&diss=y

[62] "What is business email compromise (bec)?" [Online]. Available: https://www.microsoft.com/en-us/security/business/security-101/what-is-business-email-compromise-bec#:~:text=Business%20email%20compromise%20(BEC)%20is%20a%20type%20of%20cybercrime%20where,can%20use%20in%20another%20scam.

[63] J. S., "Defined: Phishing vs bec." [Online]. Available: https://www.linkedin.com/pulse/defined-phishing-vs-bec-jaclyn-jax-scott/

[64] "71% of organizations experienced bec attacks over the past year," June 2021. [Online]. Available: https://www.helpnetsecurity.com/2021/06/25/bec-attacks-past-year/

[65] M. Rosenthal, "How phishing attacks are delivered," January 2022. [Online]. Available: https://www.tessian.com/blog/phishing-statistics-2020/#:~:text=Symantec%20research%20suggests%20that%20throughout,as%20the%20primary%20infection%20vector.

[66] P. Abbate, "Internet crime report 2020." [Online]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

[67] L. S. Zuoguang Wang and H. Zhu, "Defining social engineering in cybersecurity," *IEEE Xplore*, vol. 8, pp. 85 094–85 115, 2020. doi: 10.1109/ACCESS.2020.2992807. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9087851

[68] C. Reed, "21 social engineering statistics – 2022," May 2022. [Online]. Available: https://firewalltimes.com/social-engineering-statistics/

[69] K. Donegan, "Explore 5 business email compromise examples to learn from." [Online]. Available: https://www.techtarget.com/searchsecurity/feature/Explore-5-business-email-compromise-examples-to-learn-from

[70] A. O'Driscoll, "40+ covid-19 cybersecurity statistics: Have threats increased?" November 2022. [Online]. Available: https://www.comparitech.com/blog/information-security/covid-19-cybersecurity-statistics/

[71] "2021 sonicwall cyber threat report." [Online]. Available: https://www.sonicwall.com/medialibrary/en/white-paper/2021-cyber-threat-report.pdf

[72] "Drive-by download." [Online]. Available: https://en.wikipedia.org/wiki/Drive-by_download

[73] N. M. M. . G. D. Richardson, R., "Ransomware: The landscape is shifting a concise report." *International Management Review*, vol. 17, no. 1, pp. 5–86, 2021. [Online]. Available: http://www.americanscholarspress.us/journals/IMR/pdf/IMR-1-2021/V17n121-art1.pdf

[74] "Ransomware definition," *Trend Micro*, 2023. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/definition/ransomware

[75] A. Fox, "Half of ransomware attacks have disrupted healthcare delivery, jama report finds," January 2023. [Online]. Available: https:

//www.healthcareitnews.com/news/half-ransomware-attacks-have-disrupted-healthcare-delivery-jama-report-finds#:~:text=From%202016%20to%202021%2C%20the,of%20more%20than%20two%20weeks.

[76] "Emotet." [Online]. Available: https://www.malwarebytes.com/emotet

[77] "Emotet uses coronavirus scare in latest campaign, targets japan," January 2020. [Online]. Available: https://www.trendmicro.com/vinfo/mx/security/news/cybercrime-and-digital-threats/emotet-uses-coronavirus-scare-in-latest-campaign-targets-japan

[78] C. San Carlos, "January 2020's most wanted malware: Coronavirus-themed spam spreads emotet malware," February 2020. [Online]. Available: https://www.checkpoint.com/press/2020/january-2020s-most-wanted-malware-coronavirus-themed-spam-spreads-emotet-malware/

[79] D. Backford and S. Larson, "Exploiting covid-19: How threat actors hijacked a pandemic," September 2022. [Online]. Available: https://www.proofpoint.com/sites/default/files/analyst-reports/pfpt-covid-research.pdf

[80] "United states and united kingdom sanction members of russia-based trickbot cybercrime gang," February 2023. [Online]. Available: https://home.treasury.gov/news/press-releases/jy1256#:~:text=During%20the%20height%20of%20the,hospitals%20across%20the%20United%20States.

