NOVA IMS Information Management School

MGI

Mestrado em Gestão de Informação
Master Program in Information Management

Smart techniques and tools to detect Steganography

A viable practice to Security Office Department

João Carlos Zêzere da Silva Moura

Dissertation presented as partial requirement for obtaining the Master's degree in Information Management

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação
Universidade Nova de Lisboa

NOVA Information Management School

Instituto Superior de Estatística e Gestão de Informação

Universidade Nova de Lisboa

Smart techniques and tools to detect Steganography

by

João Carlos Zêzere da Silva Moura

Dissertation proposal presented as a partial requirement for the degree of Master of Information Management

Advisor/Supervisor: Professor Doutor Vítor Manuel Pereira Duarte dos Santos

August 2022

AKNOWLEDGEMENTS

First, I would like to express all my gratitude to Professor Dr. Vitor Duarte dos Santos from NOVA IMS for accepting to be my supervisor in this dissertation, giving the perfect guidance from the beginning and being always available to help me achieve this goal. With the guidance of Professor Victor Duarte dos Santos, we planned together the perfect strategy to establish and successfully achieve each milestone throughout this last year.

Secondly, I would like to thank all the participants who helped me in the interviews, not only the interviewers themselves, who helped me to be available to be interviewed and to share their opinions to validate and improve this study, but also my friend Sergio Sousa, who was a key player in inviting some friends to be part of the expert panel.

Finally, and most important, I would like to say a special thanks to my dearest family, my wife Carla and my daughter Sofia, who I lived apart for the past year, dedicating all my energies to develop this study and not sharing with them the time they deserve and for not sharing great moments in family. To my most important people of my life, a special thank for their support and understanding every time I said I couldn’t be available. This work is also their effort in being so supportive, never letting me to break down.

ABSTRACT

Internet is today a commodity and a way for being connect to the world. It is through Internet is where most of the information is shared and where people run their businesses. However, there are some people that make a malicious use of it.

Cyberattacks have been increasing all over the recent years, targeting people and organizations, looking to perform illegal actions. Cyber criminals are always looking for new ways to deliver malware to victims to launch an attack.

Millions of users share images and photos on their social networks and generally users find them safe to use. Contrary to what most people think, images can contain a malicious payload and perform harmful actions.

Steganography is the technique of hiding data, which, combined with media files, can be used to place malicious code. This problem, leveraged by the continuous media file sharing through massive use of digital platforms, may become a worldwide threat in malicious content sharing. Like phishing, people and organizations must be trained to suspect about inappropriate content and implement the proper set of actions to reduce probability of infections when accessing files supposed to be inoffensive.

The aim of this study will try to help people and organizations by trying to set a toolbox where it can be possible to get some tools and techniques to assist in dealing with this kind of situations. A theoretical overview will be performed over other concepts such as Steganalysis, touching also Deep Learning and in Machine Learning to assess which is the range of its applicability in find solutions in detection and facing these situations. In addition, understanding the current main technologies, architectures and users' hurdles will play an important role in designing and developing the proposed toolbox artifact.

KEYWORDS

Data hiding; Steganography; Steganalysis; Image steganalysis; Digital forensics; Deep learning; Machine Learning; Artificial Intelligence

INDEX

1. INTRODUCTION 1

1.1. CONTEXT 1
1.2. MOTIVATION 2
1.3. OBJECTIVE 3
1.4. RELEVANCE OF THE STUDY 3

2. METHODOLOGY 5

2.1. DESIGN SCIENCE RESEARCH 5
2.2. RESEARCH STRATEGY 7

3. LITERATURE REVIEW ON STEGANOGRAPHY 8

3.1. CYBER SECURITY OVERVIEW 8
3.1.1. Basic concepts 8
3.1.2. CIA Triad 8
3.1.3. Impact on the Organizations 9
3.1.4. Areas 10
3.1.5. Threats 11
3.1.6. Detecting and preventing techniques 12
3.2. STEGANOGRAPHY 14
3.2.1. What is steganography 14
3.2.2. Terminology 15
3.2.3. Steganography vs Cryptography vs Watermarking vs Obfuscation 15
3.2.4. History and Evolution 16
3.2.5. How Steganography works – the prisoner’s problem 17
3.2.6. The example of the Least Significant Bit technique 18
3.2.7. Types of Steganography techniques: three different ones 19
3.2.8. Taxonomy 21
3.2.9. Steganography Methods 22
3.2.10. Steganography major threats 24
3.3. TECHNOLOGIES AND PROCESSES TO FIGHT STEGANOGRAPHY 29
3.3.1. Steganalysis 29
3.3.2. Digital forensics 29
3.3.3. Tools and Techniques 29
3.3.4. Indicators of Compromise (IoC) 32
3.4. CHALLENGES AND OPPORTUNITIES 32
3.4.1. Challenges 32
3.4.2. Opportunities 33

4. TOOLBOX OF TECHNIQUES AND SMART AND ADAPTATIVE TOOLS TO CONTROL STEGANOGRAPHY 34
4.1. THE TECHNIQUES AND TOOLS TO CONTROL STEGANOGRAPHY TOOLBOX........ 34
4.2. ASSUMPTIONS........ 34
4.3. WORKFLOW OF IMPLEMENTATION OF THE TOOLBOX 37
4.3.1. Prevention 38
4.3.2. Reaction 39
4.3.3. Collection........ 40
4.3.4. Documentation 41
4.3.5. Update........ 41
4.4. TOOLBOX PROPOSAL........ 42
4.4.1. 1st Strategy - Malware Installation prevention........ 42
4.4.2. 2nd Strategy – using steganalysis tools and techniques 55
4.4.3. Use Cases 60
4.5. EVALUATION & DISCUSSION 77
4.5.1. Evaluation 77
4.5.2. Discussion........ 77
5. CONCLUSIONS........ 80
5.1. SYNTHESIS 80
5.2. LIMITATIONS 81
5.3. FUTURE WORK........ 81

LIST OF FIGURES

Figure 1 – The framework of work according Hevner's approach 5

Figure 2 – The CIA Triad Triangle 9

Figure 3 – Information Hiding tree –Adapted from (Koley, 2016) 14

Figure 4 – Steganography evolution through time – Adapted from (Zielińska et al., 2014) 16

Figure 5 – The Steganography process – Prisoner's Problem – Adapted from (Hashim et al., n.d.) 17

Figure 6 – The Steganography image covering example – Adapted from (*Steganography Definitions*, n.d.) 19

Figure 7 – The Steganography Taxonomy tree – Adapted from (Hashim et al., n.d.) 22

Figure 8 – Toolbox Workflow – Stages of execution 37

LIST OF TABLES

Table 1 – Pros and Cons of each technique (Warkentin et al., 2008) 20

Table 2 – Malware Hiding Techniques (Cabaj et al., 2018) 28

Table 3 – Actions that should be taken in the Prevention Phase of the toolbox 38

Table 4 – Actions that should be taken in the Reaction Phase of the toolbox 39

Table 5 – Actions that should be taken in the Collection Phase of the toolbox 40

Table 6 – Actions that should be taken in the Documentation Phase of the toolbox 41

Table 7 – Actions that should be taken in the Update Phase of the toolbox 41

Table 8 – Actions should be taken to overcome malware infection using Steganography 54

Table 9 – Tools to detect and clean steganographic content files and applications 59

Table 10 – Malware summary through covered scenarios 63

Table 11 – Tools to detect and clean steganographic content files and applications 76

Table 12 – Experts' interviews opinions 79

1. INTRODUCTION

1.1. CONTEXT

Cyberattacks are no longer a new issue. They are increasing every day, regardless of whether their targets are ordinary people, companies, public or government institutes, or even entire countries, as was Estonia in 2007.

Cyber-attacks usually try to perform Data Breach, Cyber-espionage, Data Exfiltration, among others, by taking advantage of the victim. Cyber-crime can be based on some ideology, such as terrorist attacks, to steal information, or even to be the center of the spotlight. These attackers are always looking for new ways to bypass protections and deliver and install malicious software in order to run systems to steal or block data and ask for money for its recovery.

Files sent over the Internet are commonly used to perform such actions. However, because executable files are seen as dangerous, attackers are now using non-executable files, such as images and documents, which are mistakenly seen as safe, and which allow malicious code to be executed on the targeted victim's machine when the file is opened.(A. Cohen et al., 2020)

The internet world has been used as a stage to launch these cyber-attacks by operational groups. But how do they exchange messages with each other in a way that is not intercepted? It is recurrent that messages are exchanged using Steganography (Pope et al., 2012)… a technique that allows messages to be sent inside other seemingly harmless messages. Steganography is always associated to malicious use, although it can be used in the right way as well. (Yedroudj, n.d.)

In conjunction with Cryptography, which is used so that only those by right have access to messages that only concern them, Steganography aims to place information where no one can see it is there (Atawneh et al., 2013). In some situations, steganography is more advantageous than cryptography, and in others, cryptography is used to encrypt the message that is sent within the media file. These techniques are not mutually exclusive. (Steganography - An Experiment in Python, n.d.)

There are some techniques already developed to combat this phenomenon. New scientific methods to address steganography issues, such as the detection of hidden messages using steganography, usually in multimedia files. These methods, called steganalysis techniques, try to gather the evidence about the presence of hidden messages and try to break the security of its carrier. (Johnson & Jajodia, 1998) (Nissar & Mir, 2010). Within the perimeter of steganalysis there are several techniques that help define strategies to combat steganography, where one can find visual steganalysis, statistical steganalysis;, universal or blind steganalysis, and others.. (Karampidis et al., 2018)

Although, and despite the Steganalysis techniques, it is also important to look other techniques reported in another innocent type of files, such as PDF that can be infected, which already is used Neural Networks (Jeong et al., 2019) and Active Machine Learning (Nissim et al., 2019) to address file infection detection. It is important to wonder if those techniques are reliable on this study as well.

Due to its lossy compression, JPEG is the most used image format used by most people and companies, as well in the cyberspace. Due to the perception that JPEG files are harmless, cyber criminals use them to perform attacks. Because of that, there are already several studies that provide to users some Frameworks with some Best Practices to help to detect suspicious image files.

(Kunwar & Sharma, 2017)

But, despite most of its misuse, Steganography may also be used to provide ways of encryption/decryption or authentication to a system(Datta et al., 2021) and there are some cases that it is used for legitimate business applications such as protecting strategic corporate information during transmission (Warkentin et al., 2008).

So more than a technique to hide data and messages; steganography is being used to deliver malware on mobile devices and computers. Cyber-attacks are becoming more and more sophisticated, finding increasingly clever ways of infiltration to bypass all levels of security installed around organizations.

Organizations increasingly need to track all traffic, in transit or at rest, to assess all information passing from outside to inside, inside to outside, and even circulating within the organization. To do so, they have to be equipped with increasingly sophisticated techniques and policies for detection and rapid action against all malicious code and sharing of confidential information.

1.2. MOTIVATION

The problem with cybersecurity is that whatever is defined now, tomorrow is no longer valid. It has a very short period of validity. The forensic practice is evolving in a reactive way, creating mechanisms that allow to respond to the creative techniques elaborated by agents of insecurity and it is not clear how the nations will be able to protect themselves from this phenomenon, which has been widely used by terrorist groups with the purpose of seeking the radicalization of young people in order to join their ranks of fighters and prophets of hate. This is why it is so important to equip security forces with mechanisms that reduce response time in detecting hate messages, the passing of secret information or important documentation. It is important that companies and systems are able to have fast mechanisms to detect tampered images in near real time and that the methods detected are quickly learnt to create barriers almost automatically.

If steganography is the art of hiding messages, steganalysis is the art of detecting then. In recent years, law enforcement and the media have shown some interest in both steganography and steganalysis. (Nissar & Mir, 2010)

With the use of steganalysis it is possible to understand and analyze the tampering of the images. However, the use of defense techniques takes time to be learnt, assimilated and policies created so that a future attack is again effective and quickly responded to.

For this, it will be important to use complementary techniques that can help the world's police to respond almost simultaneously, deciphering messages, blocking contents and identifying criminals.

Artificial intelligence, deep learning and machine learning will be the weapons that can help raise the level of suspicion and be on alert 24x7 on the network and in the exchange of messages between different agents. The improvement in the sophistication of systems to create barriers of defense means that attackers will seek to use situations in which it is permitted to enter the barricade to gain entry at their expense. For this, it will always be important to have a system that immediately detects and quickly learns the defense technique so that it can overcome the human intention of creating disruption.

Additionally, by allowing steganography to send images inside other images, this is a suitable platform for sharing prohibited files, such as child pornography. The following approach will attempt to contribute on techniques aimed at combating the practice of sharing inappropriate digital content and others such as (High Technology Theft Apprehension and Prosecution (HTTAP) Program, 2011).

However, Steganography it is not only a technique to hide messages. Attacks using Malware and malicious code, or like Extortion, Denial-of-service attacks, cyber stalking, and many more can be behind an innocent phot image, video or audio spread in social media.

1.3. OBJECTIVE

The main purpose of this study is to set a Toolbox of techniques and smart and adaptative tools to control Steganography which can be easy to be used for any kind of company.

In order to accomplish this objective, we shall define intermediate objectives like:

- Assess which processes and mechanisms already exist.
- Identify which ones are effective and continue to meet the daily challenge of detecting criminal activity, and which ones will have to be improved and/or eventually considered outdated and replaced by new ones, and which new procedures could be created
- Determine which help Cyber-security techniques, allied with Artificial Intelligence and Machine Learning techniques, can give us in order to be able to act in an almost instantaneous way".
- Build a toolbox of techniques and intelligent tools for Steganography
- Validate the toolbox

1.4. RELEVANCE OF THE STUDY

This study aims to assess the state of the art at this moment. Which tools and which techniques exist to deal with the Steganography problem, either from the point of view of the passage of information, or the capacity of intrusion, breaking the barriers of defense, attack files and with the aim of destruction of the computer systems.

As already referred attackers are always looking for new ways to bypass protections and deliver and install malicious software to run systems to steal or block data and ask for money for its recovery.

The files sent over the Internet are commonly used to perform such actions. But, due to executable files are seen as dangerous, attackers are now using non-executable files, such as images and documents, which are mistakenly seen as safe, and which allow malicious code to be executed on the targeted victim's machine when the file is opened(A. Cohen et al., 2020).

Thus, it is intended to approach new techniques and ways in order to detect and quarantine possible invaders, as well as to have the ability to identify them, being able, or not, to give the ability to alert the authorities.

It is also intended to identify which techniques are in evolution and which ones will only be possible through certain technological evolutions. In fact, to what extent can quantum computing solutions help, or not, the ability to speed up Steganalysis to quickly conceal situations.

Additionally, the aim is to assess what policies can be created for society to start dealing with this type of situation. What are the implications that may result from being exposed to invasion attacks by media files, which may open doors to identity theft, access to privileged information by sending video or audio files?

The large-scale use of social networks and message sharing platforms, in which the sharing of images serves as fait-divers, may open systems and personal equipment. In this way, it is important to create a set of rules and policies that we can all adopt, as we already do in relation to phishing, so that they become part of our lives in order to protect ourselves and our children.

But the battle it is not only focused on the private side of our lives, at home. Organizations fight a continuous battle for control over the user desktop. Employees with admin permissions always try to install unapproved applications if given the opportunity. Likewise, they can install steganography software. The first lines of defense against these practices are – as for any unapproved software – company policies and limiting user permissions, and in a context of COVID19, where most of employees were in lockdown, performing their jobs at home, this control was far from being possible (Warkentin et al., 2008).

Unfortunately, these techniques tent to be heavy to be set up and it would be a good endeavor to evaluate the ability to reduce this technique so that it can be at the level of a mobile phone application and that it can always be available, just like an anti-virus is nowadays.

2. METHODOLOGY

The intended output of this study is a toolbox to be used as a security policy, practice or framework on organizations, and eventually, for anyone who wants to have techniques for avoid malwares on his devices that might be spread through media files. So, considering the March & Smith approach (March & Smith, 1995), the study to be developed will focus on a technique and not on a theory. This leads us to identify that a Design Science Research (DSR) will be developed.

2.1. DESIGN SCIENCE RESEARCH

Hence, and considering having a Cibersecurity problem, where it is important to report the evolution of criminal techniques and the using of new ones, a knowledge base must be used to provide past knowledge to the study to ensure its innovation (A. R. Hevner, 2007).

So, and having Hevner's (A. Hevner et al., 2004) approach as a beacon, this study will start by studying the environment in which Steganography may occur. Basing the study upon it, 5 important steps will be addressed: Environment study; Knowledge Base search; Design, Development & Validation; Application on Organization; Knowledge Base update (A. Hevner et al., 2004)

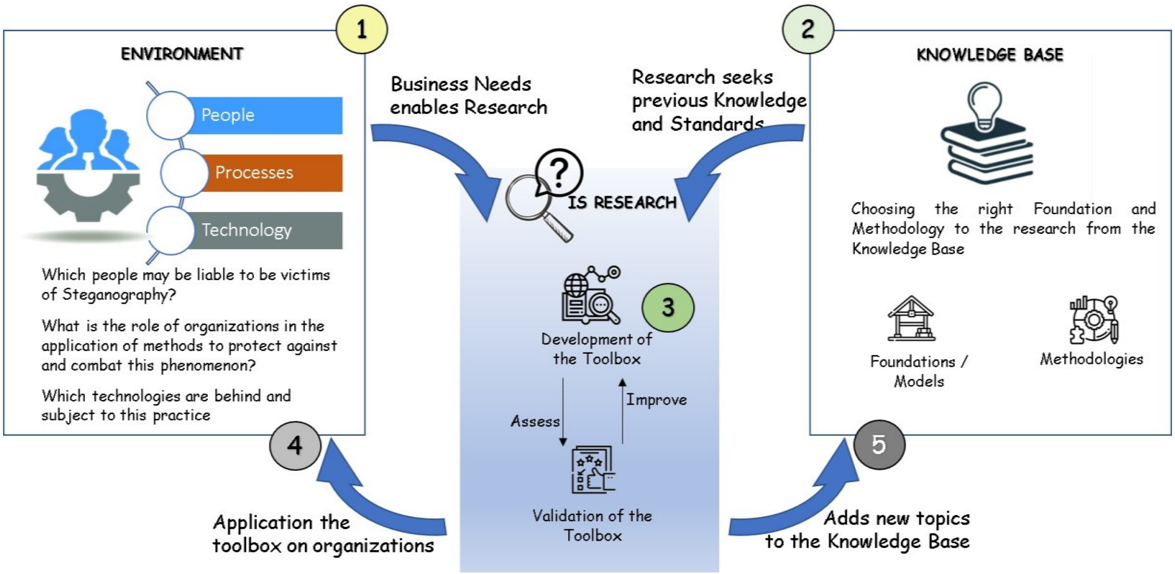
1
ENVIRONMENT
People
Processes
Technology
Which people may be liable to be victims of Steganography?
What is the role of organizations in the application of methods to protect against and combat this phenomenon?
Which technologies are behind and subject to this practice
Business Needs enables Research
Research seeks previous Knowledge and Standards
2
KNOWLEDGE BASE
Choosing the right Foundation and Methodology to the research from the Knowledge Base
Foundations / Models
Methodologies
IS RESEARCH
3
Development of the Toolbox
Assess
Improve
Validation of the Toolbox
4
Application the toolbox on organizations
5
Adds new topics to the Knowledge Base

Figure 1 – The framework of work according Hevner's approach

Step 1 – Environment Study

In the first step it will be necessary to assess common problems of the environment. Who is eligible to be a victim of Steganography? Which are the real problems to organizations? In this phase it will also be needed to assess which technologies and processes are already in place to fight Steganography and which are the main problems technologies and processes face. It will be in this phase, where the Literature Review will be done the and the Research Question will be found.

The focus will always be on the search, identification, and delimitation of the need, setting a perimeter of action. Additionally, it is important to assess which techniques and practices are already used nowadays to fight this situation, namely, which foundations and methodologies are companies using worldwide. It is important to assess everything that is done at a global level in order to select the best practices.

Step 2 – Knowledge Base Research

At this stage it will be wondered what Methodologies and Foundations will be needed to be used to address the techniques to deliver the proper toolset. Which standards can be addressed to develop the toolbox.

Step 3 – Design, Development & Validation

Based on previous two aspects, and with the definition of a well-defined perimeter, an artifact will be created that will try to respond to the needs of organizations regarding the systematic control of on transit contents. Naturally, all its development will be validated as a product and, consequently, refined to become a better solution. In the IS Research phase. This phase, referred as Step 3 will be separated in two recurring minor phases: the development itself, where new processes, techniques and technologies will be developed to address Steganography issues, and the validation of the toolbox. The Validation subphase will evaluate the quality and the capacities of the toolbox and all the needed improvements will go back to the Development subphase. No product is a good product without intensive testing and validation, so the last half of the 3rd stage will be dedicated the toolbox validation in order to refine all the goals achieved.

Steps 4 & 5 – Application on Organization & Knowledge Base update

Finally, when the toolbox should be ready, it should be installed on organizations (Step 4) and the Knowledge Base shall be updated with new techniques and foundations (indicated as Step 5).

2.2. RESEARCH STRATEGY

The research strategy has to follow the logic of our DSR Methodology. Like it was stablished for step 1 it is intended to assess the environment about how Steganography affects companies. It will be assessed major dangers and risks due to Steganography. Like it will be seen in further chapters, Steganography can be a vehicle for infection and intrusion, taking the C&C of the servers, as well as a critical way for data exfiltration which can lead to industrial property robbery, identity theft and data breaching.

The goal of the second phase of the study is to obtain the state of the art. To highlight what is already known about Steganography and how researchers have approached it. How it has been developed in recent years as well the ways to detect it and to fight it. For this second stage it is critical to select accurate articles that can certify the scientific basis of the study. This selection it will based on worldwide known scientific publications databases and on scientific workgroups.

These articles and publications will be the base for having a critical overview of the existing knowledge and to find out what is missing. It will be based on this scenario that it will be pointed out major dangers and risks due to Steganography and which tools and techniques could be addressed to face the problems generated by Steganography. Somehow it will be addressed Steganalysis and Digital Forensics which are tools to detect and to get evidence of malicious use.

The strategy of the analysis will be chronological, starting from older publications, looking for definitions and the early days of steganography and its evolution towards today, especially the evolution of the threats and the technology which is used to cover steganography.