[81] "Ryuk ransomware." [Online]. Available: https://www.malwarebytes.com/ryuk-ransomware

[82] "Ransomware ryuk." [Online]. Available: https://www.trendmicro.com/es_es/what-is/ransomware/ryuk-ransomware.html

[83] N. Copppinger, "Netwalker ransomware guide: Everything you need to know," November 2020. [Online]. Available: https://www.varonis.com/blog/netwalker-ransomware

[84] A. O. I. Team, "Take a "netwalk" on the wild side," August 2020. [Online]. Available: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/take-a-netwalk-on-the-wild-side/

[85] M. Novinson, "Equinix breach: 7 things to know about netwalker ransomware attacks," September 2020. [Online]. Available: https://www.crn.com/slide-shows/security/equinix-breach-7-things-to-know-about-netwalker-ransomware-attacks/4

[86] J. Greig, "Fbi, doj say less than 25% of netwalker ransomware victims reported incidents," June 2022. [Online]. Available: https://therecord.media/fbi-doj-say-less-than-25-of-netwalker-ransomware-victims-reported-incidents

[87] "Ddos attacks in the time of covid-19," *Imperva*, 2020. [Online]. Available: https://www.imperva.com/resources/resource-library/reports/ddos-in-the-time-of-covid-19-report-ty?lang=EN&asset_id=3955

[88] "What is a ddos attack?" [Online]. Available: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

[89] L. Abrams, "U.s. health department site hit with ddos cyber attack," March 2020. [Online]. Available: https://www.bleepingcomputer.com/news/security/us-health-department-site-hit-with-ddos-cyber-attack/

[90] "Cyber threats trends: Jan-jun 2020." [Online]. Available: https://www.cdn.neustar/resources/whitepapers/security/neustar-cyber-threats-trends-report-2020.pdf

[91] H. Mahmoud, "Efficientip: New data shows how healthcare suffered from cyberattacks more than other industries during pandemic," July 2021. [Online]. Available: https://www.businesswire.com/news/home/20210708005058/en/EfficientIP-New-Data-Shows-How-Healthcare-Suffered-from-Cyberattacks-More-than-Other-Industries-During-Pandemic

[92] C. C. Ranjit Bhaskar, CISA, "Better cybersecurity awareness through research," May 2022. [Online]. Available: https://www.isaca.org/resources/isaca-journal/issues/2022/volume-3/better-cybersecurity-awareness-through-research

[93] "Proofpoint's 2022 state of the phish report reveals email-based attacks dominated the threat landscape in 2021; tailored security awareness training remains critical for protecting hybrid work environments," February 2022. [Online]. Available: https://www.globenewswire.com/en/news-release/2022/02/22/2388990/35374/en/Proofpoint-s-2022-S

tate-of-the-Phish-Report-Reveals-Email-Based-Attacks-Dominated-the-Threat-Landscape-in-2021-Tailored-Security-Awareness-Training-Remains-Critical-for-Protecting-.html

[94] "2023 state of the phish." [Online]. Available: https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-state-of-the-phish-2023.pdf

[95] "Beware of criminals pretending to be who." [Online]. Available: https://www.who.int/about/cyber-security

[96] M. C. Linda Rosencrance, Peter Loshin, "two-factor authentication (2fa)." [Online]. Available: https://www.techtarget.com/searchsecurity/definition/two-factor-authentication

[97] C. McCart, "15+ two-factor authentication statistics 2020-2022," July 2022. [Online]. Available: https://www.comparitech.com/studies/data-breaches-studies/two-factor-authentication-statistics/

[98] "The 3rd annual global password security report." [Online]. Available: https://lp-cdn.lastpass.com/lporcamedia/document-library/lastpass/pdf/en/LMI0828a-IAM-LastPass-State-of-the-Password-Report.pdf