The Design of the toolbox will be outcome of the gathering of the current tools and techniques which can help companies to set strategies in order to deal with steganography. In Cybersecurity there are always two ways to face cyberattacks: one it's using technical methods like investing in technology and software, and the other one is investing in human capital, like awareness to employees and well-trained cybersecurity teams. The toolbox will comprehend both subjects.

Will the approaches of the toolbox reliable? That is what the last stage of this study will try to figure out by asking to some elected companies SOC's to validate. Remember that a SOC (Security Office Center) is team comprehended with members from company other teams, technical as well strategic

3. LITERATURE REVIEW ON STEGANOGRAPHY

3.1. CYBER SECURITY OVERVIEW

3.1.1. Basic concepts

Cyber Security is a way of performing protection of the assets over the cyber space.

According to NIST, Cyberspace means: "A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.", while Cybersecurity is "The ability to protect or defend the use of cyberspace from cyber attacks."(Paulsen & Byers, 2019)

However, protecting assets concerns not only to protect infrastructure, especially servers and terminals. Beyond infrastructure there is information which it needs to be protected. Information is the companies and countries most valuable asset. Infrastructure can be replaced for brand new one, whereas information is irreplaceable. Moreover, information leak gives an advantage to competitors. According to Benjamin Disraeli, a former Prime Minister of the United Kingdom, stated that:

> "As a rule, he or she who has the most information will have the greatest success in life."

In other words, one of most important aspects of Cybersecurity is regarding the protection of the information. Looking again to NIST definitions, Information Security is "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability."

Criminals are always one step ahead and looking for new breaches and creating new ways to perform their attacks, although, governments and researchers are always trying to anticipate new problems to prevent new ways of being attacked.

3.1.2. CIA Triad

CIA Triad defines the three main goals of protecting the information. Like a triangle that is meant to keep in balance through three vertexes, CIA comes from (European Union Agency for CyberSecurity/Threat and Risk Management/Glossary, n.d.):

- C - Confidentiality: to keep information private and safe from unauthorized access
- I - Integrity: to keep data protected from modification, deletion or tampering from any unauthorized party
- A - Availability: to unsure its fully availability anytime and anywhere to authorized parties

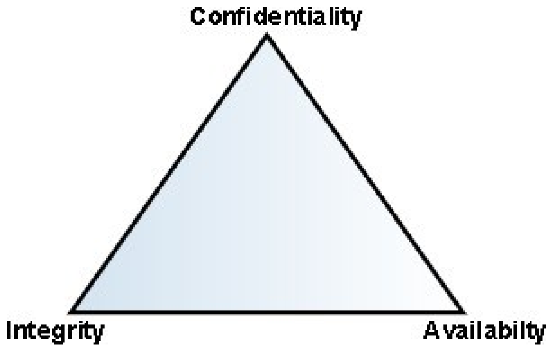

Figure 2 – The CIA Triad Triangle

All Cyber security on information systems is a balance between these three topics.

3.1.3. Impact on the Organizations

Cybersecurity has become a critical issue in organizations, not only derived from the disruption they can cause, especially regarding infrastructure and virus spreading, but also to steal industrial property and classified documents for organizations and particularly about companies' strategic information.

A lack of Cybersecurity affects, firstly, the organization itself. What it should have been done that wasn't done to protect the company? In many ways, this a question that affects the company.

Secondly, there are always financial implications due to its production have been disrupted, the bank account had been assaulted or, eventually, it can be asked for a payment to rescue compromised infrastructures.

Finally, Cybersecurity evolved to be a matter of warfare, which companies are being carried out to the warfare field as pawns.

3.1.3.1. Organizational impact

The most important thing for a company is not to lose control of their systems. They must maintain a high state of awareness of their infrastructure to detect intrusions in order to protect themselves and react in the event of an attack. Loss of control will affect the company's business and revenue, either by directly affecting their operation and reducing, or even disabling their ability to produce goods and services due to the disruption of the physical infrastructure, or by stealing intellectual property and counterfeiting their products.

A lack of cybersecurity allows to cybercriminals to control the company. To face cyberattacks companies must be prepared with tools and techniques to get the control back and fight back the attack. Moreover, it will be important to show to the attacker that company is well prepared to face the attack in to order to go back to a normal situation.

3.1.3.2. Financial impact

Cyberattacks affects tremendously companies, not only because they stole on their bank accounts or through a ransomware, through the impossibility of production of goods and services, or eventually through their intellectual property, but because of reputation damage it may cause.

Even Cyber incident assurances tends to rise the annual price after a security incident, and to the assurance company it affects the companies rating regarding Cybersecurity performing.

3.1.3.3. Strategical impact

Cybersecurity has become a key element for the development of any company and any country. Nowadays it has become a weapon of warfare, which no longer will be made with cannons and bullets, but with the theft of information and in the domain of critical infrastructures.

Has the Power who controls what others' needs. The one who can control what an organization needs controls the company and cyberattacks can take the advantage of controlling companies' servers and their infrastructure which is critical to their businesses.

Cybersecurity has already changed the paradigm of warfare. The arsenal of weapons is no longer a measure of power. As an example, weapons from USA are more powerful than North Koreas'. However, due to cyberwarfare, North Korea has the ability to cause more disruption in USA than in the other way around. Disabling a power plant has much more impact in USA than it has in North Korea, because most of North Koreans only have electric power on their homes for short periods of time during the day. Additionally, cyberattacks can be deployed from anyplace in the world… it is not necessary to take place from a country with so few IP addresses like North Korea is.

Organizations are always the first line of defense of a country. They are the first to face the consequences of a well-planned cyberattack. There are always situations drawn to attack civilians and small businesses, which its intention is to scam and to steal using phishing to access bank accounts, ransomwares to extortion, data breaching to perform sextortion, among others.

However, cyberattacks to companies are more comprehensive because companies can be used as part of strategy performed from a Nation State with the proper resources to defeat companies' lines of defense, to get classified information or to disrupt its operation in case of critical infrastructures. Moreover, companies are not allowed to respond to attacks because cyberdefense actions are restricted to law enforcement like National CERTs and Cyberarmies.

When a country is attacked in a conventional way, he has the right to respond. However, in case of a cyberattack to a company it is hard to define which approach should be taken: it should be seen as an attack to the company, from the criminal point of view, or an attack to the country through that same company, which this last hypothesis can be seen in the military point of view. So, in many cases, governments try to not to act on behalf of the attacked companies because it is too hard to get evidence of the purpose of the attack. (Sanger, 2019)

3.1.4. Areas

Cybersecurity is always about intrusion to an oblivious infrastructure to take advantage. That advantage can be data breaching, espionage, intellectual property robbery or even taking control of the entire infrastructure to ask for a ransom. So, security to intrusion can be defined through three vectors:

3.1.4.1. Cloud Security

Cloud security concerns about technology, protocols, and best practices that protect cloud computing environments, applications running in the cloud, and data held in the cloud.

Cloud-based data storage has become a popular option over the last decade due to its enhanced privacy so, this Is a matter of cyber security dedicated to securing cloud computing systems, by keeping data private and safe across online-based infrastructure, applications, and platforms, whether the client that use them is an individual, small to medium business, or enterprise uses. (Kapersky's Resource Center/What Is Cloud Security, n.d.)

3.1.4.2. Network Security

The objective of this area is to develop procedures to protect networks and data against breaches, intrusions, and other threats. The procedures in this area involve hardware and software solutions, as well as processes or rules and settings regarding network usage and accessibility.

It usually involves access control and the use of security software, such as viruses and antivirus, application security, network analysis, as well as firewalls, VPN encryption and others .(Check Point/Network Security, n.d.). Usually, network security is considered the most important part of Cybersecurity, where a set of hardware and countermeasures can be defined.

3.1.4.3. Application Security

Application security is the features within applications in order to prevent security vulnerabilities from threats. These threats can be unauthorized access and modification.

Intrusion on the system will always take advantage and try to use applications to get the control and access the information. If those applications are not robust to block the intrusion, data will be stollen.

So, application security is another layer of defense which, combined with Zero Trust policy, it will block the access to sensitive information.

3.1.5. Threats

There are several threats that can be installed on system, like:

- **Malware**: application with the purpose to intrude on a machine to data breach financial details, to classified and sensitive corporate or personal information. There are several types of them.
- **Virus:** It is a program that can be replicated by changing existing programs on the system with its own code, and which spreads through all systems and network, corrupting and destroying data and file systems.
- **Worms:** A stand-alone program that can be propagated and run independently of other files. It differs from viruses that need a host program to spread. Its main purpose is to reduce computational power and network bandwidth, slowing down the system.
- **Trojan:** Acting like the Trojan Horse, it seamlessly enters the organization pretending a real application. Installs a backdoor program that creates an entrance for attackers to steal users'

credentials, credit card credentials, and more. (R. Cohen, 2019)

- **Spyware:** Virus that collects user information without the user's knowledge or consent. It is usually used to perform advertising or malvertising directly to the user and considering the user's preferences.
- **Adware:** It redirects users' search requests to advertising websites. It also collects users' marketing data to customize advertisements to display to users based upon their searching profile.
- **Ransomware:** It acts like a Trojan and its main purpose is to encrypt data from computers, making the organization's system unusable. Usually, companies have to pay a ransom to get the key to decrypt access, but there have been some infections just to cause disruption, without any ransom to decrypt the key.
- **Command and Control (C&C; C2) attacks:** usually placed in a server by an attacker to send commands to compromised computers or other servers, usually infects using a malware, and to steal data. This kind of attacks can compromise an entire network. ("Command and Control [C&C] Server," n.d.); ("Command and Control Explained," n.d.)
- **Exploit kits (EK):** Is an automated threat that scans for vulnerabilities on browser-based application and to run malware. Its main purpose is to, automatically and silently, exploit vulnerabilities of a user computer while his browsing the web. EK usually start with a website that was compromised. That page will silently divert web traffic to a landing page.("What Is an Exploit Kit?," n.d.)
- **RAT (Renote Access Trojan):** Remote administration tool. Includes a back door to take the administrative control of a targeted computer. After its infection, the cybercriminal can take control of the web cam, access confidential information, format drives, etc ("RAT (Remote Access Trojan)," n.d.)
- **Malvertisement:** infected online advertisement. Ads hosted in malicious as well as legitimate sites, and social networks. After hitting a malvertisement, the system is infected with a malware. ("Malvertisement," n.d.)
- **FAKEAV:** Fake Antivirus: malware cheat users saying their computers are infected and persuade them to acquire fake antivirus software. To be more convincing the malware shows a fake scanning result (Celestino, 2012)
- **Spear phishing:** Whereas phishing random individuals, spear phishing is a phishing method that targets specific individuals or groups("Spear Phishing," n.d.)
- **APT – Advanced Persistent Threat:** States-sponsored malware and attacks and tends to be active for a long of time. Usually they are more sophisticated and require more knowledge and skills to execute them("What Is an Advanced Persistent Threat (APT)?," n.d.), ("APT [Advanced Persistent Threat]," n.d.)

3.1.6. Detecting and preventing techniques

Most techniques to detect and to prevent intrusion are regarding hardware. They usually are programed in the integrated chips. But technology does not solve everything whatsoever.

Technology must be combined with reliable countermeasures as well. Additionally, investment on technology must be done on reliable vendors. Technology it is not all the same and some may have vulnerabilities.

3.1.6.1. Types of Network Security Protections

There are several types of Network protections that a company can use to prevent intrusions on its systems. Systems team usually uses tools and techniques with that purpose, like:

- **Firewalls**: controls all network traffic (inbound and outbound), based on a set of preconfigured rules
- **Network Segmentations:** divides the network into smaller segments, defining boundaries between them, and where its assets are grouped by function, risk, or role.
- **Access Control:** Set of rules and hierarchies where is defined who (people or groups and the devices) have the access to network applications and systems. It can be defined in the company's Active Directory or LDAP protocol.
- **Remote Access VPN:** encrypted, remote access to the company network from the outside, allowing users access to perform actions on systems from outside the company's computing infrastructure.
- **Zero Trust Network Access (ZTNA):** Policy that reduces user permissions to what the user should have access to in order to perform his job
- **Email Security:** Best practices and technology applied to protect e-mail accounts and their content from malicious threats
- **Data Loss Prevention (DLP):** Combination of best practices and technology in order to prevent data breaching and data exfiltration, especially on sensitive data such as personally identifiable information (PII) and in compliance with some regulatory rules such as: PCI DSS, SOX, HIPAA, etc.
- **Intrusion Prevention Systems (IPS):** Technology to prevent, or even detect, network security attacks. Denial of service and brute force are the best known, but the list has more types of attacks to exploit network vulnerabilities.
- **Sandboxing:** special and isolated environment where the code can be run or files can be opened safely. Usually, Sandboxes are on machines that mimics end-user environments.
- **Hyperscale Network Security:** capability to scale out the architecture in order to fulfill the system needs.
- **Cloud Network Security:** Applications and workloads that are hosted on cloud data centers and out of companies on-premises environment.

3.1.6.2. Types of application security

Applications use in general some techniques to prevent protect and prevent the access by unauthorized users. Some examples of those security features can be seen in the home banking app, either in the internet browser and the cell phone app, which perform some actions in order to ensure that the one is attempting to use it is the one who really should.

The first important feature is Authentication. This feature is responsible for checking whether the user is authorized to access to the application. User must provide credentials that should be validated to a database where users are registered. Usually, these credentials are complemented with another factor, like a code retrieved from the user's cell phone in order to improve the level of security with another security layer.

The second feature is Authorization, where the user is validated whether is authorized to have access to all features of the application or to only some parts of it. Sometimes some menus of applications are disabled depending on the user's level of access. For instance, a user with reader access usually cannot save new documents. Authorization comes always after Authentication

Encryption is a security measure very useful during the usage of the application to protect sensitive data from being seen for a cybercriminal. Such data in transit, like in cloud-based applications where data travels between user and the cloud, and at rest, like in filesystem, must be kept encrypted to prevent it being read. They can be accessed, or even stolen, but using good encryption technique, they can be kept secret.

To register who accessed data, a logging technique can be implemented to record all actions taken when accessing the data. Only with this method systems can be audited in order to assess who got access to data and how.(VMWare/Application Security, n.d.)

3.2. STEGANOGRAPHY

3.2.1. What is steganography

Steganography is a subdiscipline of hiding information and contrary to what one might think, it is a very old technique for people to communicate with each other in such a way that third parties cannot understand or even guess that people are transmitting hidden information. Its main objective is that no one notices that there is a hidden message in a seemingly normal message. Otherwise, using a message encrypted with a code is easily recognized as a transformed message so that only those who know the decryption key can translate the message.(Johnson & Jajodia, 1998)

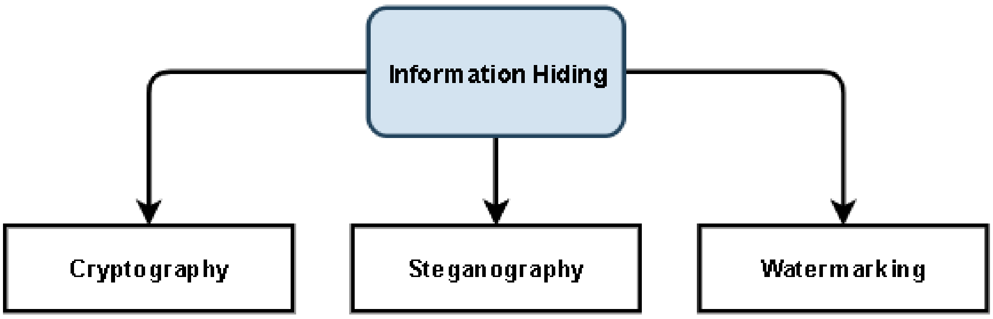

Figure 3 – Information Hiding tree –Adapted from (Koley, 2016)

Steganography comes from the Greek words "Steganos" = Hidden + "Graphia" = Writing, which means "covered writing" (Petitcolas et al., 1999). It allows the sending of undetectable messages embedded in other innocent-looking files, known as carriers. Carriers can be images, audio, video, text, or any other digital mean.

3.2.2. Terminology

There are some new terms used in steganography that shall be introduced and which will be used in the rest of this thesis:

- **embedded data / Steganogram:** message that one wishes to send secretly (Petitcolas et al., 1999)
- **Covert channel:** Channel used to hide data in legitimate transmissions
- **Steganography bandwidth:** amount of secret data one is able to send per time unit. (Cho et al., 2019)
- **Undetectability:** inability of someone to detect a steganogram within a carrier. (Cho et al., 2019)
- **cover-text / cover-image / cover-audio:** innocent-looking object that is used to place embedded data (Petitcolas et al., 1999)
- **Stego Object:** Cover object + embedded data
- **stego-key:** Object used to control the process. It as to restrict detection and recovery of the embedded data only to those who are part of the communication.(Petitcolas et al., 1999)
- **size of the payload:** amount of embedded information that can be hidden (Johnson & Jajodia, 1998)
- **Robustness:** Amount of changing that steganogram can withstand without destroying the secret data. (Cho et al., 2019)
- **Exploit kit:** is a silent threat used to spread malware by attacking system weaknesses

3.2.3. Steganography vs Cryptography vs Watermarking vs Obfuscation

The major concern of cryptography is regarding protecting the content of the message, while steganography tries to hide its existence. In another words, biggest difference between them is that on cryptography it is not possible to read the message while in steganography it is not even possible to see that there is a message to read.

On the other hand, watermarking is the practice of altering a media in order to hide information regarding that media. It is very useful to protect intellectual property by embedding watermarks in media for confirmation of payment of its use (Atawneh et al., 2013).

Finally, and another term that can confuse users is Data Obfuscation, which is different from Data Hiding. Whereas Data Hiding attempts to hide data in a way that no one can see it, Data Obfuscation attempts to replace data to look like real data, making it useless to cybercriminals. This technique is largely used to avoid censorship. (What Is the Comparison between Steganography and Obfuscation in Information Security?, 2022)

3.2.4. History and Evolution

Like it was previously said, Steganography is a very ancient technique firstly referred on Ancient Greece. Herodotus reported how king Darius used by shaving a prisoner's scalp and wrote a message and, after the hair was grown, he was sent to the king's son-in-law Aristogoras in Miletus to deliver the message undetected by the enemy. And how Demeratus thought to send a message Xerxes, King of Sparta, who was planning to invade Athens, by removing the wax of tablet, writing in the wood, and covering it again with wax.

Romans had the idea of sending messages by writing between the lines of innocuous documents with invisible ink made from urine, milk, or juice fruits. When the document was heated, the ink would darken and the message it would be visible. (Warkentin et al., 2008)

The Middle Age brought new techniques and the first use of Linguist Syntax and Semantics that relied on the manipulations on the written as well on spoken language with the aim of tricking the perception of who was receiving the message.

Until the XX century many techniques were developed like writing in an eggshell, in the Renascence, or using music scores, during Age of Enlightenment, or even newspapers in the XIX century. During the XX century many new techniques were developed leveraged by World War I and II and the Cold War, including one based on cryptographic ciphers for putting steganograms into messages, which was intended to insert content into digital signatures.(Zielińska et al., 2014).

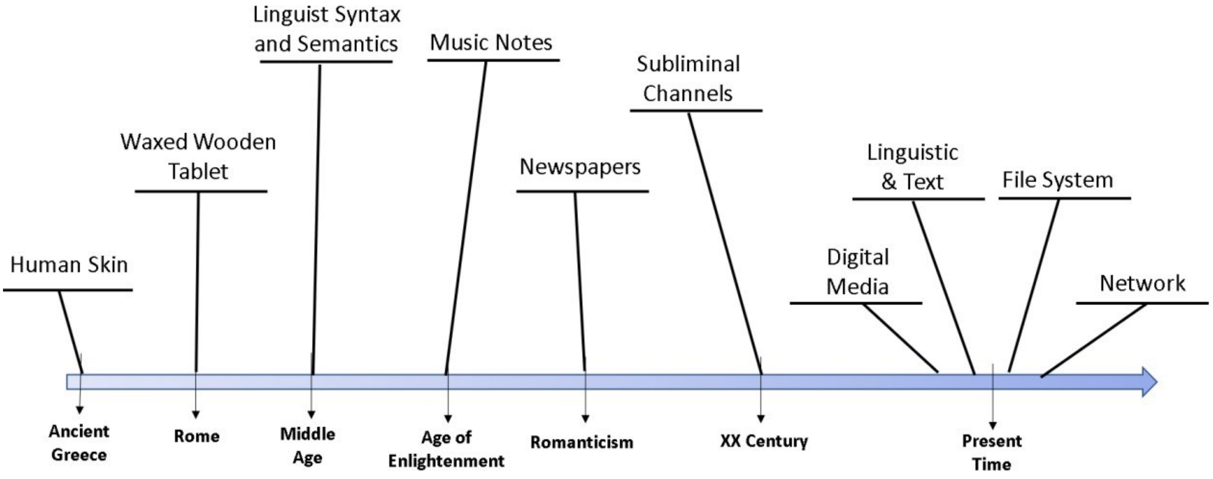

Figure 4 – Steganography evolution through time – Adapted from (Zielińska et al., 2014)

3.2.5. How Steganography works – the prisoner's problem

The framework was firstly introduced as a framework by Gustavus Simmons in 1983 in the Prisoner's Problem (Simmons, 1984) where it was explained why it is needed a covert channel to communicate in a way that no one can detect. The introduced scenario refers two prisoners, Alice and Bob, each one isolated in his cell that want to communicate with each other to plan their escape without the Warden notices it.

Bob and Alice are locked in each cell having their personal computers to communicate to each other but over a network monitored by the warden. If they try to encrypt their communication, the warden will notice they are trying to communicate in a way that warden can't find their plan to escape and send them to solitary.

However, Alice and Bob share a secret between them in a such way that the warden can't differentiate normal communication from covert communication.

Alice places the secret message "M" inside the cover object "C" with the help of the Stego key "K", obtaining the Stego object "S". After that, the "S" is sent through a public channel to Bob. The procedure is shown below:

- The Cover Object "C" is an innocent-looking and unsuspicious object used to embed the data which is to be concealed
- The secret-Key "K" is the key to encode and decode the Message "M"
- Stego-Object is the outcome after embedding the Message "M" into the Cover Object "C" using the Stego-Key "K"

Prisoners' intention is to send the message to each other without the warden realizing it. They hardly expect that the Warden won't get the difference between cover object and stego object. because if the Warden has some steganalysis techniques to extract the secret message from the stego object he can analyze and get the Alice and Bob's escaping plan. (Hashim et al., n.d.).

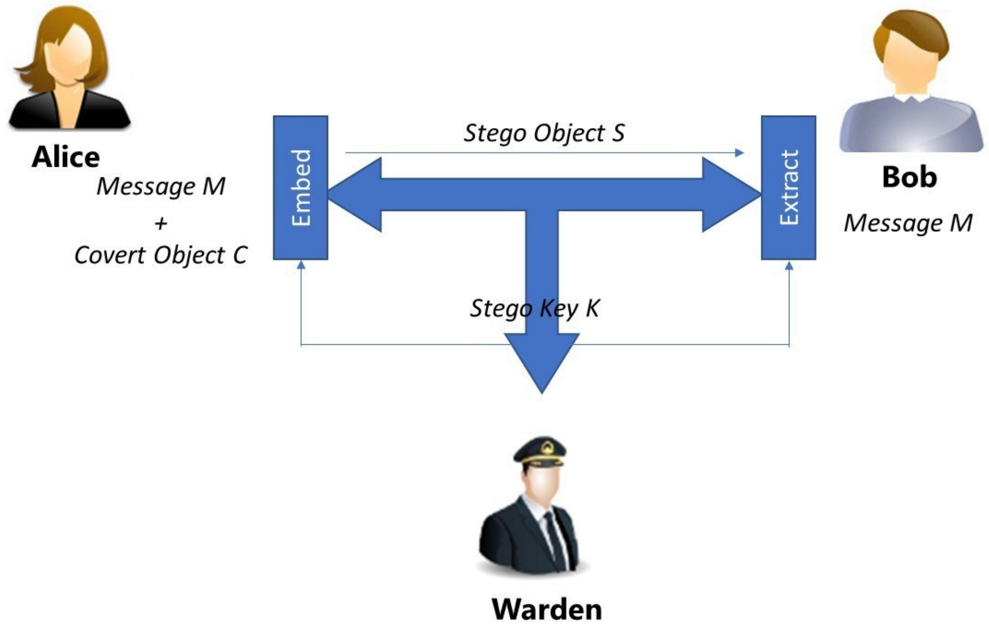

Figure 5 – The Steganography process – Prisoner's Problem – Adapted from (Hashim et al., n.d.)

3.2.6. The example of the Least Significant Bit technique

The most popular technique used to hide information is inside of images. This happens because pictures are very likely to be innocent looking and harmless and bringing to people who are seeing them a sense of joy.

Giving a small example how Steganography can mean a serious way if concealing messages using a carrier, replacing the least Significant Bit of each pixel of an image file, it is possible to change 3 bits of information, given that each pixel has 3 bytes of information for the RGB channels. The Least Significant Bit is the last one of a byte, which changing each LSB of each 3 channels of a pixel it won't make any difference to the naked eye. For instance, considering the following color encoding:

10010101	00001101	11001001	🟪	RGB (149; 13; 201)
00011101	10111101	01001111	🟩	RGB (29; 189; 79)
11101011	11111000	01000110	🟨	RGB (235; 248; 70)

The LSB algorithm can hide the following nine bits **000000011** by changing the last bit in each octet as needed. This results in:

1001010**0**	0000110**0**	1100100**0**	🟪	RGB (148; 12; 200)
0001110**0**	1011110**0**	0100111**0**	🟩	RGB (28; 188; 78)
1110101**0**	1111100**1**	0100011**1**	🟨	RGB (234; 249; 71)

This example shows that changing nine LSB does not change colors at first glance whatsoever. Changes are imperceptible to the human eye.

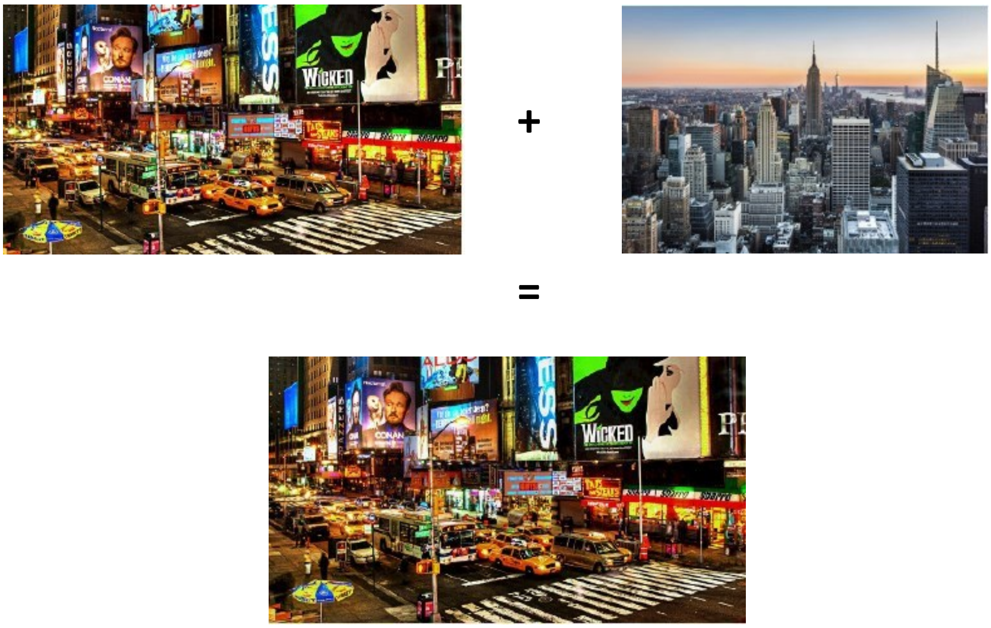

Figure 6 – The Steganography image covering example – Adapted from (*Steganography Definitions*, n.d.)

Images may not only bring other images inside, but also malware code, and steganography can happen through different covert channels and using different types of techniques to hide information.

Finally, LSB is not only applied on images, but it can also be used all digital media, since they can be represented in octets. So, the longer is the representation of the information better payload capacity the file has, and more information can be concealed.

3.2.7. Types of Steganography techniques: three different ones

It is possible to embed information in inside a carrier file with three distinct methods. types of methods. Information can be injected, not altering the digital content of the carrier file. Alternatively, part of the content can be substituted with the message. Finally, the last method proposes a change of the content, generating a completely new file.

3.2.7.1. Injection Techniques

The cover object and message can be part of the file without changing its structure in any small part or the whole file. Some examples of this technique include storing data in unused space in file headers, data packets sent over networks, and unused disk space (Warkentin et al., 2008). In other words, the overall format of the file Is easy to put information in reserved space. Although it is also easy to detect it since the location of empty file space is usually known. Other big problem of this technique is that capacity is limited, and some new techniques tends to force to have some modification of the carrier file (Pope et al., 2012).

3.2.7.2. Substitution Techniques

In this technique, a small amount of the cover file is substituted with the hidden message. One big example of this technique is the Least Significant Bit which uses the structure of an image to be carrier if the message, changing a little information in it. The LSB technique will be better explained in one of next chapters. (Warkentin et al., 2008)

3.2.7.3. File Creation

One last technique is to create a new, unsuspicious file, where the hidden information originates its own carrier, like it could be seen in the application SpamMimic.

The message can easily be hidden in the text. However, this technique is rather inefficient because it tends to enlarge original files. For instance, the sentence of three words "steganography is interesting" is converted in a text file with a word count of 574, despite being a less suspicious technique. (Warkentin et al., 2008)

3.2.7.4. Comparison between techniques

In the following table there is a side-by-side comparison about these three different techniques.

Technique	Method	Carrier File	Comments
Injection	Information hidden on "open" file space	No change on the file	Limited by the space available on the file
Substitution	Part of the content is replaced by the hidden message	Some degradation of the quality, especially images and audios	Limited by the file size which to be detected in case of largely increasing of its size
File Creation	Hidden message is placed into the new file, increasing its size	New carrier file is generated	Extremally inefficient

Table 1 – Pros and Cons of each technique (Warkentin et al., 2008)

3.2.8. Taxonomy

Steganographic techniques were developed alongside the computers and networking development. Four main branches evolved from that development and which were: digital media; linguistic; file system; and network steganography (Zielińska et al., 2014). In fact, it can be classified into two different main categories: technical and linguistic. While technical steganography uses investigative procedures to hide information (M. Khan et al., 2015), linguistic steganography utilizes natural language text as way of hiding information, using mostly synonym substitution (Chang & Clark, 2014).

On the other hand, technical steganography has two areas, which are the Cover, regarding the mean that the message can be concealed, and the Method, which is the technique used to conceal the message into the Cover.

In the Cover branch, secret contents are embedded in carrier file, like image file, to hide that contents without a distorting the carrier file and by using one of six types of steganography mechanisms: image; audio; video; text; DNA; and protocol (Hashim et al., n.d.).

In fact, image, audio, video steganography can be aggregate in Digital Media Steganography, which use techniques to change bit representation of information, turning innocent looking media files in carriers of malware and other malicious information, whereas text steganographic methods uses syntactic and semantics structure of the text as a carrier, such as displacement of punctuation marks or word order. In Text Steganography, some SPAM messages can be used as a carrier, due to the large amounts of such mail emitted every day (Zielińska et al., 2014).

Another way of Steganography is File Steganography, and it was firstly proposed by Anderson, Needham, and Shamir, where information can be embedded even in isolated computing environments. This was designed to give the user a very high level of protection (Anderson et al., 1998).

Later trends of steganography, more robust and effective because they have a higher payload capacity are DNA Steganography and Protocol or Network Steganography, especially the last one since it is not permanent, like in Digital Media, which is limited by the size of file, in network transmission steganography is always happening.

DNA Steganography is a data hiding technique using DNA sequences. Despite the algorithms proposed in image steganography to embed information are good, its capacity it is not very high, and they cannot conceal large amount of data, DNA steganography has been proposed to overcome that lack of the capacity. Using DNA sequences as carriers, critical data can be sent by encrypting and hiding messages in a large number of DNA strands, preventing messages from being read and deciphered by adversaries. (Al-Harbi et al., 2020).

Finally, another fast-developing field in terms of steganography is Network Steganography which exploits the protocols of the OSI reference model. The methods may use several protocols simultaneously, modifying of their properties to embed steganograms, usually in packets header. As stated earlier, network steganography has some advantages over digital media. Digital media are limited to the size of the carrier file, whereas the network, despite it can be much slower than digital media, allows data to leak for longer periods of time. Even worse than that, if no one notices that traffic is being exchanged and captures it, there will be nothing left for forensics to analyze because it leaves no evidence and cannot be traced. It should be noted that network methods are much more difficult to detect and to remove from networks (Zielińska et al., 2014).

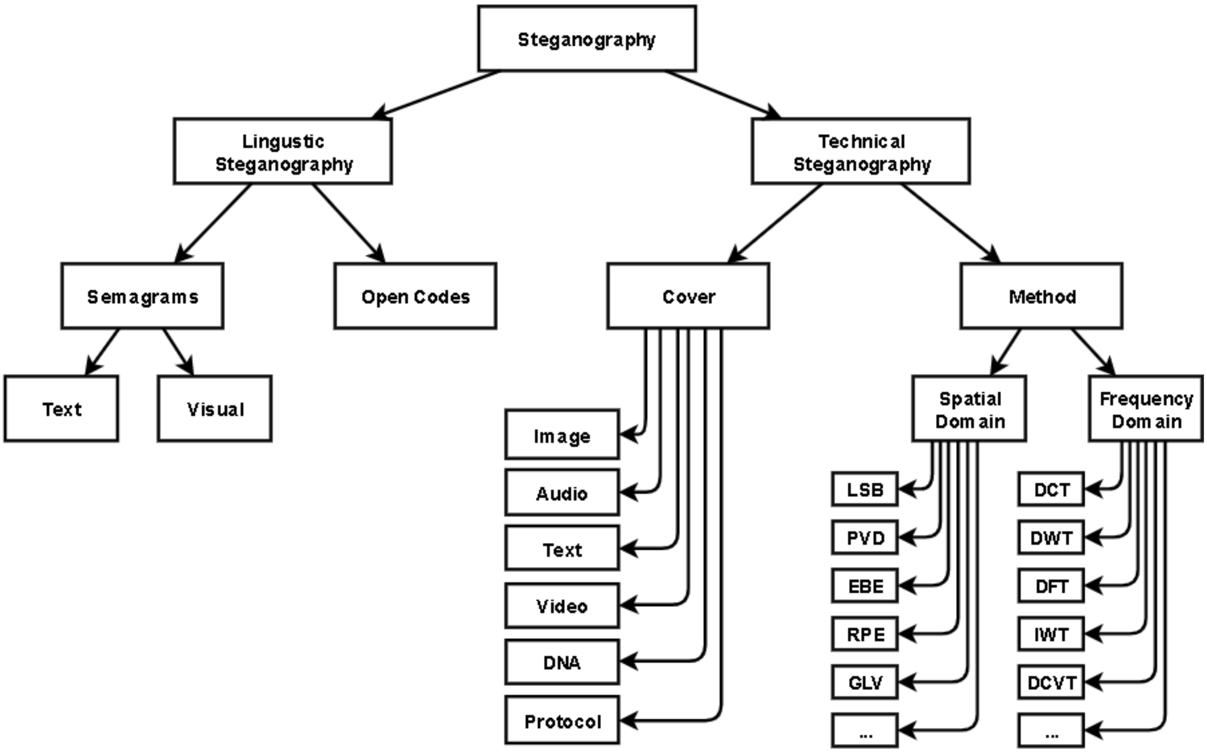

Figure 7 – The Steganography Taxonomy tree – Adapted from (Hashim et al., n.d.)

In the Method branch, especially regarding to the Image Cover, steganography techniques are classified in two different kinds, like spatial domain and frequency domain.

The spatial domain is to be applied directly on all the pixels of the image file, and there are several methods which can be used for this purpose: LSB (matching and substitution), Gray level modification GLV, etc, which are simple to use and have been utilized in a significant number of steganography applications. However, they cannot be used in files which utilize compressed formats, because they have lesser information, and its detection is easier to get. There is always a trade-off difficult to get between capacity and size: to be transferred over networks, files are either small (having low payload capacity) or compressed. Compressing files can lead to a destruction of the hidden data, so it is preferable to use frequency domain, like it is used to JPEG files.

The frequency domain method incorporates the secret message by converting the image into frequency domain (Hashim et al., n.d.). In these methods images are compressed before embedding the data in it. These compression algorithms can be the Discrete cosine transform (DCT), Discrete Fourier Transform (DFT), and more as shown in Figure 7 (Pope et al., 2012).

3.2.9. Steganography Methods

The starting point is always using images because they are easier to be used as an example like it was previously showed. However, there are several methods to perform steganography and it can be supported in many ways.

3.2.9.1. Audio Methods

Sound is the compression of air particles and propagates through the air. Different pressures on the air of these particles produce the propagation of energy in a wave form with different frequencies and wavelengths, which when reaching the ear is interpreted as different sounds. When it is turned in digital format, waves are discretized into regular intervals and shrunk to a maximum value.

After the digitization of analog sounds, the digital sound passes through compression codec to turn its transmission and storage more efficient.

In digital audio files, messages are placed in the frequency, amplitude, phase, files spaces, or compression components (Pope et al., 2012). In fact, there are several techniques to hide data, and some of them combined or improved depending on the mean that is used. The main goal is always to conceal data and not to be uncovered. For example, the LSB method is known for its low robustness to noise addition, although it is very easy to incorporate new data and very easy to develop and that it can be used along with some other hiding techniques. But in fact, it has lower security performance, which makes it more vulnerable even to simple attacks. Usually, data transformation, such as adding noise and compressing the hidden message, is very likely to corrupt the file. On the other hand, the message can be easily extracted by removing the plan, since the embedding process is very deterministic. (Djebbar et al., 2012).

3.2.9.2. Image/Video Methods

Image and video offer greater storage for hiding data, depending on its formats. Compressed image and video formats usually tend to destroy hidden information when using spatial domain, so this kind of technique mostly uses frequency domain. Another reason to use compressed formats is to reduce the file size as it is necessary to be stored and eventually transferred through networks.

In an image file, the hidden can be placed in the metadata of the image or attached to the end of the file. Images are not only pixels with a location, and with some color and intensity attributes. (Pope et al., 2012).

3.2.9.3. Network Methods

Network steganography it can be categorized in two main areas: storage channel and timing channel.

Storage channel modifies values in the cover object to create a storage covert channel. This technique hides information in in unused bits of a header in the protocol header fields or in the data field of a packet. This is most used technique since each layer adds new header fields to the existent ones.

On the other hand, channel timing attempts to modify the tming of "events" in a cover file to create a hidden timing channel in order to store data in packet timing. But this technique is difficult to handle because of its complexity and limited user control to manage how the protocol and operating system adjust the timing of events. (Soni, 2020)

3.2.10. Steganography major threats

Steganography is typically associated on covert communication between 2 parties. For instance, extremist individuals or groups. However, security reports have been showing the increasing importance of information hiding to malicious software developers.

Once the malware used encrypted communications for Command and Control (C&C) purposes and now are hiding the malware within the "background noise" of the data transferred in the network.

For example, previously, malicious traffic for Command and Control (C&C) purposes could be noticed from regular network traffic. However, it is now completely disguised within the "background noise" of data exchanged over the network. The good news is that there have been improvements in how to identify and block C&C communications from botnets (Cabaj et al., 2018).

3.2.10.1. Covert Channels and Data Hiding

Cyber-Attacks with malwares usually have five phases: (1) reconnaissance (gathering of information), (2) scanning the target, (3) gaining access to the target, (4) maintaining the access and (5) covering the tracks. Attacks regarding information hiding techniques takes place mostly in phases 2-4 (Cabaj et al., 2018).

Network traffic allows to keep transmitting hidden data whereas a digital media file has a limited capacity. The channel for transmitting steganographic information is called to as a covert network channel. It allows covert communication over a network. Control protocols can be used on top of covert channels, representing a form of Command and Control (C&C) channel. Malware are also capable to create and use covert channels for data exfiltration, bypassing companies' firewalls. (Cabaj et al., 2018).

Another area referred in the paper "Covert channels in IoT deployments through data hiding techniques", with significant level of vulnerability are the devices connected to Internet of Things eco-systems, which are not resilient to intrusion, hacking and sabotage attacks. This was showed by events such as the DDoS attack mounted using the Mirai botnet, which was fully composed by IoT devices (Caviglione et al., 2018). In fact, the referred paper details an experiment to analyze Exfiltration and C&C in a hypothetic Industry 4.0 facility and which showed that steganography allowed to use at least any sensors of the IoT to transmit a hidden flow of information. After that it was proposed to continue developing more general and high-level methodologies because it was stated that was "the first step of an extensive classification and formalization of attack patterns for IoT environments".

3.2.10.2. Information Hiding Malware

In the following table is a listing for each malware that uses steganography to hide information and to spoof its behavior to trick users.

Technique	What it does	Malware Examples	Date	Desktop / Mobile	Malware functionalities	Carrier file Type used to conceal malware
Modifications on digital media files	• hiding settings or configuration files of malwares • provides the malware an URL from which can download additional components • stores the whole malicious code on the file	Vawtrak/ Neverquest	2015	Desktop	Steganography is used to place settings in favicons of the websites. Vawtrack gets the image's pixels LSB to get an URL where its configuration file can be downloaded.	Images
		Zbot	2014	Desktop	Downloads a JPEG on the infected system containing its configuration data attached at the end of the image.	Images (JPEG)
		Lurk Stegoloader	2014	Desktop	The LSB of BMP or PNG image files are used to place an encrypted URL where it can download additional software	Images (BMP, PNG)
		AdGholas	2015	Desktop	Hides encrypted JavaScript code in images, text and HTML code	• Images • Text • HTML Code
		Magento	2016	Desktop	• Uses images to conceal details of payment cards • Payment details are hidden inside of images of products of the infected Magento e-commerce platform • Downloads modified images, the attacker exfiltrates the stolen data.	Images
Malware mimicking legitimate apps or their traffic behavior	Depends on imitation of legitimate software and/or their	Android/ Twitoora		Mobile/ Android	• The malware is spread through a SMS or a fake URL • Mimics an app, leading the user to install it and spreading the malware.	• App • MMS

Technique	What it does	Malware Examples	Date	Desktop / Mobile	Malware functionalities	Carrier file Type used to conceal malware
	traffic.	Irongate	2016	Desktop / SCADA	• operates in industrial control systems scenarios. • it records some seconds of truly traffic from a programmable logic controller. After that it uses it as a smokescreen (malicious commands are masked with legitimate ones) when sending back modified data. • It changes-controlled processes in an unsuspected way and without security alerts.	Network Traffic
		Fakem RAT	2012	Desktop	Covers its C&C traffic to look like Instant Messengers or HTTP conversations	HTTP Traffic
		Carbanak/ Anunak	2014	Desktop	• It redirects users to a landing page designed to discover the victim's vulnerabilities in order to provide the most appropriate exploitation. • Malware dynamically creates a Google Sheets spreadsheet to manage each infected victim • Using a Google service gives the sense of security that allows to break some lines of defense regarding third-party services	Application
		SpyNote Trojan	2016	Android	• Application mimicking the Netflix app • Provides the attacker with the ability to perform some actions, such as accessing the user's contacts, copying the user's files, and listening to the user's communication	Netfilx Application
		domain fronting (Technique)	2017	Desktop	• Hides the true destination of the connection by imitating legitimate traffic • exploits HTTPS traffic to communicate with an infected host looking like a Google search. • Malicious traffic is generated when exchanging data with the attacker	HTTPS Traffic

Technique	What it does	Malware Examples	Date	Desktop / Mobile	Malware functionalities	Carrier file Type used to conceal malware
Information hiding in ransomware		TeslaCrypt (as part of the Neutrino exploit kit)	2016	Desktop	• It redirects users to a landing page designed to discover the victim's vulnerabilities in order to provide the most appropriate exploitation • After the successful exploitation, a payload is executed • contacts a server in order to collect data, which responds with an HTTP 404 error page embedding C&C commands into the HTML comment tag	Adobe Flash program
		Cerber	2016	Desktop	• through a fake document, it loads a malicious macro-code that downloads a JPEG file to the targeted machine. • The payload is embedded inside of an innocent-looking image	Image
		SyncCrypt	2017	Desktop	• Mails with Windows Script Files in attach looking like court orders • After opening the attachments, a malicious code downloads an image containing the core components of the malware	Image
Informationhiding in exploit kits	Inside exploit kits, allowing developers with few programming skills to create, customize and distribute malware	Stegano/ Astrum	2016	Desktop	• malicious code is embedded inside banner ads by modifying the alpha channel in PNG images • After that, the users' browsers with infected ads parse a JavaScript that extracts the malicious code, redirecting users to the exploit kit landing page. • Finally, on the landing page the payload is executed, usually using Flash vulnerabilities.	Image (PNG)
		DNSChanger	2016	Desktop	• Hides an AES encryption key inside of an ad to decrypt the network traffic generated by the exploit kit. • DNSChanger launches brute-force attacks against victims' routers to take control of their network and place advertisements on all exchanged traffic	Network Traffic

Technique	What it does	Malware Examples	Date	Desktop / Mobile	Malware functionalities	Carrier file Type used to conceal malware
		Sundown	2016	Desktop	Is used to: • PNG files uploaded through an Imgur album are used to exfiltrate information stolen (see, the CryLocker ransomware campaign); • hides the exploit code delivered to thevictims.	Image (PNG)

Table 2 – Malware Hiding Techniques (Cabaj et al., 2018)

Some of these malware software can either embed information or perform techniques to bypass steganalysis techniques to detect steganography. (Caviglione, 2017).