[99] A. Li, "Google auto-enabled 2sv for over 150m people leading to 50% decrease in compromised accounts," Febreuary 2022. [Online]. Available: https://9to5google.com/2022/02/08/google-account-2sv/

[100] "The state of email security 2020." [Online]. Available: https://www.mimecast.com/resources/ebooks/the-state-of-email-security-report-2020/download/

[101] N. James, "81 phishing attack statistics 2023: The ultimate insight," February 2023. [Online]. Available: https://www.getastra.com/blog/security-audit/phishing-attack-statistics/

[102] "Spam and phishing in 2020," February 2021. [Online]. Available: https://securelist.com/spam-and-phishing-in-2020/100512/

[103] "Coronavirus advice for consumers," 2020. [Online]. Available: https://www.ftc.gov/news-events/features/coronavirus/scams-consumer-advice

[104] "Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016," April 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[105] "Reporting computer, internet-related, or intellectual property crime." [Online]. Available: https://www.justice.gov/criminal-ccips/reporting-computer-internet-related-or-intellectual-property-crime

[106] "Computer misuse act 1990." [Online]. Available: https://www.legislation.gov.uk/ukpga/1990/18/contents

[107] "2021 state of the phish." [Online]. Available: https://www.overleaf.com/project/63ecb81045cae46e2cfe83a1

[108] "Mitigating malware and ransomware attacks," *National Cyber Security Centre*, February 2020. [Online]. Available: https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

[109] "What is endpoint security?" [Online]. Available: https://www.trellix.com/en-us/security-awareness/endpoint/what-is-endpoint-security.html

[110] "Malwarebytes endpoint detection and response." [Online]. Available: https://www.malwarebytes.com/resources/files/2019/11/malwarebytes-edr-solution-brief.pdf

[111] "Corporate endpoint security software market revenue worldwide from 2018 to 2020, by vendor." [Online]. Available: https://www.statista.com/statistics/1170427/market-revenue-endpoint-security-software-products-by-vendor/

[112] "Ransomware protection and response," *NIST*, May 2021. [Online]. Available: https://csrc.nist.gov/projects/ransomware-protection-and-response

[113] "Ataques ddos: aprenda a proteger su red de esta amenaza," February 2022. [Online]. Available: https://odatacolocation.com/es/blog/ataques-ddos-aprenda-a-proteger-su-red-de-esta-amenaza/

[114] "What is network segmentation?" [Online]. Available: https://www.vmware.com/topics/glossary/content/network-segmentation.html#:~:text=Network%20segmentation%20is%20a%20network,services%20to%20each%20sub%2Dnetwork.

ANEXO

OBJETIVOS DE DESARROLLO SOSTENIBLE

Grado de relación del trabajo con los Objetivos de Desarrollo Sostenible (ODS).

Objetivos de Desarrollo Sostenibles	Alto	Medio	Bajo	No Procede
ODS 1. **Fin de la pobreza.**				x
ODS 2. **Hambre cero.**				x
ODS 3. **Salud y bienestar.**		x		
ODS 4. **Educación de calidad.**		x		
ODS 5. **Igualdad de género.**				
ODS 6. **Agua limpia y saneamiento.**				x
ODS 7. **Energía asequible y no contaminante.**				x
ODS 8. **Trabajo decente y crecimiento económico.**		x		
ODS 9. **Industria, innovación e infraestructuras.**	x			
ODS 10. **Reducción de las desigualdades**.				x
ODS 11. **Ciudades y comunidades sostenibles**.		x		
ODS 12. **Producción y consumo responsables.**				
ODS 13. **Acción por el clima.**				x
ODS 14. **Vida submarina.**				x
ODS 15. **Vida de ecosistemas terrestres.**				x
ODS 16. **Paz, justicia e instituciones sólidas.**	x			
ODS 17. **Alianzas para lograr objetivos.**	x			

Reflexión sobre la relación del TFG/TFM con los ODS y con el/los ODS más relacionados.