3.3. TECHNOLOGIES AND PROCESSES TO FIGHT STEGANOGRAPHY

As it was referred before, steganography is an ancient technique to hide data during transmissions. In that way, since the beginning of steganography there were always developing of techniques to be performed as countermeasure to detect steganography messages.

Steganography evolved alongside with the development of the technology. Since these techniques are always conceal and to cover information, it is very useful to criminals, lead to cybercriminal since most of it is performed on computer networks. Because of that, nowadays there are some techniques to fight the problems driven by steganography. Some of them are to detect and to delete, and others are to collect evidence of criminal acts.

3.3.1. Steganalysis

Steganalysis is the area of study to develop tools and techniques to detect the presence of steganography so that the secret message may be stopped before it is received. (Z. Khan & Mansoor, 2009).

The second goal is to identify the tool to try to spoof, corrupt or even extract the secret message for the sego object. Usually, steganalysis follows two distinct approaches: the first one is to use a specific algorithm to a particular situation and the second is to develop a master and broader algorithm to comprehend all kinds of situations. Both have its pros and cons and wider techniques tend to be less accurate but more effective to new types of steganography (Z. Khan & Mansoor, 2009).

In fact, Steganalysis and Steganography goes hand in hand, developing new techniques to hide information, as well developing new techniques to detect those hidden messages. Is like developing a poison and its antidote at the same time (Warkentin et al., 2008).

Steganalysis is categorized in visual, structural, statistical, and learning steganalysis. Visual and structural are regarding to look to the structure of a given file. Statistical method uses statistical models to detect steganography and it can be split in two different branches: specific statistical and universal statistical. Learning steganalysis also known as blind steganalysis is one of universal statistical steganalysis using cover-objects and stego-objects as training dataset. This steganalysis technique tries to detect steganography without regard to steganography techniques (Jung, 2019), which it will be the technique mostly referred in this thesis.

3.3.2. Digital forensics

Digital Forensics cares about to preserve the digital evidence for a future criminal inquiry. It develops methods to collect, validate, preserve, document, and analyze evidence of events found to be criminal. The most visible known cases involve audiovisual files, such as in child pornography, although there are some other important cases of industrial espionage, intellectual property robbery and fraud. (Warkentin et al., 2008).

3.3.3. Tools and Techniques

An organization is used to deal with a significant amount of data coming and going every day. Naturally, it cannot be aware to every channel they have to spoof every communication, applying specific algorithms to detect and to extract secret messages from files and communications.

There are good hardware and software solutions to avoid intrusion, like IDS' but the biggest problem of Steganography is that systems cannot even guess that a secret message is present. In the other hand, criminals are always one step ahead from researchers and the techniques of steganalysis. In this case it is important to have a wider algorithm trying to fetch malware and steganographic communications, even though that algorithm could be less accurate. Ideally, given the amount of information coming in and going out of an organization, the main purpose of IT is to detect the presence of Steganographic techniques in files and in the network packets.

Some authors have already proposed to use machine learning to develop processes which helps to detect the storage-based network steganography, due to some frameworks can be prepared and trained to detect steganography.

Machine learning is a branch of Artificial Intelligence where a computer-based technique has the ability to learn without the need to be programmed. It has three different leaf which are: supervised learning, unsupervised learning and reinforcement learning (Jung, 2019).

Supervised learning is based in functions that guides an input to an output connecting them. This technique is mostly used in speech recognition, spam detection and object recognition, and it uses the following algorithms: Nearest Neighbor, Naive Bayes, Decision Trees, Random Forest, Linear Regression, Support Vector Machines (SVM), Neural Networks.

Unsupervised learning learns from tested data that has not been labeled, classified, or categorized. The field of Its application is cluster analysis, principal component analysis, vector quantization and self-organization. Usually, it is associated to the k-means clustering, and Association Rules algorithms.

Reinforcement learning cares about on how to interact with the model to improve some notion of cumulative reward. It has much success in investment decisions, chess game software, robotics, and inventory management where it must learn actions to be performed. The algorithms used in this type of Machine Learning are Q-Learning, Temporal Difference (TD), Deep Adversarial Networks.

Finally, Deep Learning is a sub area of Machine Learning where the basis of its learning technique is on data representations (Jung, 2019). Deep Learning has also associated several methods like: Classic Neural Networks, Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNNs), Generative Adversarial Networks, Self-Organizing Maps, Boltzmann Machines, Deep Reinforcement Learning, Autoencoders, Backpropagation, Gradient Descent. (Deep Learning Techniques, n.d.)

in 2019, a study brought together previous studies comparing Machine Learning with Signature-based detection, Statistics-based detection and MAP based detection. The study refers that SVM was used to detect network steganography in TCP/IP and Naïve Bayes to detect secret information hidden in TCP/IP header, which were considered effective. In the other hand, Random Forest was used to detect storage-based network steganography. In the end of the experiment results showed that Random Forest is more effective than SVM and Naïve Bayes to detect storage-based network steganography. The conclusion was that Machine Learning can bring more accuracy in the detection of abnormal behavior of steganographic packets. (Cho et al., 2019)

Other authors tried to develop machine learning algorithms, using some frameworks such as TensorFlow, Theano, Keras, Caffe, Torch, Deep Learning 4j, MxNet, CNTK, Lasagne, BigDL and so on. They used three frameworks such as scikit-learn, TensorFlow, and Keras due they were tested on stego-images. After the experiment, where they previously stated that many training data and test data should be collected and normalized to increase accuracy, and after that they prepared data and trained the models. It was concluded that the process and possibility for several machine learning frameworks were considered, so the issue of the accuracy was not so important as people might think. In fact, to leverage the accuracy, many datasets should be prepared and normalized previously. (Jung, 2019).

In the same year, another steganalysis paradigm based on the representative deep learning method CNN (convolutional neural network), where the model was designed and adjusted according to the features of steganalysis, turning that model more effective in getting the statistical characteristics such as neighborhood correlation. Another goal of the study was to create steganalysis detectors without distinguishing specific types of steganalysis algorithms. Unfortunately, the research showed that methods couldn't be able to be completely universal, given that the process of constructing the detector, where it is necessary to know specific type of information of the steganographic algorithm to be detected to accomplish the generation of the dataset for training the model. In this case, it was set that it was important to have a deeper knowledge of detectors for different steganalysis algorithms (Zou et al., 2019).

Previously in 2015, CNN was already studied and obtained the first results of steganalysis by Deep Learning approaching the performances of the two-step approach EC (Ensemble Classifier) + Rich Models (RM). During the period 2015-2018 methods have been evolved, and in the end, despite considering that many things were not yet solved, it was clear that CNN was very present in the steganalysis community (Chaumont, 2020), which empowers the idea to find a solution in this technique to solve steganography threats.

Same CNN algorithm was proposed to detect malware in PDF files. It was stated that the advantages of using deep neural networks was that was is not necessary to define features because the neural networks would automatically extract or compute features. Used to tackle the malware detection the experimental results showed that the proposed neural network is much more effective than several representative machine-learning models. Same to other convolutional neural networks but having different settings (Jeong et al., 2019). An important property of CNN is that it can extract complex statistical dependencies, and already in 2017, it was used to learn the optimized deep hierarchical representations for image steganalysis, and it was trained to distinguish covers from stegos (Ye et al., 2017).

Regarding to tools, in 2020, some authors identified some approaches to fight steganography, especially: Visual Detection; Detection of steganographic Artifacts; Steganalysis Based on Image Quality Metrics; First-order statistical Analysis; Steganalysis Based on JPEG Compatibility; RS Analysis; Pairs Analysis Palette Quick Pairs Analysis; Raw Quick Pairs Analysis; Chi square Attack. Mostly regarding looking at images in order to detect Stego-images in it.

Along with these approaches, same authors referred some tools as well like: StegSpy; Stegdetect; Stegbreak; Stego Suite; and StegAnalyzer. StegSpy software is not able to perform universal detection and it only can detect some hidden information originated through some stego software. StegoDetect can detect data stored in JPEG images using open source softwares and it is able to detect parts of the message with jsteg, jphide, nvisible Secrets, Outguess 0.1, 3b, F5 (page header analysis), AppendX and Camouflage. There are some of these open-source projects in the web developing techniques to detect steganography for user testing (Open-Source Steganography Projects, n.d.)

Finally, Stego Suite is a software that can apply the blind detection, and it can detect the use of digital steganography in all its forms. Among those referred this one is the one that can really help organizations in several kinds of steganography (M. Hassan et al., 2020).

In this way, knowing that steganography is a complex field of study, there are already a set of techniques and tools being evolved to help organizations, law enforcement, and digital forensics to address this problem.

3.3.4. Indicators of Compromise (IoC)

To have a closest following of the network traffic going in and out of the organization's network some IoC should be defined and monitored. Working as evidence of a data breach or any other attack, these can show that an attack is being in execution, what tools are being used and who is launching them.

These kind of indicators are usually collected from the security software like anti-virus or anti-malware, looking for traces in the system and in log files .(Popa, 2021)

There are some IoC's suggested to be collected like:

- Unusual traffic on the network
- Suspicious files and applications, or even processes working in the system
- Activity in administrator or privileged accounts
- Traffic coming in from countries which company does not work with
- Forced attempts of access or logins that might indicate a brute force attack
- Sudden increase of number of requests from the system which might indicate a DoS.
- Sudden changes in system settings like Domain Name Servers (DNS) configurations
- Files found in folders they shouldn't be

("Indicators of Compromise," n.d.)

3.4. CHALLENGES AND OPPORTUNITIES

Challenges and Opportunities can always set a direction on the course of this study. First, in the Challenge side, identifying what needs to be evaluated and the problems that we need be aware of. Second, on the Opportunities side, all the steps we will be able to make to address the subjects referred as challenges.

3.4.1. Challenges

Nowadays, Cybercrime focuses upon three directions: increased stealth, commoditization of malware, and exploitation of Internet of Things (IoT) devices. It is indeed a fact that Cybercriminals are always one step ahead, so they will continually try to improve their information-hiding techniques, making it harder to detect and trace back malware to its origin.

According to (Cabaj et al., 2018) the malware types provided lists the major trends that were highlighted by (Mazurczyk & Caviglione, 2015) when it was referred that information-hiding techniques would continually be introduced, and their degree of sophistication would increase. Moreover, they could be incorporated into every type of malware to provide stealthy communication of both C&C and the exfiltration of user data. Along with that these malwares could remain cloaked and continuously leaking sensitive data.

Like it was previously said, steganalysis tools and techniques tries to, firstly, detect the presence of steganography so that can be stopped before it is received. (Z. Khan & Mansoor, 2009), and after that tries to extract the secret message or code. In that way, the biggest challenge shall be to develop mechanics to detect the presence of the steganogram, to detect the covert channel in order to block an eventual malware or a data leakage. It could be an eventual thought about Digital Media steganography, but that it is complex to put that into practice in an organization. It would need to be used through a steganography application and as well to extract. It would be easier to steal the documents right away instead of sneaking them out through stego-object, trying to not be detected by company's IDS' and Firewalls.

Another big challenge, and regarding to the communication network field, is to prepare organizations to the new protocols such as Skype, BitTorrent and Stream Control Transmission Protocol, especially when trying to detect covert communications among many similar connections. According to (Cabaj et al., 2018), there are many other key challenges which can outcome from steganography over network communications such as the ongoing IPv4 to IPv6 transition, where Malware can take advantage of misconfigured nodes, by hiding in HTTPS or Transport Layer Security (TLS) traffic, by managing distributed denial of service (DDoS) attacks. The next dimension of cyberattacks will be the IoT devices: networked sensors, CCTV cameras, smart TVs and smart home equipment, industrial equipment, etc.

Finally, another and most recently big issue that came to be a rather interesting challenge as well, is the IoT technology. It is now clear that its networks seem to be not yet prepared to these kinds of events. Therefore, there are some organizations and industrial facilities already over 4.0 Industry ecosystem logic, remotely controlling their devices through IoT, which will come across from attacks targeting IoT and industrial control systems coming from Internet (Caviglione et al., 2018).

To overcome all these challenges, the next step for this study is to create a map of each different situation an organization may have with regard to steganography. Even though, steganography is not always used in a malicious way; it can be used to protect and hide information, especially in countries where politics restricts citizens expression rights. However, it will not be the intension of this study.

After the identification of each situation, the challenge will be to determine which best practices should be taken to address each steganography situation. It does not have to be a technique based upon on a technology feature and where it can be used only a set of support team actions which can deal with the situation. Those actions can be determined by the organization's Security Office Center.

3.4.2. Opportunities

There are several opportunities in overcoming the problem of steganography in the context of the organization. In fact, this study is an opportunity to define a strategy to prevent and fight steganography. It will be an opportunity to further leverage the responsibilities of the SOC to address cybersecurity issues and cyber-attack prevention actions.

As referred in (Jung, 2019), and regarding using Machine Learning to be part of a blind steganalysis technique, prediction and accuracy would be different depending on the framework used and how datasets were used, suggesting that companies should test some frameworks and prepare some dataset to teach models to detect malware. Refining the usage of Machine Learning, some authors are already using CNN methods (Zou et al., 2019), (Chaumont, 2020), (Jeong et al., 2019) to have a global technique that can learn to detect stego-objects. So, there is an opportunity to set the conditions to improve detection algorithms, to test models and to create artifacts to be installed on the systems environments to, like a warden, monitor the traffic and to alert eventual steganography.

4. TOOLBOX OF TECHNIQUES AND SMART AND ADAPTATIVE TOOLS TO CONTROL STEGANOGRAPHY

4.1. THE TECHNIQUES AND TOOLS TO CONTROL STEGANOGRAPHY TOOLBOX

After the intensive study about Steganography already done by carefully reading the literature about this subject, it is already reasonable to think that organizations can face severe problems due to the damages that this kind of technique can produce.

One of most common situations in steganography is the malware installation. It acts under covered and has the ability to exploit vulnerabilities, like opening ports to allow data breaching. There are several kinds of malware as showed by (Cabaj et al., 2018) . For a large period of time users and organizations thought that executable files (with extension *.exe) or zipped files were the ones that could be harmful. For this reason, email attachments were being remove when reaching the mail server to avoid deploying malicious software, like viruses, trojans and many other malware. However, cybercriminals soon realize that it was needed to look for new techniques to avoid being detected when going through the lines defense in depth placed on the organization's infrastructure.

This Toolbox presented in this study intends to deliver, not only, some tactical solutions to address each kind of situation analyzed, but also a good set of best practices defined as strategies as a complement of the analyzed toolbox.

In order to solve steganography issues this toolbox intends to deliver, not only, some tactical solutions to address each kind of situation analyzed, but also a good set of best practices defined as strategies as a complement of the analyzed toolbox.

Organizations must face this toolbox as a manual which gives some guidance about tools and processes to help organizations to face this kind of cyber threats. Remember that steganography is only a vehicle to conceal not only information but the acting of spreading malwares. So sometimes it is intended to block steganography tools or to block the malwares concealed in images provided for other vehicles like emails other shared files.

There are two kinds of software those who deals with steganography itself and those who deals with the consequences of installing malware shared by infected material. In the first part it is intended to describe all the available software who deals with malware installation, and then the ones who directly deals with steganography tools and techniques.

4.2. ASSUMPTIONS

Based upon what it has been studying in the literature review about Steganography, it was defined that for a cyber security professional, or eventually a cyber security team, to become more aware, conscious, responsive, well-knowledge and smarter on these topics, one should:

- This study regards only to the malicious use of steganography and its impacts on companies – It will not be applied to the use of steganography to improve authentication processes to companies' systems
- There are specific cases for the use of steganography and those limits the number of possible situations of its use
- The assessed tools may only deal with steganography. It is not intended to assess the combination between steganography and cryptography.

- Those who use steganography are perfectly aware that they are committing a crime and will incur in legal penalties, so it is important to analyze the intentions of those cybercriminals
- The process to generate steganography needs to use proper software that shall be analyzed.
- It is assumed that steganography is a complement to conceal information and code to install malware and not to conceal messages in carrier files to send to outside the company acting as part of information robbery
- Installed Malware may include Trojans, Viruses, Worms, RAT, FAKEAV, and many other malicious software
- Although Steganography can be part of security techniques to prevent intrusion, this study will only touch the malicious use of Steganography
- Steganography has several techniques to spread hidden information and the process to its detection has high latency and complex
- The complexity of Steganography can turn anti-virus completely useless because it can obfuscate the presence of malware to the anti-virus software, which forces to analyze several different techniques to protect organizations from the damages it may cause
- Detecting steganography forces to use several techniques which need several steps to be succeeded
- Due to COVID 19 the labor has changed and many of working people started to work at home using their own computers to access organizations infrastructure which exposing it to malware infiltration and intrusion
- There are several ways a carrier file can reach the infrastructure: attached on an email, downloaded from a site, torrent, ftp, etc. The intention is to analyze if the existent software and techniques can help to detect and block when the infected file reaches the infrastructure.
- It is assumed that are some scenarios which steganography can happen, and which will be used to compromise an organization. It will be assumed those scenarios like the following ones:
    - Scenario 1: Steganography is used to insert a malware in an innocent-looking image, sent through an email attachment, and which is installed after the image had been opened
    - Scenario 2: Steganography is used to insert a malware in an PDF File, sent through an email attachment, and which is installed after the PDF document had been opened
    - Scenario 3: Steganography is used to insert a malware in an innocent-looking image, posted on an image on a website, and which is installed after the image had been opened
    - Scenario 4: Steganography is used to insert a malware in a web ad, and which is installed after the ad icon has been clicked on
    - Scenario 5: The user clicks on an image obtained through a download from a web site, torrent, ftp server, which contains a malware placed through steganographic methods and which deploys a malware
    - Scenario 6: Steganography is used to insert a malware in an innocent-looking image or PDF, placed in a filesystem (on-premises or cloud) irregularly brought to inside the organization (p.e. through a flash drive or even a user laptop which in different networks outside of the company), and which is installed after the file had been opened

  - Scenario 7: A malware is placed in a mobile phone app through steganography techniques and a user installs the app on the cell phone thinking that is a legitimate one. The malware takes the control of the cell phone.
  - Scenario 8: Hidden commands through steganography techniques are sent through network packages
  - Scenario 9: Steganography is used in Exploit Kits, where the victim without knowing is redirect to an exploit kit landing page, which exploits the victim's computer searching for vulnerabilities and installing a malware to take the control of the computer
  - Scenario 10: Steganography is used to insert malware into an innocent-looking image sent through an email link or a Malvertisement campaign and installs a malware after the link or banner is clicked on
- Despite Adobe Flash Player has been decommissioned many companies still uses software developed with this technology which makes them still a target for the attackers. ("Adobe Flash Player EOL General Information Page," n.d.)

4.3. WORKFLOW OF IMPLEMENTATION OF THE TOOLBOX

Based upon the previous assumptions, it is proposed a workflow to be a template for the day-by-day of the organization. This should be used to establish the guidelines for the work.

The proposed workflow depends upon some steps which can carefully detail some tasks within in order to deal with damages created by steganography:

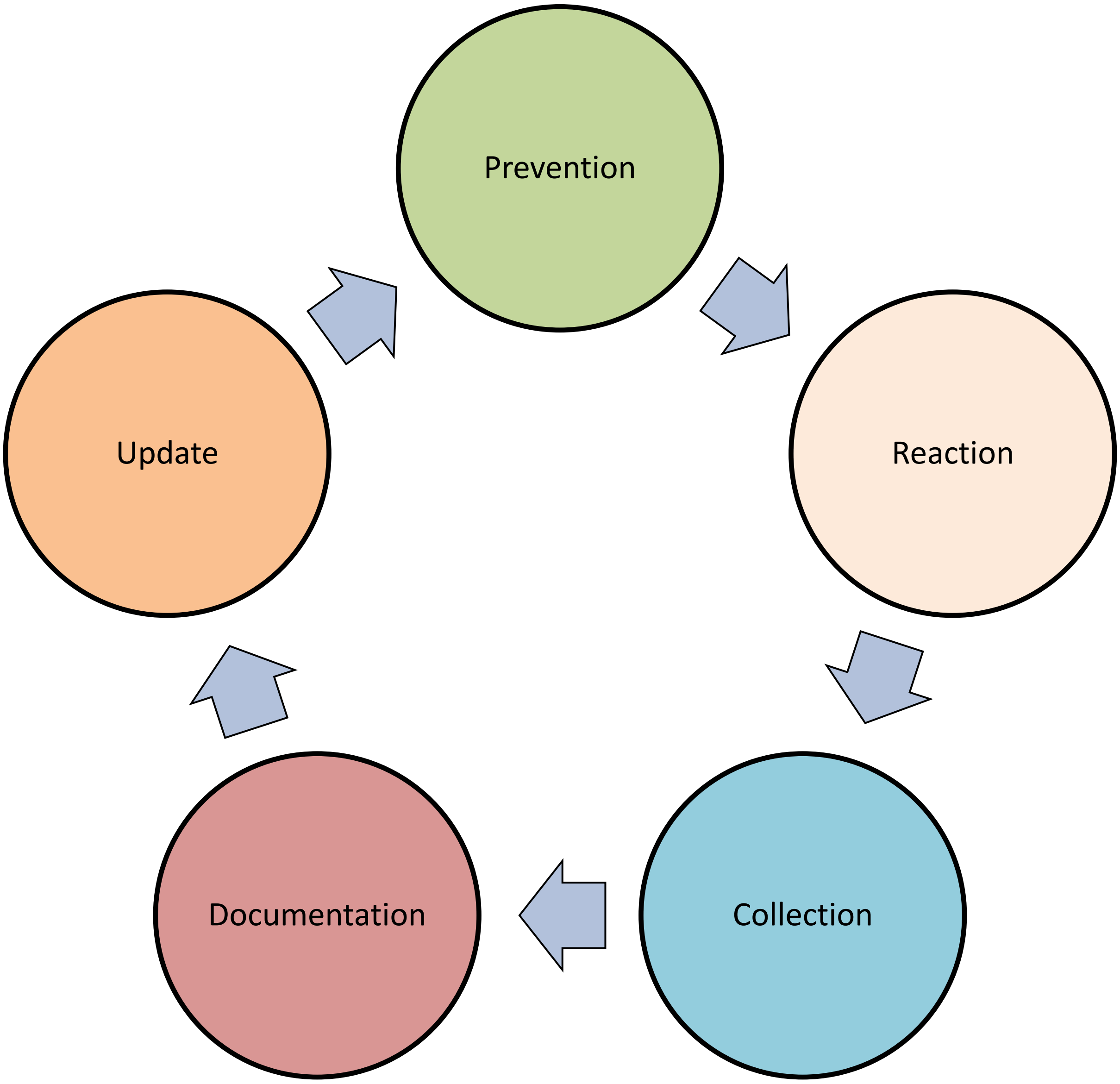

Figure 8 – Toolbox Workflow – Stages of execution

4.3.1. Prevention

Like the name says, the Prevention phase allows the organization to set some best practices for the organization to reduce the probability of compromise. Being the Risk the product between Probability of the attack by the Impact of that attack, reducing the variable of Probability, the organization is intentionally reducing the magnitude of the Risk.

There are some steps that should be implemented considered as Prevention Methods:

Method	Description
Training	• Plan and perform basic trainings of cybersecurity to all users of the company, including outsourcers. • Foster the vision of the company regarding cybersecurity intentions and the impacts of cyberattacks to the organization • Plan yearly basis train to update teams' knowledges, new insights and new company policies and techniques updated during last year
Stego software	Install Steganography Security Software to prevent in real-time files with steganographic content which can come up through email attachments and/or file downloading. The software it can be used in manual to mode to scan a suspicious file or an entire system.
Anti-Virus and Anti-Malware	Install a comprehensive Antivirus to detect and remove a wide range of malware like Trojans, Virus, Trojans, Worms, Ransomware, and many other. Anti-virus Software should be updated with the most recent version to comprehend the most recent virus versions and techniques.
Patching the system	Take actions in order to update organization's systems always updated with new releases of software. These new releases have always new patches to improve the security of the operative systems, reducing the probability of an attack.
Settings on the network (Network & Infrastructure security, Web Security, Messaging Security)	Implement settings on the network to control traffic, like a secure web gateway to police internet traffic, and like network segmentation to treat different protocols in each section, and to isolate and to protect most critical systems. Implement a Secure Email Gateway (SEG) to perform previous analysis to mails before delivering it onto user's mailbox. Steganography security software, like Steganalyzer will help to prevent Covert Channels, and Stego Suite will help to prevent carrier files transfer ed through the network.
Identify the most critical systems to the organization	Create a rank of each system and its level of criticality: • Most vulnerable ones to steganography • Most important ones to the organization Set a list of those it should have backup Ser a plan of action in case of an attack to keep the system alive and to keep the business operating

Table 3 – Actions that should be taken in the Prevention Phase of the toolbox

4.3.2. Reaction

The reaction phase starts after detecting some malware or eventually after an attack. To face problem, some countermeasures should be taken:

Method	Description
Identifying suspicious cases	Automated processes for detection, like Stegoanalyzer, or any occurrence that can be suspicious shall be followed for an identification of carrier file, the location of it, and the application who brought the file onto the system.
Quarantine	All files detected through Stego Software should be set in Quarantine to be further analysis. After that it should be performed a deep scan to the detected file to extract the stego-object inside the carrier file
Detecting false positives	Analyze suspect cases to see if they are false positives. False positives shall be unmarked and used by the organization. Bad files shall be removed after its documentation
Emergency plans	Activate emergency plans to disable some systems and some network areas to prevent the spreading of malware through network and to reduce the infection
Contact authorities	Contact National CERT and Judiciary Police in order to help in identification of the source of the problem and to perform Digital Forensics evidence.

Table 4 – Actions that should be taken in the Reaction Phase of the toolbox

4.3.3. Collection

The Collection phase it should be performed after the response of an attack. It intends to assess and collect all information about the malware, the attackers and their motivation to register and prevent future similar attacks.

Method	Description
Assess and collect all information about the malware	Collect the information regarding the malware: • how it works • what it infects • which technique used to be deployed • which damages had been created • Who is attacker is and what are his motivation for its spreading • Which countermeasure had been used to solve the infection and which results had been achieved
Indicators of Compromise	Collect the forensic evidence from security software regarding the attack Assess whether is reliable to create new indicators of compromise
Go to the community	Contact the worldwide community in order to achieve if there is any evidence of its previous use Gather information of the attackers and its motivation Share the information already got when assessing the attack

Table 5 – Actions that should be taken in the Collection Phase of the toolbox

4.3.4. Documentation

This phase intends to update the current documentation regarding malware, damages, stakeholders and known techniques to fight new threats and prevention and reaction methods.

Method	Description
Toolbox documentation	Assess if there are new updates
List of Malware	Updated list malware that uses Steganography to be spread
Software and techniques used	Countermeasure used to face each malware
Known Participants	List of people or organizations responsible for the development and/or the deployment of malware
Indicators Of Compromise	Register the Indicators of Compromise of the attack.

Table 6 – Actions that should be taken in the Documentation Phase of the toolbox

4.3.5. Update

Finally, the Update phase aims to update the items in the toolbox in order to be used as new actions.

Method	Description
Acquire new software versions	Renew of the current licenses or assess whether the current software comprehends all known malware
Rethinking combat strategy	Rethinking combat strategy whether to decide if it is necessary implement new actions or to redefine the existent ones
Rethinking the network configuration	Rethinking if the present configuration plan and assess whether it is necessary to implement new lines of defense in depth.
Update the training programs	Upgrade the current training programs with new information of new malware, threats, or defense techniques

Table 7 – Actions that should be taken in the Update Phase of the toolbox

4.4. TOOLBOX PROPOSAL

4.4.1. 1st Strategy - Malware Installation prevention

As referred on the Literature Review, the most common use of steganography is to spread malware. Steganography is not by itself a mean for steal or to hide information. Is just a mean to deploy malicious content for compromise an entire information system. So, the first strategy for setting a line of defense, is to assess how can organizations protect themselves for each identified malware by knowing each one's purpose, how are they deployed and which tools, techniques and countermeasures can be addressed to fight them.

Threat Technique	Malware	Format used	Available information	Tools, Techniques & Countermeasures
Modifications on digital media files	Vawtrak/ Neverquest	Image	**Which is its main purpose:** To obtain unauthorized access to bank accounts through home banking sites. **How It works:** Infected computers are collected in a botnet farm to collect login credentials from online accounts of banks and financial brokers. Those credentials are used in injected code and proxying the infected computer to transfer fraudulently money from the victim's accounts to other bank accounts under control of the botnet administrators. The process injects a DDL on the browser process. When the user goes to the target URLs, the malware injects extra code into the page which it can bypass 2 FA and initiate the money transfer from the victim's account and hiding the evidence of that transfer. **How it is deployed:** Usually delivered through one of these 3 ways: • attached in an email as spam: covered as a campaign from a financial institution, the user is the user is persuaded to open the attachment. It is a zip file that includes an executable file within and that will install the	Using Anti-Malware which can recognize Vawtrak and which can protect and remediate for every malware. (Bailey, n.d.)

<u>Threat</u> Technique	Malware	Format used	Available information	Tools, Techniques & Countermeasures
			malware. • As the payload to an exploit kit: For instance, a malicious flash redirector can be inserted into the page and traffic is sent to the EK landing page. This page will contain an obfuscated JavaScript that will try to exploit a vulnerability in the infected browser and load malware as the payload. • downloaded by loader malware delivered through the exploit kit or the spam email: through loader malware that downloads the installer. (Wyke, 2014) **Malware Today:** Its activity has declined after its developer arrest. But some other banking trojans, were connected to the development group behind Vawtrak (R. Cohen, 2019)	
	Zbot / Zeus	Image	**Which is its main purpose:** One of the most widespread banking malwares. Debuted in 2007, grabs user credentials by redirecting users to fakes web pages with same look&feel. (R. Cohen, 2019) Designed for data theft or to steal account information from home banking pages, it is also used on social networks, and e-commerce sites. (Caraig, n.d.) **How It works:** It relies on a list of online banking sites to steal user credentials. It monitors user's web browsing even through https, using Windows titles and urls for its attacks. Sometimes this exposes the user's account. (Caraig, n.d.) **How it is deployed:**	1. Foster users to have a cybersecurity culture being cautious when opening email message and when clicking URLs. Always be suspicious 2. Use an up-to-date and comprehensive anti-virus solution that can detect and block bots, and that can detect and remove all kind of malicious software (viruses, Trojans, worms, unwanted browser plug-ins, and malware). (Caraig, n.d.)

Threat Technique	Malware	Format used	Available information	Tools, Techniques & Countermeasures
			Through spammed messages or downloaded from compromised websites. Usually used on legitimate looking company sites, like governmental agencies. (Caraig, n.d.) **Malware Today:** It was mostly neutralized by antivirus software, but it is still being spread across the web through thousands of variants (eg Citadel, Gameover, and Atmos). (R. Cohen, 2019)	
	Lurk Stegoloader	Image	**Which is its main purpose:** Download and execute secondary malware payloads. (Stone-Gross, 2014) **How It works:** Embeds encrypted URLs into an image file by manipulating pixels. (Stone-Gross, 2014) **How it is deployed:** Through an HTML on compromised websites that loaded a Flash-based exploit. When browsing an infected site, if the user is running a vulnerable version of Adobe Flash, the EK drops a DLL and executes the malware. (Stone-Gross, 2014) **Malware Today:** Not found any information related but it is reasonable to think the malware has been evolved.	The Stegoloader is very difficult to be detected. So, it is needed to develop multilayered defenses, combining prevention, detection and brief response time to be capable to break malware life cycle, Once its detection it is necessary to run a malware removal in the system. (Tamir, 2015)
	AdGholas	Image, text, html	**Which is its main purpose:** For many purposes, from financial information and personal one to file encryption.	Recommended to perform a defense-in-depth approach to security. So, it is recommended to:

Threat Technique	Malware	Format used	Available information	Tools, Techniques & Countermeasures
			(Chen, 2017) **How It works:** The attacks are able to conceal traffic through HTTPS, which turns its detection very challenging. (Chen, 2017) **How it is deployed:** Using Malvertisement campaigns, by exploiting flaws in the delivery of ads. Flaws in third party ad servers or in redirection of ads to legitimate sites, attackers spread malware and/or redirect users to malicious webpages. (Chen, 2017) **Malware Today:** Not found any information related but it is reasonable to think the malware has been evolved.	• Keep the systems updated and Patched • Secure browsers from malicious websites • Regularly monitor the network and endpoints • Perform the principle of least privilege • Foster a culture of cybersecurity (Chen, 2017)
Malware posing as other legitimate applications or mimicking their traffic behavior	Android/ Twitoor.A	SMS, malicious URLs	**Which is its main purpose:** Designed to control botnets through Direct Messages from Twitter rather than a conventional control-and-command server. (Barth, 2016) **How It works:** Attackers create some fake profiles to post encrypted commands to the malware. The infected computers ask for new commands to its “boostmaster”. This kind of structure, a botnet using C&C, built upon a social media is extremely difficult to be detected and takedown which allows malware to be active during a long period of time. (Paganini, 2015)	The malware is not active and is not a threat by itself. However, every user should be cautious and suspicious when using social networks whether using company’s endpoints or whether using professional profiles in personal endpoints.

Threat Technique	**Malware**	**Format used**	**Available information**	**Tools, Techniques & Countermeasures**
			How it is deployed: A maliciously Twitter account receives instructions for actions like downloading secondary payloads to be installed. (Barth, 2016) **Malware Today:** The project was a PoC and the Python code was available on GitHub. Some developers were invited to fork the project. It is not active as a malware.	
	Irongate		**Which is its main purpose:** To compromise industrial control systems (ICS), by controlling industrial processes in a simulated Siemens control system environment (Paganini, 2016) **How I t works:** Replaces a DDL with a malicious one, which acts a broker between a PLC and the legitimate monitoring application. The new DLL records five seconds of 'normal' traffic from the PLC to the application, sending after different data back to the PLC, while it replays the recorded to process operators. (Homan, 2016) **How it is deployed:** It seems to require manual execution. It was not identified what triggers the payload to install. (Homan, 2016) **Malware Today:** Developed as a Proof Of Concept, it never worked in the real world. Researchers hope this malware will never be evolved to a real threat.	Perform defensive techniques for ICS networks like: • Network security monitoring, • indicator of compromise (IoC) matching, • practice guidance from vendors Besides that, in the long run, it should be implemented solutions that: • Perform some checks of integrity between the code generated from vendor and user's code • Create mechanisms to check I/O data against expected process data (Homan, 2016)

Threat Technique	**Malware**	**Format used**	**Available information**	**Tools, Techniques & Countermeasures**
			(Homan, 2016), (Paganini, 2016)	
	Fakem RAT (Remote Access Trojan)	Covers its C&C traffic	**Which is its main purpose:** To keep its presence in a targeted network to perform Data Exfiltration when needed. ("Hiding in Plain Sight: The FAKEM Remote Access Trojan," 2013) **How I t works:** Performing a mixture between good and bad traffic and using ports allowed by firewalls. It uses HTTP and HTTPS to have normal look like traffic, but giving full control over the compromised systems ("Hiding in Plain Sight: The FAKEM Remote Access Trojan," 2013) **How it is deployed:** FAKEM are trojans and they are deployed as many other trojans are. In this case, steganography is used to uncover traffic and not to conceal malware code in media files. ("Hiding in Plain Sight: The FAKEM Remote Access Trojan," 2013) (Czyż, 2020) **Malware Today:** FAKEM is not a malware… is a family of remote access trojans. There always new ones and some of them are simply busted. (Donohue, 2013)	Using specific Anti Malware software that can help network administrators to detect the traffic the malware produces, which is easily detectable. Usually, attackers try to blend malicious traffic with legitimate one to avoid detection. Some attempt to disguise some traffic to look like Windows® Messenger and Yahoo!® Messenger traffic and some other to look like ordinary web traffic. ("Hiding in Plain Sight: The FAKEM Remote Access Trojan," 2013)
	Carbanak/ Anunak	Remote Access Trojan (RAT)	**Which is its main purpose:** To perform intrusions on banks' networks (Cimpanu, 2019), (Paganini, 2019) **How I t works:** Injected into bank employees' computers to compromise networks in order to	Recommended to perform a defense-in-depth approach to security. So, it is recommended to: • Keep the systems updated and Patched • Regularly monitor the network, firewalls and endpoints

<u>Threat</u> Technique	Malware	Format used	Available information	Tools, Techniques & Countermeasures
			gain access to sensitive systems capable of transferring money from a bank's accounts (Cimpanu, 2019), (Paganini, 2019) **How it is deployed:** Placed on VirusTotal list of files and where users could use them and being infected. VirusTotal is an Antivirus. (Cimpanu, 2019), (Paganini, 2019) But it is usually spread through email attachments, sending a VB script attached file and asking the victim to open attach file. (Paganini, 2019), (Mendrez, 2016) **Malware Today:** The original group that developed the malware was arrested in 2018 by Europol. But in 2019 it was reported that some members of the initial group had split into smaller groups, so it is most likely they are still evolving this malware to target banks accounts. (Cimpanu, 2019), (Paganini, 2019)	• Perform the principle of least privilege • Foster a culture of cybersecurity • Protect bank accounts avoiding accessing them through the infected computer • Use a security software capable of detecting it and removing it (GoldSparrow, 2015)
	SpyNote Trojan	Remote Access Trojan (RAT)	**Which is its main purpose:** Like many other RATs, the main purpose is to control devices. In this case, this malware was found in a surveillance campaign targeting Syrian citizens was state-sponsored. The purpose was to infect Android mobile devices to spy people who owns these devices. (Czyż, 2020) **How I t works:** It may masquerade as a legitimate application. Malware, after successful installation, would install a legitimate embedded application Then, connects to a C2 server to control cell phone applications	Subscription of a malware protection and remediation software for protecting PCs from malware (“SpyNote RAT,” 2019)

<u>Threat</u> Technique	Malware	Format used	Available information	Tools, Techniques & Countermeasures
			(Czyż, 2020) **How it is deployed:** Apps are shared through several channels, although they are not available in Google Play Store. Users are cheated and download and install these innocent-looking apps which are spywares. The malware is usually spread through spear phishing an attachment or a link. (Czyż, 2020) **Malware Today:** It has been updated. The MobiHok RAT is one of the examples of it. ("SpyNote RAT," 2019)	
	domain fronting (Technique)	HTTPS traffic	**Which is its main purpose:** To bypass internet traffic hiding the traffic to a specific website by masking it as a different domain. It is very useful to bypass censorship. But an attacker can obfuscate its traffic and his consequent attacks. (Truong, 2021) **How I t works:** It fakes the destination of the client's message by rerouting it through CDN. To the firewall, the HTTPS request appears to be going to a legitimate site, but it is going to a malicious site which is usually blocked. The domain names become different at different network layers. (Truong, 2021) **How it is deployed:** DNS Fronting is a technique and not a malware. Its installation is rather complex, but very sophisticated:	Prevention is the best way to fight DNS Fronting. So, it should be set a proxy server for all internet connections leaving the organization's network. Proxy servers can be configurated to see whether the "http 1.1 header domain is the same that is in the URL" or not. When the domains can't match to each other the system should report an alert. (Truong, 2021), (Henson Security Tools, 2019) Although, there is always the possibility to proactive try to detect whether traffic is malicious or not, by using a combination between JA3 Fingerprints with Unsupervised Machine Learning techniques. The algorithm can learn how to recognize some patterns from the dataset. This simply can detect whether the client application is

Threat Technique	Malware	Format used	Available information	Tools, Techniques & Countermeasures
			1. The cyberattacker sets a server on the same CDN as the target company's server 2. Once installed, probably through phishing, calls back but the call does not to attacker's domain, but to legitimate domain hosted on the CDN, setting a TLS communication between Malware and the server hosted on the CDN. (Henson Security Tools, 2019) **Malware Today:** Is not a malware. Is a technique and it largely used to bypass censorship in third-world countries or in countries where there is no freedom of speech.	malicious or not. (Truong, 2021)
Information hiding in ransomware	TeslaCrypt (spread using the Neutrino exploit kit)	HTML comments tag	**Which is its main purpose:** It is a Ransomware. It encrypts files and asks for a ransom of $500 to rescue the system through a decryption key. (Sai, 2015), (Dell SecureWorks Counter Threat UnitTM Threat Intelligence, 2015) **How I t works:** Generates a memory corruption vulnerability. Then, uses the vulnerability to execute code and infect unpatched computers.It infects gaming files, game saves, user profiles, etc, among other file types. (Sai, 2015), (Kaspersky, n.d.) **How it is deployed:** The malware infected computers through the Adobe Flash exploit known as Angler. (Sai, 2015) **Malware Today:** Already extinct. Master key has been released (Abrams, 2016a)	• Keep the system backup, especially the most important files on a regular basis. Keep the backups in safe drive and disconnected form the systems. • Patch and update the software of the systems • It is crucially important to update your software in a timely fashion, especially the web browser and its plugins. • Install a security software like an anti-virus with updated databases of the most recent virus, malware, trojans and other of malicious software. (Kaspersky, n.d.)