En mi tesis, he explorado el impacto de la ciberseguridad y los ciberataques en nuestra sociedad desde diversas perspectivas. En particular, mi investigación ha establecido ciertas conexiones con diversos de los Objetivos de Desarrollo Sostenible(ODS) establecidos por las Naciones Unidas. A continuación, describiré cómo ha contribuido a los siguientes ODS: 3, 4, 8, 11, 12, 16 y 17.

ODS 3: La salud y el bienestar son de importancia crítica tanto para las personas como para las comunidades. Mi investigación exploró el impacto de los ciberataques durante la pandemia de COVID-19 y cómo los ciberataques afectaron los niveles de estrés y ansiedad de las personas. El estudio sugiere medidas para combatir los ataques cibernéticos y crear conciencia sobre sus riesgos, así como formas de reducir el estrés de incidentes similares.

ODS 4: La educación de calidad es un pilar esencial del desarrollo sostenible. Mi investigación ha enfatizado la importancia de los ciberataques e identificado varias técnicas de ciberseguridad que pueden ayudar tanto a nivel individual como organizacional. El propósito es fortalecer la preparación de las personas contra diversas amenazas a través de la educación en seguridad cibernética y contrarrestar los riesgos de los ataques cibernéticos.

ODS 8: El trabajo decente y el crecimiento económico pueden verse afectados por ciberataques que amenazan la seguridad laboral y obstaculizan el crecimiento económico. Por lo tanto, se debe enfatizar la importancia de varias amenazas en el lugar de trabajo. Por lo tanto, he propuesto una estrategia para proteger sus activos digitales. Mi objetivo es crear un entorno de trabajo seguro y promover el crecimiento económico sostenible.

El ODS 9: Industria, innovación e infraestructura también están muy relacionados con la ciberseguridad. En mi trabajo, analicé el impacto de los ciberataques en la infraestructura técnica y propuse soluciones para fortalecerla. Al impulsar la innovación segura y proteger la infraestructura crítica se quiere contribuir al desarrollo de una industria fuerte y resistente a ciberataques.

El ODS 11: Ciudades y comunidades sostenibles, es relevante en el contexto de la ciberseguridad ya que los ciberataques pueden afectar a las comunidades. Mi investigación enfatizó la importancia de la protección cibernética en entornos urbanos y sugirió acciones para fortalecer la seguridad comunitaria. Mi objetivo es contribuir a construir comunidades seguras.

El ODS 12: Producción y consumo responsable también se aplica al trabajo, ya que los ciberataques pueden tener un gran impacto en la seguridad de los diferentes productos y la privacidad del consumidor. Al enfatizar la importancia de la seguridad y promover el uso de buenas prácticas en la tecnología, se pretender fomentar una cultura de producción y consumo responsable.

ODS 16: La paz, justicia y las instituciones sólidas son esenciales para garantizar un entorno seguro. Instituciones fuertes y medidas de seguridad son esenciales ya que los ataques pueden acabar con la paz y la estabilidad. A través de mi investigación, he tratado de proponer soluciones para hacer frente a estas amenazas.

Finalmente, el ODS 17: Las alianzas para lograr los objetivos son esenciales para abordar juntos el desafió de la ciberseguridad. En la investigación, se destaca la cooperación entre gobiernos, organizaciones y sociedad en su conjunto, para así fomentar el uso de alianzas estratégicas y promover enfoques interdisciplinarios para abordar los desafíos.

En resumen, mi tesis propone analizo la evolución del COVID-19 desde un punto de vista de la ciberseguridad explorando el impacto y la efectividad de los sistemas en línea. A través de la concienciación, educación y las distintas propuestas que propongo aspiro a contribuir a los distintos ODS.