<u>Threat</u> Technique	Malware	Format used	Available information	Tools, Techniques & Countermeasures
	Cerber	Image / JPEG	**Which is its main purpose:** It is a RansomWare. It encrypts computers files and then holds them hostage, demanding a ransom payment to enable decryption. But this malware is a RaaS (Ransomware as a Service), which is licensed to other criminals in exchange for a percentage of the ransom. (Belcic, 2021) **How I t works:** It encrypts files, giving new extension to files, and lock them up until its decryption with the correct decryption key. It can also be spread through network shares. (Belcic, 2021) **How it is deployed:** Through malvertising, infected websites or phishing emails. Installation can happen by opening infected attachments or websites, or hitting a malicious ad. (Belcic, 2021) **Malware Today:** The malware is still active. (Belcic, 2021)	AntiVirus Prevention is always the best method to fight ransomware, and all organizations must foster a cybersecurity culture among users, by training them to: • Be suspicious about emails and attachments. Even from apparently known names, but emails out of context or written in strange way. • Do not click in links even they appear be trustful, because sometimes the URL of the link is not the same as the redirected URL • Do not click on ads • Back up systems in a regular basis • Keep systems patched and with the last version software • Use an anti-ransomware to protect in case on infection. Belcic, 2021)
	SyncCrypt	image	**Which is its main purpose:** It is a RansomWare. After encrypting victim's system ask for $429 for the decryption key file, which it will be sent by email. (Paganini, 2017) **How I t works:** The execution of an attachment extracts the Jscript file embedded in an image.	• Perform regular backups • Keep the systems updated and Patched • Regularly monitor the network and endpoints • Perform the principle of least privilege • Foster a culture of cybersecurity among the users

Threat Technique	Malware	Format used	Available information	Tools, Techniques & Countermeasures
			The hidden file is a ransomware which it will encrypt files from the system. Files are encrypted using AES encryption and the malware schedules a task to scan the system for some file types to be encrypted. (Paganini, 2017) **How it is deployed:** Spread through spam emails with attachments containing Windows Scripting files. Mails are fake and are sent as court orders. (Paganini, 2017) **Malware Today:** In December 2021 it was reported as still active with a high damage level. (Meskauskas, 2021)	• Provide a systematic scan of all attachments with an anti-virus • Install security software on the systems • Make sure every account and system are protected with hard passwords • use proper software for its generation • make sure the passwords are unique for each system – do not reuse passwords. (Abrams, 2016b), (Paganini, 2017)
Information hiding in exploit kits	Stegano/ Astrum	Image / PNG	**Which is its main purpose:** For many purposes, from financial information and personal one to file encryption. (Chen, 2017) **How I t works:** If the malicious Flash file is successful, it will download the payload onto the victim's machine. (Shargh, 2017) **How it is deployed:** It is used as part of the AdGholas malvertising campaign. The campaign uses scripts in banner ads on legitimate websites. The scripts executed redirect users to an Astrum exploit kit server which attacks the user's computer.	Very difficult to detect because uses encryption in the malicious payload which bypasses most of the signature-based antivirus. It shall be needed good endpoint protection in order to catch Astrum just after flash files is decrypted and before its execution. (Shargh, 2017) Even tough, there is some software pretending to be ant-virus, like the Astrum Anti-virus Pro. Which is a fake anti-spyware program. After its installation, it starts to report many notifications alerting about fake issues that user must remove. Organizations must be suspicious and to license only certified anti-virus software. (*How to Remove Astrum Antivirus Pro (Uninstall Instructions)*, 2008)

Threat Technique	Malware	Format used	Available information	Tools, Techniques & Countermeasures
			(Shargh, 2017) **Malware Today:** Like any other Trojan it has been evolved. Recent payloads can include other malware. Most recently Astrum was spreading the Mole Ransomware. So, despite some vulnerabilities have been patched, systems with software outdated (Windows system not updated) are still at risk. (Shargh, 2017)	
	DNSChanger		**Which is its main purpose:** To change systems' DNS configurations in order to, for instance: • Redirect users' computers to malicious sites • Delivering addition malware, like FAKEAV • Use fake ads on redirect sites as legitimate ones in the legitimate sites • Avoid users to update their computers with real security software . (Celestino, 2012) **How I t works:** Modifies systems' DNS settings, without the users noticing, to use foreign DNS servers, prepared by cybercriminals to redirect to malicious sites when trying to access certain sites. . (Celestino, 2012) **How it is delivered and activated:** Dropped by other malware which after is installed, silently modifies systems' DNS settings **Malware Today:**	The technique to fix the problem is to reset the DNS Settings. It should be supported on a IT professional to perform the tasks required when resetting the DNS Settings. After fixing the problem, it should be installed a good anti-virus to remove the Trojan and avoid being reinfected. (Celestino, 2012)

Threat Technique	Malware	Format used	Available information	Tools, Techniques & Countermeasures
			In 2011 the Rove Digital Command-and-Control was identified. The botnet has been removed. (Celestino, 2012)	
	Sundown	Image / PNG files	**Which is its main purpose:** Sundown drops Chthonic banking Trojan, which is a variant of the Zeus malware, that was used in scam with the pay pal system, which "requested money" from users. (SecurityWeek News, 2016) **How I t works:** By exploiting vulnerabilities in Adobe Flash (.swf), Silverlight (.xap), JavaScript files, and many others. ("Updated Sundown Exploit Kit Uses Steganography," 2016) **How it is deployed:** Through malvertising campaigns and encoding a script in the alpha channel of the PNG image of the ad. The alpha channel is where it is defined the transparency of the pixels, turning very difficult its detection. ("Updated Sundown Exploit Kit Uses Steganography," 2016) **Malware Today:** Still active. In 2019 it was reported in North America and Europe. (Segura, 2021)	Like Astrum countermeasure, in this case a good endpoint solution shall be taken to detect and act against the malware in real-time. Some solutions can block the exploit every time the tries to access the URL is hosted in. ("Updated Sundown Exploit Kit Uses Steganography," 2016)

Table 8 – Actions should be taken to overcome malware infection using Steganography

4.4.2. 2nd Strategy – using steganalysis tools and techniques

Another line of defense to prevent steganography is to use steganalysis. This method is much more driven to detect files with steganographic content. Whereas the previous method was to find software produced to be spread using steganography, the present method tries to find carrier files to clean them up before its content can deploy any malicious code. Note that not every malicious code can be part of a malware.

In the market there are some software to help researchers and investigators to detect and clean files and applications that can generate steganographic information.

Tool Name	**Main Purpose**	**Functionalities**	**In which formats it operates**	**In which situations can be used**		
				Scenario	**Technique**	**Limitations**
StegSpy	Detects steganographic content on files (N. A. Hassan & Hijazi, 2017)	Detects if the carrier stores any steganographic content. It just can detect steganography made from the following software: • JPHideandSeek, • Hiderman • Masker • JPegX, • Invisible Secrets (M. Hassan et al., 2020)	All files produced by Steganography Software such as: • JPHideandSeek, • Hiderman • Masker • JPegX, • Invisible Secrets (just images) (N. A. Hassan & Hijazi, 2017)	Incoming email	Stegspy shall automatically analyze email text and its attachments to detect whether there is any steganographic content on the mail body, header or in its attachments before anyone can execute it.	• The software cannot be automated on a service. It must be used upon each file manually. • Applied only to files generated to a limited number of software,
				Downloading a file from a site and/or transferring from an ftp server	Stegspy shall automatically analyze the downloaded file to detect whether there is any steganographic content on the in it before anyone can execute it.	
				Introducing a flash drive/external disk on laptop/desktop.	Stegspy shall automatically analyze the downloaded file to detect whether there is any steganographic content on the in it before anyone can execute it.	

Tool Name	Main Purpose	Functionalities	In which formats it operates	In which situations can be used		
				Scenario	Technique	Limitations
Stegdetect & Stegbreak – a set of tools provided separated but developed by Niels Provos under the same principles						
Stegdetect	Detects steganography on image files (N. A. Hassan & Hijazi, 2017)	Detects steganographic content in JPEG image (N. A. Hassan & Hijazi, 2017)	All image (some just on jpg format) files produced by Steganography Software such as: • JSteg, • JPHide, • Invisible Secrets, • OutGuess, • F5, • Camouflage, • appendX (N. A. Hassan & Hijazi, 2017)	Incoming email	Steodetect shall automatically analyze email text and its attachments to detect whether there is any steganographic content on the mail body, header or in its attachments before anyone can execute it.	Stegodetect can be automated, but limited to files generated by specific number of software applications N. A. Hassan & Hijazi, 2017)
				Downloading a file from a site and/or transferring from an ftp server	Steodetect shall automatically analyze the downloaded file to detect whether there is any steganographic content on the in it before anyone can execute it.	
				Introducing a flash drive/external disk on laptop/desktop.	Steodetect shall automatically analyze the downloaded file to detect whether there is any steganographic content on the in it before anyone can execute it.	
Stegbreak	Cleans files with Steganographic content (N. A. Hassan &	Used in conjunction with Stegdetect, it breaks the file with dictionary attacks to the file to extract the correct image and the file	Files generated by • JSteg-Shell • JPHide	After file detection it can be broken to remove stego-object on it.	Applying directly on the file to break it.	N/A

Tool Name	Main Purpose	Functionalities	In which formats it operates	In which situations can be used		
				Scenario	Technique	Limitations
	Hijazi, 2017)	inside of it (M. Hassan et al., 2020)	• OutGuess 0.13b (N. A. Hassan & Hijazi, 2017)			
Stego Suite – a set of tools provided as a package						
Stego Hunter	Detects steganography programs	Finds steganography applications on the entire system. It allows to identify carrier files associated to those applications. (M. Hassan et al., 2020)	Media files: • Image • Bmp • Gif • Png • jpg • Sound • Wav (M. Hassan et al., 2020)	Used for Digital Forensics to collect evidence of using steganography tools to intentionally hide malicious contents on files.	Used directly on assessed system	N/A
Stego Watch	Detects steganographic content on files (M. Hassan et al., 2020)	After having marked files, the software scans the whole file (M. Hassan et al., 2020)				
Stego Analyst	To make a deep analysis on a carrier file (M. Hassan et al., 2020)	Gets evidence that steganography is being used in media files.				
Stego Break	To get the password phrase in a carrier file	Using a dictionary attack				

Tool Name	Main Purpose	Functionalities	In which formats it operates	In which situations can be used		
				Scenario	Technique	Limitations
StegAnalyzer – 3 different types of tools						
StegAlyzerAS - Steganography Analyzer Artifact Scanner	Digital forensic tool to perform analysis on wider scale (M. Hassan et al., 2020)	It scans suspected media or suspected media images in some steganography applications. (M. Hassan et al., 2020)	Information not available	Not applicable. I tis used for Digital Forensics	–	–
StegAlyzerSS - Steganography Analyzer Signatures Scanner	Digital forensic tool to scan files on suspicious media (M. Hassan et al., 2020)	It scans for files on suspicious media looking for signatures within the files. (M. Hassan et al., 2020)	Information not available	Not applicable. I tis used for Digital Forensics	–	–
StegAlyzerRTS - Steganography Analysis Real-Time Scanner	Network security application - provides real time detection of digital steganography. (M. Hassan et al., 2020)	Performs real time analysis on carrier files to detect fingerprints and signatures. Widely used either to detect internal use of steganography downloaded software and to detect insider downloading by comparing the fingerprints of the files. (M. Hassan et al., 2020)	Information not available	Incoming email	StegAlyzerRTS shall automatically analyze email text and its attachments to detect whether there is any steganographic content on the mail body, header or in its attachments before anyone can execute it.	–
				Downloading a file from a site and/or transferring from an ftp server	StegAlyzerRTS shall automatically analyze the downloaded file to detect whether there is any steganographic content on the in it before anyone can execute it.	–

Tool Name	Main Purpose	Functionalities	In which formats it operates	In which situations can be used		
				Scenario	Technique	Limitations
				Introducing a flash drive/external disk on laptop/desktop.	StegAlyzerRTS shall automatically analyze the downloaded file to detect whether there is any steganographic content on the in it before e anyone can execute it.	–

Table 9 – Tools to detect and clean steganographic content files and applications

4.4.3. Use Cases

4.4.3.1. Malware Summary

Technique	Malware	Method	Purpose	Distribution	Most likely covered Scenario
Tampering digital media files	Vawtrak/ Neverquest	Modification of LSBs of favicons in websites	Hides an URL to download a config file	It can be delivered through 3 different ways: • attached in an email as malvertisement a campaign • As the payload to an exploit kit: For instance, a malicious flash redirector. • downloaded by loader malware delivered through the exploit kit or the spam email: through loader malware that downloads the installer	Very comprehensive methods. It can be framed in scenarios that involve: • Images though LSB modification • And that your delivery method is one of the following 3: • Mail attachment ➡ ***Scenario 10*** • As part of an exploit kit ➡ ***Scenario 9*** • As a payload to an exploit kit, like a favicon, or an ad with flash ➡ ***Scenario 4***
	Zbot	Appends data to a JPEG file (at the end of the file)	Hides configuration data	The malware reaches the user through • spammed email messages, probably with links and regarding malvertisment • downloaded from compromised websites.	It can be framed in scenarios that involve: • Tampering a JPEG file • And that your delivery method is one of the following 2: • spammed messages ➡ ***Scenario 10*** • Website ➡ ***Scenario 3***
	Lurk/ Stegoloader	Modification of the LSBs of BMP/PNG files	Hides an encrypted URL for downloading additional malware components	Through an HTML on compromised websites that loaded a Flash-based exploit	It can be framed in scenarios that involve: • Modifying BMP and/or PNG files • And delivered through an Exploit Kit through flash file in website ➡

Technique	Malware	Method	Purpose	Distribution	Most likely covered Scenario
					Scenario 9
	AdGholas	Data hiding in images, text, and HTML code	Hiding encrypted malicious JavaScript code	Using Malvertisement campaigns, by exploiting flaws in the delivery of ads.	It can be framed in scenarios that involve: • Modifying images, and text and html code • Delivered by malvertisement campaigns with flash ads ➡ ***Scenario 10***
Acting as a legitimate app	Android/ Twitoor.A	Disguised as a pornography player or an MMS app	Cheating users to install malicious apps	Through phishing/smishing	Addressed in scenarios that involve: • Mobile apps mimicking legitimate ones ➡ ***Scenario 7***
	Irongate	Malicious DLL disguised as a legitimate one.	Impersonates good commands to PLC system with malicious ones but returning good outcome to the users	Like the Stuxnet, using a flash drive	Addressed to scenarios involving situations that users bring their own devices to the company's ecosystem ➡ ***Scenario 6***
	Fakem RAT	Impersonates MSN and Yahoo Messenger messages or HTTP conversation traffic	It conceals C&C traffic	Deployed as many other trojans are	No established scenario regarding steganography. It can be deployed in many different ways. However, MSN and Yahoo Messenger are both in disuse for communicating between people. Peers today use Whatsapp, Themes or Zoom, among others.
	Carbanak/ Anunak	Through Google cloud- based services	It conceals C&C traffic	It is listed 2 possible ways: • Placed on VirusTotal list of files • spread through email attachments, sending a VB script attached file	When somehow the user installs a malware received from: • phishing, mail attachments ➡ ***Scenario 8*** • downloads from a site thinking the

Technique	Malware	Method	Purpose	Distribution	Most likely covered Scenario
					downloaded file are completely harmless due the confidence from the source ➡ ***Scenario 5***
	SpyNote Trojan	Impersonating Netflix app	Tricking users into installing malicious app to gain access to confidential data	Through phishing/smishing	Addressed in scenarios that involve: • Mobile apps mimicking legitimate ones ➡ ***Scenario 7***
	Domain fronting	Bypasses the internet traffic through a specific website by masking it as different domain.	Obfuscate traffic in cases of censorship	Is a technique and not a malware. However, the most likely way to this technique is initially deployed is through email phisihing.	• Besides this does not install any kind of malware, it is reliable to be initialized through email phisihing ➡ ***Scenario 10***
Through a ransomware	TeslaCrypt	Data hiding in HTML comments tag of the HTTP 404 error message page	Embedding C&C commands	–	Decommissioned
	Cerber	Image steganography	Embedding malicious executable	Using: • Malvertising • Infected websites • phishing emails.	It can be framed in scenarios that involve: • Modifying an image file • And that your delivery method is one of the following 3: • spammed messages ➡ ***Scenario 10*** • infected Website ➡ ***Scenario 3*** • Malvertising ➡ ***Scenario 10***
	SyncCrypt	Image steganography	Embedding core components of ransomware	Through spam emails with attachments containing Windows Scripting files	It can be framed in scenarios that involve: It can be framed in scenarios that

Technique	Malware	Method	Purpose	Distribution	Most likely covered Scenario
					involve: • Modifying an image file • And that its delivery method is the following one: • Email spammed messages with attachments ➡ ***Scenario 1***
Through an exploit kits	Stegano/ Astrum	Modifying the color space of the used PNG image	Hiding malicious code within banner ads	Used as part of the AdGholas malvertising campaign.	Same scenarios as regarding AdGholas malware
	DNSChanger	Modification of the LSBs of PNG files	Hiding malware AES encryption key	Through malware that was installed	All Scenarios addressing steganography through PNG files, which are: • Lurk/ Stegoloader ➡ ***Scenario 9*** • Stegano/ Astrum (AdGholas) ➡ ***Scenario 10*** • Sundown ➡ ***Scenario 9***
	Sundown	Hiding data in white PNG files	Exfiltrating user data and hiding exploit code delivered to victims	Through the vulnerabilities of: • Adobe Flash (.swf) • Silverlight (.xap) • JavaScript files • others	It can be framed in scenarios that involve: • Modifying PNG file • And that its delivery method is the following one: • Website with an ad banner ➡ ***Scenario 9***

Table 10 – Malware summary through covered scenarios

4.4.3.2. Use Cases through techniques

In the following table is a listing that maps the expected malware with the studied situation and its response techniques in each phase.

Covered Scenario (# + description)		**Expected Malwares**	**Comments and possible Damages**	**Toolbox usage**	
				Phase	**Techniques**
1	A user receives an email with an image in attach and clicks in it. The file opens and executes a hidden code.	• SyncCrypt	Innocent-looking pictures can be seen as harmless, but it can hide a ransomware. Ransomwares can block the user machine as well be spread all the network infecting and blocking other computers. Even though, there are tools that can provide automatic detection in images, this being the first line of defense, usually promoting the analysis of email attachments before they can be delivered to users. In addition, there is security software available that can prevent the installation of malware, this being the second line of defense in depth	Prevention	• Training Sessions • Security Software installation and automation for real time detection: • Anti-Virus • Anti-Malware • Steganography detection Software • Network segmentation and Systems configurations • Set a Business Continuity and Recovery plan or include the steganography actions on them
				Reaction	• Isolate suspicious files • Run steganography clean tool over the suspected files to extract the stego-object from carrier file • Contact the authorities in case of an attack
				Collection	• Extract information the from the Security Software to collect IoCs • Get information regarding the malware like: • Name • Damages caused • Developer and its motivation • Deployment technique
				Documentation	• Update the information regarding new malware • Update the workflow of the toolbox

Covered Scenario (# + description)		Expected Malwares	Comments and possible Damages	Toolbox usage	
				Phase	Techniques
				Update	• Update training programs for next training sessions • Update the techniques set • Perform new strategies on the system
2	A user receives an email with unsuspicious PDF Document and clicks in it. The file opens and executes a hidden code.	Malware placed in nonexecutable files are very dangerous because: • are easy to bypass some security programs, delivering a high risk of false positives • they are often considered having lesser risk by common users (Jeong et al., 2019)	PDFs are less suspicious formats having malware. However, they are easy to bypass. Malware can infect not only the user's machine, as well be spread through all the network infecting and blocking other computers There is no tool or method to prevent this type of Steganography. Preventing malware installed by execution code hidden in PDF Files may be resolved by preventing the malware	Prevention	• Training Sessions • Security Software installation and automation for real time detection: • Anti-Virus • Anti-Malware • Set a Business Continuity and Recovery plan or include the steganography actions on them
				Reaction	• Isolate suspicious files • Contact the authorities in case of an attack
				Collection	• Extract information the from the Security Software to collect IoCs • Get information regarding the malware like: • Name • Damages caused • Developer and its motivation • Deployment technique
				Documentation	• Update the information regarding new malware • Update the workflow of the toolbox
				Update	• Update training programs for next training sessions • Update the techniques set

Covered Scenario (# + description)		Expected Malwares	Comments and possible Damages	Toolbox usage	
				Phase	Techniques
					• Perform new strategies on the system
3	A user clicks on an innocent-looking image posted on a website that has malware placed inside with steganography technique. The malware is installed after the image has been opened	• Zbot / Zeus • Cerber • SyncCrypt	Innocent-looking pictures can be seen as harmless, but it can hide a ransomware or any other malware. Malware can infect not only the user's machine, as well be spread through all the network infecting and blocking other computers Even though, there are tools that can provide automatic detection in images, this being the first line of defense, usually promoting the analysis of files when being uploaded to memory and before being opened. In addition, there is security software available that can prevent the installation of malware, this being the second line of defense in depth	Prevention	• Training Sessions • Security Software installation and automation for real time detection: • Anti-Virus • Anti-Malware • Steganography detection Software • Network protection policies and Systems configurations • Set a Business Continuity and Recovery plan or include the steganography actions on them
				Reaction	• Isolate suspicious files • Run steganography cleaning tool over the suspected files to extract the stego-object from carrier file • Contact the authorities in case of an attack
				Collection	• Extract information the from the Security Software to collect IoCs • Get information regarding the malware like: • Name • Damages caused • Developer and its motivation • Deployment technique
				Documentation	• Update the information regarding new malware • Update the workflow of the toolbox

Covered Scenario (# + description)		Expected Malwares	Comments and possible Damages	Toolbox usage	
				Phase	Techniques
				Update	• Update training programs for next training sessions • Update the techniques set • Perform new strategies on the system
4	A user clicks on a web ad, and which is installed after the ad icon has been clicked on	• Vawtrak/ Neverquest	Advertisements can always hide numerous problems. They are designed to be eye-catching and their appealing appearance and well-intentioned message is just a deception to get them clicked. These can hide links and malware that install backdoors into your system. Malware can infect not only the user's machine, as well be spread through all the network infecting and blocking other computers Even though, there are tools that can provide automatic detection in images, this being the first line of defense, usually promoting the analysis of files when being uploaded into memory and before being opened. In addition, there is security software available that can prevent the installation of malware, this being the second line of defense in depth	Prevention	• Training Sessions regarding Cyber Security • Do not allow administration privileges on company's end points • Security Software installation and automation for real time detection: • Anti-Virus • Anti-Malware • Steganography detection Software • StegAnalyzer to detect covert channels network traffic • Network protection policies and Systems configurations • Every now and then it should perform a system scan with Steganography cleaning tool Stegspy, which scans files and applications through all system. Set a Business Continuity and Recovery plan or include the steganography actions on them
				Reaction	• Isolate suspicious files • Run steganography cleaning tool over the suspected files to extract the stego-object from carrier file Contact the authorities in case of an attack

Covered Scenario (# + description)		Expected Malwares	Comments and possible Damages	Toolbox usage	
				Phase	Techniques
				Collection	• Extract information the from the Security Software to collect IoCs • Get information regarding the malware like: • Name • Damages caused • Developer and its motivation • Deployment technique
				Documentation	• Update the information regarding new malware • Update the workflow of the toolbox
				Update	• Update training programs for next training sessions • Update the techniques set • Perform new strategies on the system
5	A user clicks on an image obtained through a download from a web site, torrent, ftp server, which contains a malware placed through steganographic methods and which deploys a malware	• Carbanak/ Anunak	Innocent-looking pictures can be seen as harmless, but they can hide a ransomware or any other malware. Malware can infect not only the user's machine, as well be spread through all the network infecting and blocking other computers Even though, there are tools that can provide automatic detection in images, this being the first line of defense, usually promoting the analysis of files when being uploaded to memory and before being opened.	Prevention	• Training Sessions regarding Cyber Security • Do not allow administration privileges on company's end points • Security Software installation and automation for real time detection: • Anti-Virus • Anti-Malware • Steganography detection Software • StegAnalyzer to detect covert channels network traffic • Network protection policies and Systems configurations • Every now and then it should perform a system scan with Steganography cleaning tool Stegspy,

Covered Scenario (# + description)		Expected Malwares	Comments and possible Damages	Toolbox usage	
				Phase	Techniques
			In addition, there is security software available that can prevent the installation of malware, this being the second line of defense in depth		which scans files and applications through all system. • Set a Business Continuity and Recovery plan or include the steganography actions on them
				Reaction	• Isolate suspicious files • Run steganography cleaning tool over the suspected files to extract the stego-object from carrier file • Contact the authorities in case of an attack
				Collection	• Extract information the from the Security Software to collect IoCs • Get information regarding the malware like: • Name • Damages caused • Developer and its motivation • Deployment technique
				Documentation	• Update the information regarding new malware • Update the workflow of the toolbox
				Update	• Update training programs for next training sessions • Update the techniques set • Perform new strategies on the system
6	A user clicks in an innocent-looking image or PDF, placed in a filesystem (on-premises or cloud) irregularly brought to inside	• Vawtrak/ Neverquest • Zbot / Zeus • Lurk / Stegoloader • AdGholas	Users that bring their own device to the organization's network need to be aware that their equipment might be an infection starting point and they are putting the at risk by	Prevention	• Training Sessions regarding BYOD policies • Do not allow administration privileges on company's end points • Security Software installation and automation for real time detection:

Covered Scenario (# + description)		Expected Malwares	Comments and possible Damages	Toolbox usage	
				Phase	Techniques
	the organization (p.e. through a flash drive), and which is installed after the file had been opened	- Irongate - Carbanak/ Anunak - Cerber - SyncCrypt - Stegano/Astrum - DNSChanger - Sundown	compromising systems and end points. Even though, there are tools that can provide automatic detection in images, this being the first line of defense, usually scanning the system (servers, network, and personal computers) defined as a system policy. In addition, there is security software available that can prevent the installation of malware, this being the second line of defense in depth. Finally, there should address a very narrow policy regarding using equipment from outside of the park of the company's devices.		- Anti-Virus - Anti-Malware - Steganography detection Software - StegAnalyzer to detect covert channels network traffic - Network protection policies and Systems configurations - Create different Wifi Networks for internal equipment and for guest users' devices - External users should be connected under a VPN connection - Every now and then it should perform a system scan with Steganography cleaning tool Stegspy, which scans files and applications through all system. - Set a Business Continuity and Recovery plan or include the steganography actions on them
				Reaction	- Isolate suspicious files - Run steganography cleaning tool over the suspected files to extract the stego-object from carrier file
				Collection	- Extract information the from the Security Software to collect IoCs - Get information regarding the malware like: - Name - Damages caused - Developer and its motivation

Covered Scenario (# + description)		Expected Malwares	Comments and possible Damages	Toolbox usage	
				Phase	Techniques
					- Deployment technique
				Documentation	- Update the information regarding new malware - Update the workflow of the toolbox
				Update	- Update training programs for next training sessions - Update the techniques set - Perform new strategies of having cell phones to coworkers
7	A user is tricked thinking to be installing a legitimate pornography player or an MMS app installs an impersonated app. A malware is placed in a mobile phone app through steganography techniques	There are some malwares that can impersonate others and that look like the legitimate ones, like: - Twitoor.A - SpyNote Trojan	Users are tricked through phishing or smishing to install apps that look like legitimate ones. After its installation it allows the cyberattacker to use C&C on the device, performing some actions, like copying files, get user contacts. This type of malware is hard to be detected.	Prevention	- Training Sessions regarding installing mobile applications risks - Use Unified Endpoint Management (UEM) tools to manage, monitor, configurate Mobile Operating Systems, IoT, and wearable endpoints. - Do not allow administration privileges on company's endo points
				Reaction	- Uninstall the app - Perform a scan to clean up installed malware on the end point.
				Collection	- Extract information the from the Security Software to collect IoCs - Get information regarding the malware like: - Name - Damages caused - Developer and its motivation

Covered Scenario (# + description)		Expected Malwares	Comments and possible Damages	Toolbox usage	
				Phase	Techniques
					- Deployment technique
				Documentation	- Update the information regarding new malware - Update the workflow of the toolbox
				Update	- Update training programs for next training sessions - Update the techniques set - Perform new strategies of having cell phones to coworkers
8	Due to some installation user's computer or even the server starts to be commanded by an external server. Hidden commands through steganography techniques are sent through network packages	- Fake Rat - Carbanak/ Anunak	Although some malware can be prevented by security software, there is a new line of defense that can be provided by tools to prevent the steganography through traffic. Not all situations can be prevented with anti-malware. It always shall be done a closest look to network traffic to detect suspicious users, suspicious access attempts, suspicious running processes and applications, and many other surveillance techniques.	Prevention	- Training Sessions regarding cybersecuirty policies - Do not allow administration privileges on company's end points - Security Software installation and automation for real time detection: - Anti-Virus - Anti-Malware - Steganography detection Software - StegAnalyzer to detect covert channels network traffic - Network protection policies and Systems configurations - Every now and then it should perform a system scan with Steganography cleaning tool Stegspy, which scans files and applications through all system. - Set a Business Continuity and Recovery plan or include the steganography actions on them

Covered Scenario (# + description)		Expected Malwares	Comments and possible Damages	Toolbox usage	
				Phase	Techniques
				Reaction	• Isolate suspicious files • Run steganography cleaning tool over the suspected files to extract the stego-object from carrier file • Contact the authorities in case of an attack
				Collection	• Extract information the from the Security Software to collect IoCs • Get information regarding the malware like: • Name • Damages caused • Developer and its motivation • Deployment technique
				Documentation	• Update the information regarding new malware • Update the workflow of the toolbox
				Update	• Update training programs for next training sessions • Update the techniques set • Perform new strategies of having cell phones to coworkers
9	A user clicks on an ad banner which has flash vulnerability and installing an Exploit Kits, where the victim without knowing is redirect to an exploit kit landing page, The victim's computer is exploited by	• Vawtrak/ Neverquest • Lurk/ Stegoloader • Sundown	Advertisements can always hide numerous problems. They are designed to be eye-catching and their appealing appearance and well-intentioned message is just a deception to get them clicked. These can hide links and malware that install backdoors into your system.	Prevention	• Training Sessions regarding Cyber Security • Do not allow administration privileges on company's end points • Security Software installation and automation for real time detection: • Anti-Virus • Anti-Malware

Covered Scenario (# + description)		Expected Malwares	Comments and possible Damages	Toolbox usage	
				Phase	Techniques
	searching for vulnerabilities and installing a malware to take the control of the computer		Even though, there are tools that can provide automatic detection in images, this being the first line of defense, usually scanning the system (servers, network, and personal computers) defined as a system policy. In addition, there is security software available that can prevent the installation of malware, this being the second line of defense in depth.		• Steganography detection Software • StegAnalyzer to detect covert channels network traffic • Network protection policies and Systems configurations • Every now and then it should perform a system scan with Steganography cleaning tool Stegspy, which scans files and applications through all system. • Set a Business Continuity and Recovery plan or include the steganography actions on them
				Reaction	• Isolate suspicious files • Run steganography cleaning tool over the suspected files to extract the stego-object from carrier file • Contact the authorities in case of an attack
				Collection	• Extract information the from the Security Software to collect IoCs • Get information regarding the malware like: • Name • Damages caused • Developer and its motivation • Deployment technique
				Documentation	• Update the information regarding new malware • Update the workflow of the toolbox
				Update	• Update training programs for next training sessions

Covered Scenario (# + description)		Expected Malwares	Comments and possible Damages	Toolbox usage	
				Phase	Techniques
					• Update the techniques set • Perform new strategies of having cell phones to coworkers
10	A user receives an email link or a Malvertisement campaign and installs a malware after the link or banner is clicked on	• Vawtrak/ Neverquest • Zbot • AdGholas • Cerber • Stegano/ Astrum	Maldvertising campaigns and links in emails are a way to be redirected to webpages that impersonates legitimate ones which it allows to install several kinds of malware. Even though, there are tools that can provide automatic detection in images, this being the first line of defense, usually scanning the system (servers, network, and personal computers) defined as a system policy. In addition, there is security software available that can prevent the installation of malware, this being the second line of defense in depth.	Prevention	• Training Sessions regarding Cyber Security • Do not allow administration privileges on company's end points • Security Software installation and automation for real time detection: • Anti-Virus • Anti-Malware • Steganography detection Software • StegAnalyzer to detect covert channels network traffic • Network protection policies and Systems configurations • Every now and then it should perform a system scan with Steganography cleaning tool Stegspy, which scans files and applications through all system. • Set a Business Continuity and Recovery plan or include the steganography actions on them
				Reaction	• Isolate suspicious files • Run steganography cleaning tool over the suspected files to extract the stego-object from carrier file • Contact the authorities in case of an attack
				Collection	• Extract information the from the Security Software to collect IoCs

Covered Scenario (# + description)		Expected Malwares	Comments and possible Damages	Toolbox usage	
				Phase	Techniques
					• Get information regarding the malware like: • Name • Damages caused • Developer and its motivation • Deployment technique
				Documentation	• Update the information regarding new malware • Update the workflow of the toolbox
				Update	• Update training programs for next training sessions • Update the techniques set • Perform new strategies of having cell phones to coworkers

Table 11 – Tools to detect and clean steganographic content files and applications

4.5. EVALUATION & DISCUSSION

4.5.1. Evaluation

In order to validate the present toolbox a panel of professionals was challenged to assess its logic and reliability when using it towards cybersecurity problems caused by steganography. Some questions were addressed to the panel where professionals were able to express their opinion based upon on their experience and knowledge, such as:

1. Is the presented toolbox reliable to act as guidance when facing steganography problems or the fight the malware that makes use of steganography to conceal data or to spread malicious code?
2. Do you agree with the presented toolbox? Do you think it should be added any extra item to complemented it?
3. Which improvements do you think it should be done to make it reliable?

The experts of panel are from organizations and institutions and who deal in a daily basis with the security of the ecosystems of those companies. The main goal was to get their best understanding and opinion based on their professional experience on how steganography can impact the wellbeing of their organizations and how they are really prepared to face this problem.

As a disclaimer, all experts agreed to be interviewed and agreed that their names be made public and that they could be available in this study.

On the appendixes chapter are reproduced the interviews made to experts.

4.5.2. Discussion

After the interviews done, the answers were analyzed. Those answers were very useful to understand how useful it is to have a manual to describe what the problem, what are their main threats and struggles, and to have a guidance to address the presented threats.

Regarding the questions made to the panel, it is important to retain the general opinions provided:

Question	Experts' general opinion
From what you currently know about steganography, either from your own experience or from what you have read, do you think that this is a subject that has been undervalued and deserves some additional attention?	None of the experts underestimate this kind of problem, although not all are fully aware of what steganography really means and what its techniques and impacts are. However, some do not consider this technique the main vector when an attack happens.
Steganography is also used through Covert Channels in the transmission of network packets. The concerns you have are the same, whether by the installation of malware through the loading of payloads coming in files, or Covert Channels in which information is stolen	Yes, all instructions at the lowest level of the operating system are analysed, allowing visibility that was not possible with traditional antivirus solutions. Additionally, in organizations with an information classification policy, the data considered confidential is treated with specific technical and procedural controls, at network level using layer7 firewalls that have the ability to see the packets and

Question	Experts' general opinion
without the notion that it is being exfiltrated?	understand if the data flows are reliable or not. Usually, SME have the protection that is provided via an endpoint solution, which may or may not provide protection from different steganographic techniques.
The framework proposed in this thesis is composed of a set of Best Practices, including a framework for action and appropriate tactical actions, such as the use of specific software (Anti-virus, Anti-Malware, Anti-Steganography) to prevent and react to possible attacks. Therefore, and looking at this reference tool, do you think it could be useful for organizations to help them combat possible security threats?	All initiatives that intend to create methodologies and/or policies to deal with cyber incidents are important to guarantee the pillars of information security: confidentiality, integrity, availability and authenticity within an organization. The creation of this framework is one more tool available and for that reason will help to combat possible threats and it is always useful to have an incident response Framework in place to enable organizations to quickly detect, contain and remediate threats. However, the framework should be unique and applied not only to steganography issues, but to all possible incidents that arise. This makes sure that processes linked to frameworks are not duplicated. An example of this is the NIST Framework.
Do you think that the market, today, is already equipped with solutions and the necessary software capable of dealing with this problem?	Solutions already exist and address many problems. But often, the problem is not the technology itself, but identifying the weaknesses and then identifying the controls that can mitigate them. It's a matter of simultaneously using technology with making cybersecurity a priority issue within an organization, starting with top-management, and following the entire hierarchical pyramid, with no exceptions.
Regarding to what you know of the security area, and among the most common attack vectors that you know of and have witnessed, what do you think is the biggest problem in terms of Cyber Security for companies?	The biggest problem is the lack of culture and training in companies, both in their employees and in Information Systems and Technologies professionals.
Regarding to what you said before, in what way can steganography also fit into one of these attack vectors (phishing, social engineering, etc.)? Or do you think that it is not currently a problem because it is an attack vector that is used seldom and even with little capacity to be applied because the existing technological solutions block and almost eliminate this risk?	Steganography is and will be in the future, a risk for businesses. Although many existing technological solutions already block many attacks, it will only take one successful one to compromise an entire company. It is commonly used in phishing attacks by hiding a legitimate name in an email address and tricking the user. It is this social engineering technique that is the main attack vector that has the highest success rate today and remains one of the most complex cases to mitigate.
Do you agree with the framework that has been proposed? Do you think that something should be added, namely	The framework has the main points aligned with a NIST which is the market reference, and the vulnerabilities are in line with the most common techniques within this attack vector.

Question	Experts' general opinion
some kind of vulnerability where steganography can be applied and that is not being considered in the toolbox?	However, with people being the biggest concern, a greater focus on training in areas that have more successful attacks due to steganography should be recommended.
Do you think this toolbox needs some improvement, some Best Practice that is not included in it, or some more tactical intervention approach to mitigate the risks and consequences of some attack to the organization?	An item that is always underrated and this is very important is the "lessons learned". To assess what went wrong and what went right and what could be done better to optimize the process based on what we learned from putting the framework into action. The framework should be embedded in an overall security framework aligned with people, processes and technology.

Table 12 – Experts' interviews opinions

5. CONCLUSIONS

5.1. SYNTHESIS

It is clear that a large part of the application of steganography is to be able to break through defense barriers and conceal a behavior, leading users to facilitate their movements

There are some main conclusions to be drawn from this study. The first one is that steganography in enterprises occurs primarily by installing malware, and as a way to hide information within what appears to be legitimate traffic. It is not used in a straightforward way, as a way of passing information in the expectation of stealing information or hiding messages with steganography. That is, it is not used by a user placing a message inside an image to send documentation outside the company.

Steganography is essentially used as a way to hide a behavior or hide some address that leads the user to activate the installation of a payload, and often the attack comes via phishing, such as maladvertising, It is used as an auxiliary way to get malware installed, by passing code hidden in images that browse through emails or in other ways to get files behind security lines.

Another conclusion is that the market already has good solutions at the lower layer of the operating system, providing systems with more effective answers than anti-virus itself. Also at the network level, using layer7 firewalls that have the ability to see the packets and understand if the data flows are trustworthy or to understand if there are data/packets going out through unusual ports or protocols. However, this does not detect steganography, but rather anomalous behavior.

The third conclusion is that the vulnerabilities generated by steganography in enterprises, and as in all cybersecurity, revolve around the logic of People, Processes and Technology. Technology does not solve everything. Processes must be reviewed frequently, always involving people. As explained by the experts, although there is technology, the biggest problem results from people. Not just normal users, but everyone, going even through the security teams, who sometimes don't master cybersecurity issues as much as they should. Therefore, as was proposed in framework, there should be a constant updating of knowledge, through internal and external training, by the entire organization. The culture of Cybersecurity must always be present and must be companywide.

As a last conclusion, and although this framework is a good source of work, it should be included in a global framework in which there are generic methodologies that cover several types of threats, and others oriented to each type of threat. Above all, these should always have a "Lessons Learned" evaluation plan to analyze what failed, to correct the processes, and what were the responses that allowed mitigating the attack, to be maintained and given as valid to continue to be used in the future.

Therefore, although steganography is a complex and difficult technique to detect, it is only used as a complement to the company's line-of-defense breaking techniques. So even with the tactical weapons to combat steganography, companies must strengthen their focus on the strategic side of countering behavior by:

- Keeping systems patched
- Making regular backups (full and incremental)
- Detecting and preventing social engineering
- Do not allow users to install software

5.2. LIMITATIONS

The first main limitation of steganography in enterprises comprises material that is not within a covert file, as stego-object. Information that is sent over a network in free form, in network packets, is difficult to detect. None of the solutions presented can analyze Network Steganography. All traffic passing over the network can be monitored with various applications and with behavioral analytics that generate alerts, but do not detect either Storage Channel Network Steganography or Timing Channel Network Steganography. Although there are some algorithms already tested, no method is yet completely reliable (Soni, 2020).

Another important limitation to indicate concerns document files. It is still very difficult to detect malicious code within documents. Although there is already work with Deep Learning, using Convolutional Neural Networks (CNN), the studies have focused on PDF files and are not yet extended to other types of text formats (Jeong et al., 2019b)

5.3. FUTURE WORK

There are a number of concerns that should be evaluated for the future regarding the topic of steganography with the following items in mind:

- Cyberattack techniques evolve quickly and are always one step ahead of security software and hardware
- There is malware that is an extension of other malware and tends to use other malware's techniques to be more effective
- Some of the malware presented here has already been discontinued and/or replaced by newer ones, with newer variations and strains, new ways of concealment and theft mechanisms
- Some of the literature used here mentions there are malwares that use techniques to fool the antiviruses themselves so that they are undetectable.
- That all new solutions emerge to solve problems that are being discovered but are often unable to detect behavior structural changes to files and traffic circulating in the company network.

So, all the suggestions made should be reviewed over time by companies, because new techniques, variations, and mutations will emerge over time, even if the company is not the target of any attack.

These Framework should be assessed to be extended to the cloud. When using an IaaS logic, it should always be the company that guarantees the security mechanisms, so as not to spread the problem to your entire system. In SaaS and PaaS situations, all security rules should be followed with the Cloud Provider, especially with the list of software used and guaranteed by the Provider. In situations of infection and theft, especially when using a SaaS AD, which can be compromised, ultra-sensitive information (user accounts and passwords, as well as access privileges) is at risk, which can be used either for intrusion into the various systems of the organization, as well as for Ransomware and/or LeakWare situations. This scenario applies to any Cloud architecture (Private, Public, Hybrid)

REFERENCES

Abrams, L. (2016a, May 18). TeslaCrypt shuts down and Releases Master Decryption Key [THREAT ANALYSIS]. *BleepingComputer.Com Logo*. https://www.bleepingcomputer.com/news/security/teslacrypt-shuts-down-and-releases-master-decryption-key/

Abrams, L. (2016b, December 22). How to Protect and Harden a Computer against Ransomware [THREAT ANALYSIS]. *BleepingComputer.Com Logo*. https://www.bleepingcomputer.com/news/security/how-to-protect-and-harden-a-computer-against-ransomware/

Adobe Flash Player EOL General Information Page. (n.d.). *Adobe*. https://www.adobe.com/pt/products/flashplayer/end-of-life.html

Al-Harbi, O. A., Alahmadi, W. E., & Aljahdali, A. O. (2020). Security analysis of DNA based steganography techniques. *SN Applied Sciences*, *2*(2), 172. https://doi.org/10.1007/s42452-019-1930-1

Anderson, R., Needham, R., & Shamir, A. (1998). The Steganographic File System. In D. Aucsmith (Ed.), *Information Hiding* (Vol. 1525, pp. 73–82). Springer Berlin Heidelberg. https://doi.org/10.1007/3-540-49380-8_6

APT [Advanced Persistent Threat]. (n.d.). [THREAT ANALYSIS]. *Trend Micro*.

Atawneh, S., Almomani, A., & Sumari, P. (2013). Steganography in digital images: Common approaches and tools. *IETE Technical Review*, *30*(4), 344. https://doi.org/10.4103/0256-4602.116724

Bailey, R. (n.d.). Backdoor:Win32/Vawtrak.C. *Hot Fo Fix Guide*. https://howtofix.guide/backdoorwin32-vawtrak-c/

Barth, B. (2016, August 24). *Twitoor first Android malware known to leverage Twitter for command and control*. https://www.scmagazine.com/news/mobile/twitoor-first-android-malware-known-to-leverage-twitter-for-command-and-control

Belcic, I. (2021, September 7). Cerber Ransomware: Everything You Need to Know [TRHEAT ANALYSIS]. *Avast*. https://www.avast.com/c-cerber

Cabaj, K., Caviglione, L., Mazurczyk, W., Wendzel, S., Woodward, A., & Zander, S. (2018). The New Threats of Information Hiding: The Road Ahead. *IT Professional*, *20*(3), 31–39. https://doi.org/10.1109/MITP.2018.032501746

Caraig, B. (n.d.). The ZeuS, ZBOT, and Kneber Connection [THREAT ANALYSIS]. *Threat Encyclopedia*. https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/16/the-zeus-zbot-and-kneber-connection

Caviglione, L. (2017). *La nuova frontiera del Malware?* 15.

Caviglione, L., Merlo, A., & Migliardi, M. (2018). Covert Channels in IoT Deployments Through Data Hiding Techniques. *2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, 559–563. https://doi.org/10.1109/WAINA.2018.00144

Celestino, O. (2012, June 14). How DNS Changer Trojans Direct Users to Threats [TRHEAT ANALYSIS]. *Threat Encyclopedia*. https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/125/how-dns-changer-trojans-direct-users-to-threats

Chang, C.-Y., & Clark, S. (2014). Practical Linguistic Steganography using Contextual Synonym Substitution and a Novel Vertex Coding Method. *Computational Linguistics*, *40*(2), 403–448. https://doi.org/10.1162/COLI_a_00176

Chaumont, M. (2020). Deep learning in steganography and steganalysis. In *Digital Media Steganography* (pp. 321–349). Elsevier. https://doi.org/10.1016/B978-0-12-819438-6.00022-0

Check Point/Network Security. (n.d.). https://www.checkpoint.com/cyber-hub/network-security/what-is-network-security/

Chen, J. C. (2017, June 20). AdGholas Campaign Employs Astrum Exploit Kit [THERAT ANALYSIS]. *Ransomware*. https://www.trendmicro.com/en_us/research/17/f/adgholas-malvertising-campaign-employs-astrum-exploit-kit.html

Cho, D. X., Thuong, D. T. H., & Dung, N. K. (2019). A Method of Detecting Storage Based Network Steganography Using Machine Learning. *Procedia Computer Science*, *154*, 543–548. https://doi.org/10.1016/j.procs.2019.06.086

Cimpanu, C. (2019, April 23). Source code of Carbanak trojan found on VirusTotal [THREAT ANALYSIS]. *ZDnet*. https://www.zdnet.com/article/source-code-of-carbanak-trojan-found-on-virustotal/

Cohen, A., Nissim, N., & Elovici, Y. (2020). MalJPEG: Machine Learning Based Solution for the Detection of Malicious JPEG Images. *IEEE Access*, *8*, 19997–20011. https://doi.org/10.1109/ACCESS.2020.2969022

Cohen, R. (2019, August 9). Banking Trojans: A Reference Guide to the Malware Family Tree. *F5 Labs - Ap+plication Threat Intelligence*. https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree

Command and Control [C&C] Server. (n.d.). [THREAT ANALYSIS]. *Trend Micro*. https://www.trendmicro.com/vinfo/us/security/definition/command-and-control-server

Command and Control Explained. (n.d.). [THREAT ANALYSIS]. *Cyberpedia*. https://www.paloaltonetworks.com/cyberpedia/command-and-control-explained

Czyż, B. (2020, July 15). An in-depth analysis of SpyNote remote access trojan. *Buldog Job Think IT*. https://bulldogjob.com/readme/an-in-depth-analysis-of-spynote-remote-access-trojan

Datta, D., Garg, L., Srinivasan, K., Inoue, A., Reddy G, T., Kumar Reddy M, P., K, R., & Nasser, N. (2021). An Efficient Sound and Data Steganography Based Secure Authentication System. *Computers, Materials & Continua*, *67*(1), 723–751. https://doi.org/10.32604/cmc.2021.014802

Deep Learning Techniques. (n.d.). https://www.upgrad.com/blog/top-deep-learning-techniques-you-should-know-about/

Dell SecureWorks Counter Threat Unit^{TM} Threat Intelligence. (2015, May 12). TeslaCrypt Ransomware [THREAT ANALYSIS]. *Threat Intelligence Research*. https://www.secureworks.com/research/teslacrypt-ransomware-threat-analysis

Djebbar, F., Ayad, B., Meraim, K. A., & Hamam, H. (2012). Comparative study of digital audio steganography techniques. *EURASIP Journal on Audio, Speech, and Music Processing*, *2012*(1), 25. https://doi.org/10.1186/1687-4722-2012-25

Donohue, B. (2013, January 18). FAKEM RAT Mimics Normal Network Traffic [THREAT ANALYSIS]. *Threat Post*. https://threatpost.com/fakem-rat-mimics-normal-network-traffic-011813/77424/

European Union Agency for CyberSecurity/Threat and Risk Management/Glossary. (n.d.). https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary

GoldSparrow. (2015, September 9). Carbanak [THREAT ANALYSIS]. *EnigmaSoft*. https://www.enigmasoftware.com/pt/carbanak-remocao/

Hashim, M. M., Rahim, M. S. M., Johi, F. A., Taha, M. S., & Hamad, H. S. (n.d.). Performance evaluation measurement of image steganography techniques with analysis of LSB based on variation image formats. *International Journal of Engineering*, 11.

Hassan, M., Amin, M., & Mahdi, S. (2020). STEGANALYSIS TECHNIQUES AND COMPARISON OF AVAILABLE SOFTWARES. *Proceedings of the Proceedings of the 1st International Multi-Disciplinary Conference Theme: Sustainable Development and Smart Planning, IMDC-SDSP 2020, Cyperspace, 28-30 June 2020*. https://doi.org/10.4108/eai.28-6-2020.2297970

Hassan, N. A., & Hijazi, R. (2017). Data Hiding Forensics. In *Data Hiding Techniques in Windows OS* (pp. 207–265). Elsevier. https://doi.org/10.1016/B978-0-12-804449-0.00006-3

Henson Security Tools. (2019, December 2). How Domain Fronting Attacks work. Explained in seven steps. *Henson Security Tools*. https://hensonsecuritytools.wordpress.com/

Hevner, A. R. (2007). *A Three Cycle View of Design Science Research*. *19*, 7.

Hevner, A., R, A., March, S., T, S., Park, Park, J., Ram, & Sudha. (2004). Design Science in Information Systems Research. *Management Information Systems Quarterly*, *28*, 75.

Hiding in Plain Sight: The FAKEM Remote Access Trojan. (2013, January 18). [THERAT ANALYSIS]. *Trend Micro*. https://www.trendmicro.com/en_us/research/13/a/hiding-in-plain-sight-the-fakem-remote-access-trojan.html

High Technology Theft Apprehension and Prosecution (HTTAP) Program. (2011, December 13). State of California - Department of Justice - Office of the Attorney General. https://oag.ca.gov/ecrime/httap

Homan, J. (2016, June 2). IRONGATE ICS Malware: Nothing to See Here...Masking Malicious Activity on SCADA Systems [THREAT ANALYSIS]. *THREAT RESEARCH BLOG*. https://www.fireeye.com/blog/threat-research/2016/06/irongate_ics_malware.html

How to remove Astrum Antivirus Pro (Uninstall Instructions). (2008, December 25). [Rogue Programs & Scareware]. https://www.bleepingcomputer.com/virus-removal/remove-astrum-antivirus-pro

Indicators of compromise. (n.d.). [THREAT ANALYSIS]. *Trend Micro*. https://www.trendmicro.com/vinfo/us/security/definition/indicators-of-compro

Jeong, Y.-S., Woo, J., & Kang, A. R. (2019a). Malware Detection on Byte Streams of PDF Files Using Convolutional Neural Networks. *Security and Communication Networks*, *2019*, 1–9. https://doi.org/10.1155/2019/8485365

Jeong, Y.-S., Woo, J., & Kang, A. R. (2019b). Malware Detection on Byte Streams of PDF Files Using Convolutional Neural Networks. *Security and Communication Networks*, *2019*, 1–9. https://doi.org/10.1155/2019/8485365

Johnson, N. F., & Jajodia, S. (1998). Steganalysis: The investigation of hidden information. *1998 IEEE Information Technology Conference, Information Environment for the Future (Cat. No.98EX228)*, 113–116. https://doi.org/10.1109/IT.1998.713394

Jung, K.-H. (2019). A Study on Machine Learning for Steganalysis. *Proceedings of the 3rd International Conference on Machine Learning and Soft Computing - ICMLSC 2019*, 12–15. https://doi.org/10.1145/3310986.3311000

Kapersky's Resource Center/What is Cloud Security. (n.d.). https://www.kaspersky.com/resource-center/definitions/what-is-cloud-security

Karampidis, K., Kavallieratou, E., & Papadourakis, G. (2018). A review of image steganalysis techniques for digital forensics. *Journal of Information Security and Applications*, *40*, 217–235. https://doi.org/10.1016/j.jisa.2018.04.005

Kaspersky. (n.d.). TeslaCrypt Ransomware Attacks [THREAT ANALYSIS]. *Kaspersky*. https://www.kaspersky.com/resource-center/threats/teslacrypt

Khan, M., Shahab, A., & Asghar, Z. (2015). Introduction to Linguistic Steganography. *Nonlinear Engineering*, *4*(3). https://doi.org/10.1515/nleng-2015-0013

Khan, Z., & Mansoor, A. B. (2009). An evaluation of wavelet filters performance for steganalysis. *2009 2nd International Conference on Computer, Control and Communication*, 1–5. https://doi.org/10.1109/IC4.2009.4909227

Koley, S. (2016). A Novel Approach of Secret Message Passing Through Text Steganography. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2873714

Kunwar, R. S., & Sharma, P. (2017). Framework to detect malicious codes embedded with JPEG images over social networking sites. *2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, 1–4. https://doi.org/10.1109/ICIIECS.2017.8276144

Malvertisement. (n.d.). [THREAT ANALYSIS]. *Trend Micro*. https://www.trendmicro.com/vinfo/us/security/definition/Malvertisement

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems*, *15*(4), 251–266. https://doi.org/10.1016/0167-9236(94)00041-2

Mazurczyk, W., & Caviglione, L. (2015). Information Hiding as a Challenge for Malware Detection. *IEEE Security & Privacy*, *13*(2), 89–93. https://doi.org/10.1109/MSP.2015.33

Mendrez, R. (2016, November 14). New Carbanak / Anunak Attack Methodology [THREAT ANALYSIS]. *Trustwave*. https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/new-carbanak-anunak-attack-methodology/

Meskauskas, T. (2021, December 2). SyncCrypt Ransomware [THREAT ANALYSIS]. *PCRisk*. https://www.pcrisk.com/removal-guides/11589-synccrypt-ransomware

Nissar, A., & Mir, A. H. (2010). Classification of steganalysis techniques: A study. *Digital Signal Processing*, *20*(6), 1758–1770. https://doi.org/10.1016/j.dsp.2010.02.003

Nissim, N., Cohen, A., Wu, J., Lanzi, A., Rokach, L., Elovici, Y., & Giles, L. (2019). Sec-Lib: Protecting Scholarly Digital Libraries From Infected Papers Using Active Machine Learning Framework. *IEEE Access*, *7*, 110050–110073. https://doi.org/10.1109/ACCESS.2019.2933197

Open-Source Steganography projects. (n.d.). https://www.findbestopensource.com/product/h3xx-jphs

Paganini, P. (2015, November 16). Twittor tool uses Twitter direct messages to control botnets [THREAT ANALYSIS]. *Security Affairs*. https://securityaffairs.co/wordpress/42000/cyber-crime/twittor-tool-twitter-botnet.html

Paganini, P. (2016, June 2). IRONGATE, a mysterious ICS Malware discovered in the wild. *Security Affairs*. https://securityaffairs.co/wordpress/47968/malware/irongate-ics-malware.html

Paganini, P. (2017, August 21). SyncCrypt Ransomware hides its components in image files [THREAT ANALYSIS]. *Security Affairs*. https://securityaffairs.co/wordpress/62191/malware/synccrypt-ransomware.html

Paganini, P. (2019, April 23). *FireEye experts found source code for CARBANAK malware on VirusTotal*. https://securityaffairs.co/wordpress/84382/hacking/carbanak-malware-virustotal.html

Paulsen, C., & Byers, R. (2019). *Glossary of key information security terms* (NIST IR 7298r3; p. NIST IR 7298r3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.7298r3

Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G. (1999). Information hiding-a survey. *Proceedings of the IEEE*, *87*(7), 1062–1078. https://doi.org/10.1109/5.771065

Popa, A. (2021, July 1). *8 types of Indicators of Compromise (IoCs) and how to recognize them*. https://attacksimulator.com/blog/how-to-recognize-indicators-of-compromise/

Pope, M. B., Warkentin, M., Bekkering, E., & Schmidt, M. B. (2012). Digital Steganography—An Introduction to Techniques and Tools. *Communications of the Association for Information Systems*, *30*. https://doi.org/10.17705/1CAIS.03022

RAT (remote access Trojan). (n.d.). [THREAT ANALYSIS]. *SearchSecurity*. https://www.techtarget.com/searchsecurity/definition/RAT-remote-access-Trojan

Sai, O. V. (2015, May 26). Angler EK Exploiting Adobe Flash CVE-2015-3090 [THREAT ANALYSIS]. *THREAT RESEARCH BLOG*. https://www.fireeye.com/blog/threat-research/2015/05/angler_ek_exploiting.html

Sanger, D. E. (2019). *The perfect weapon: War, sabotage, and fear in the cyber age* (First paperback edition). Broadway Books.

SecurityWeek News. (2016, July 27). PayPal Abused in Banking Trojan Distribution Campaign. *SecurityWeek News*. https://www.securityweek.com/paypal-abused-banking-trojan-distribution-campaign

Segura, J. (2021, July 16). *GreenFlash Sundown exploit kit expands via large malvertising campaign*. https://blog.malwarebytes.com/threat-analysis/2019/06/greenflash-sundown-exploit-kit-expands-via-large-malvertising-campaign/

Shargh, E. (2017, July 10). How Traps Protects Against Astrum [THREAT ANALYSIS]. *Palo Alto Networks Blog*. https://www.paloaltonetworks.com/blog/2017/07/how-traps-protects-against-astrum/

Soni, T. (n.d.). *Moving target network steganography*. 82.

Soni, T. (2020). *Moving target network steganography*. 82.

Spear phishing. (n.d.). [THREAT ANALYSIS]. *Trend Micro*. https://www.trendmicro.com/vinfo/us/security/definition/spear-phishing

SpyNote RAT. (2019, September 19). [THREAT ANALYSIS]. *SPYWARE REMOVE - Your Guide to Spyware Removeal*. https://www.spywareremove.com/removespynoterat.html

Steganography definitions. (n.d.). https://towardsdatascience.com/steganography-hiding-an-image-inside-another-77ca66b2acb1

Steganography—An Experiment in Python. (n.d.). Engineering Education (EngEd) Program | Section. Retrieved May 31, 2021, from https://www.section.io/engineering-education/steganography-in-python/

Stone-Gross, B. (2014, August 7). Malware Analysis of the Lurk Downloader [THREAT ANALYSIS]. *THREAT ANALYSIS*. https://www.secureworks.com/research/malware-analysis-of-the-lurk-downloader

Tamir, D. (2015, July 8). Stopping the Evasive Stegoloader Malware [TRHEAT ANALYSIS]. *Security Intelligence Logo*. https://securityintelligence.com/stopping-the-evasive-stegoloader-malware/

Truong, J. (2021, July 13). Domain Fronting 101: What is Domain Fronting and How Does it Work? *HackerNoon*. https://hackernoon.com/domain-fronting-101-what-is-domain-fronting-and-how-does-it-work-es2v37pr

Updated Sundown Exploit Kit Uses Steganography. (2016, December 29). [THREAT ANALYSIS]. *Trend Micro*. https://www.trendmicro.com/en_us/research/16/l/updated-sundown-exploit-kit-uses-steganography.html

VMWare/Application Security. (n.d.).

Warkentin, M., Bekkering, E., & Schmidt, M. (2008). Steganography: Forensic, Security, and Legal Issues. *Journal of Digital Forensics, Security and Law*. https://doi.org/10.15394/jdfsl.2008.1039

What Is an Advanced Persistent Threat (APT)? (n.d.). [THREAT ANALYSIS]. *Kaspersky*. https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats

What is an Exploit Kit? (n.d.). [THREAT ANALYSIS]. *Cyberpedia*. https://www.paloaltonetworks.com/cyberpedia/what-is-an-exploit-kit

What is the comparison between Steganography and Obfuscation in Information Security? (2022, March 14). https://www.tutorialspoint.com/what-is-the-comparison-between-steganography-and-obfuscation-in-information-security

Wyke, J. (2014). *Vawtrak – International Crimeware-asa-Service* [Paper]. https://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/sophos-vawtrak-international-crimeware-as-a-service-tpna.pdf

Ye, J., Ni, J., & Yi, Y. (2017). Deep Learning Hierarchical Representations for Image Steganalysis. *IEEE Transactions on Information Forensics and Security*, *12*(11), 2545–2557. https://doi.org/10.1109/TIFS.2017.2710946

Yedroudj, M. (n.d.). *Steganalysis and steganography by deep learning*. 252.

Zielińska, E., Mazurczyk, W., & Szczypiorski, K. (2014). Trends in steganography. *Communications of the ACM*, *57*(3), 86–95. https://doi.org/10.1145/2566590.2566610

Zou, Y., Zhang, G., & Liu, L. (2019). Research on image steganography analysis based on deep learning. *Journal of Visual Communication and Image Representation*, *60*, 266–275. https://doi.org/10.1016/j.jvcir.2019.02.034

Annexes

Dados do Entrevistado

Nome: Ricardo Carvalho Mendes

Cargo/Função: Chief of the Security Management & IT Infrastructure Division at Oeiras Municipality

Data: 20 Julho 2022

Autor: A tese centra-se basicamente na Cibersegurança, nomeadamente na questão da esteganografia em que a ideia principal foi criar um referencial onde fosse possível cruzar as técnicas de combate a este vetor de ataque com possíveis ataques a nível de segurança. Sendo a esteganografia uma técnica que permite ocultar informação dentro de ficheiros, de podendo até esconder código malicioso, nomeadamente, de media files, bem como a exfiltração de dados através de covert channels, foi feito um levantamento das principais ameaças que existem, que impacto podem causar, que métodos usam e quais os métodos sugeridos na literatura para os combater. Foram usados alguns artigos científicos para identificar as ameaças e foram consultados os principais sites das principais empresas de cibersegurança.

Autor: Assim sendo, tenho algumas questões que gostaria de colocar**.** Do que conhece atualmente da esteganografia, quer seja por experiência própria, quer seja pelo que já leu, considera que este é um tema que tem sido desvalorizado e que mereça alguma atenção adicional?

Entrevistado: Considero que a esteganografia a par com o *phishing,* são dos temas que mais preocupam as pessoas, organizações e autoridades policiais. A razão desta preocupação prende-se com o facto que ao contrário da maior parte dos ciberataques que visam descobrir e utilizar vulnerabilidades nos sistemas tecnológicos, a esteganografia visa numa primeira fase, utilizar a componente humana de um sistema informático como ponto vulnerável de entrada, ataque e comprometimento dos sistemas.

Autor: Quer seja pela instalação de Malware através do carregamento de payloads vindo em ficheiros, quer seja por Covert Channels em que se rouba informação sem haver a noção que se está a ser exfiltrado?

Entrevistado: ____

____

____

____

____

____

____.

Autor: O referencial proposto nesta tese é composto por um conjunto de Best Practices, entre os quais uma framework de atuação e ações táticas adequadas, como o uso de software próprio (Anti-virus, Anti-Malware, Anti-Steganography) para prevenir e reagir a eventuais ataques. Desta forma, e olhando para este referencial, acha que poderá ser útil para as organizações para as ajudar a combater os possíveis ameaças de segurança?

Entrevistado: Todas as iniciativas que pretendam criar metodologias e/ou políticas para lidar com ciberincidentes são importantes para a garantia dos pilares da segurança da informação: confidencialidade, integridade, disponibilidade e autenticidade dentro de uma organização. A criação deste Framework é mais uma ferramenta disponível e por esse motivo irá ajudar a combater as possíveis ameaças.

Autor: Acha que o mercado, hoje em dia, já está dotado de soluções e do software necessário e capaz de lidar com este problema?

Entrevistado: Acho que as soluções já existem, é agora uma questão de as utilizar e fazer da cibersegurança um tema prioritário dentro de uma organização, começando pela gestão de topo e seguindo toda a cadeira hierárquica sem exceções.

Autor: Tendo em conta o que conhece da área de segurança, e entre os vetores de ataque mais comuns que tem conhecimento e que tem presenciado, o que acha que é o maior problema em termos de CiberSegurança para as empresas?

Entrevistado: Na minha opinião o maior problema em termos de cibersegurança nas empresas é a falta de cultura e formação nas empresas e seus colaboradores. Essa falta de cultura está presente tanto nos utilizadores finais como nos profissionais de Sistemas e Tecnologias de informação .

Autor: Em função do que afirmou, em que especto é que esteganografia se pode enquadrar também num desses vetores de ataque (phishing, social engineering, etc)? Ou acha que atualmente não é um problema para as empresas por não ser um vetor de ataque muito pouco usado e até com pouca capacidade de ser aplicado porque as soluções tecnológicas existentes bloqueiam e eliminam na quase totalidade este risco?

Entrevistado: Considero que a esteganografia continua a ser e irá ser no futuro um risco para as empresas. É verdade que muitas das soluções tecnológicas existentes já bloqueiam muitos dos ataques, mas como em tudo nesta área, podem bloquear mil ataques, mas basta deixar passar um, para se comprometer toda a empresa.

Autor: De alguma forma, concorda com o referencial que foi proposto? Acha que se devia acrescentar alguma coisa, nomeadamente algum tipo de vulnerabilidade por onde pode ser aplicada esteganografia e que na toolbox não esteja a ser considerada?

Entrevistado: ____
____
____
____
____
____
____.

Autor: Por fim, no seu entender, acha que esta toolbox necessita de alguma melhoria, nomeadamente, de alguma Best Practice que não esteja nela incluída, ou alguma abordagem de intervenção mais tática para mitigar os riscos e as consequências de algum ataque à organização?

Entrevistado: ____
____
____
____
____
____
____.

Muito Obrigado pela participação!

João Moura

Dados do Entrevistado

Nome: Carlos Santos

Cargo/Função: Pré-venda para a Fortinet com especialização em produtos para SoC

Data: 01/08/2022

Autor: A tese centra-se basicamente na Cibersegurança, nomeadamente na questão da esteganografia em que a ideia principal foi criar um referencial onde fosse possível cruzar as técnicas de combate a este vetor de ataque com possíveis ataques a nível de segurança. Sendo a esteganografia uma técnica que permite ocultar informação dentro de ficheiros, de podendo até esconder código malicioso, nomeadamente, de media files, bem como a exfiltração de dados através de covert channels, foi feito um levantamento das principais ameaças que existem, que impacto podem causar, que métodos usam e quais os métodos sugeridos na literatura para os combater. Foram usados alguns artigos científicos para identificar as ameaças e foram consultados os principais sites das principais empresas de cibersegurança.

Autor: Assim sendo, tenho algumas questões que gostaria de colocar**.** Do que conhece atualmente da esteganografia, quer seja por experiência própria, quer seja pelo que já leu, considera que este é um tema que tem sido desvalorizado e que mereça alguma atenção adicional?

Entrevistado: Pegando no significado do termo, parece-me que se trata de uma técnica de ofuscação e cifra, usada frequentemente nos ataques mais recentes e com tendência crescente de ransomware na tentativa de encapsular o código ou mesmo transformá-lo conhecido como malware polimórfico, os fabricantes na área da segurança de informação estão atentos à técnica onde estão em vigor nas soluções de protecção aos endpoints sistemas de análise comportamental e telemetria que permitem analisar a aplicações ao nível mais baixo, não é um tema que tenha sido desvalorizado, muito pelo contrário.

Autor: Quer seja pela instalação de Malware através do carregamento de payloads vindo em ficheiros, quer seja por Covert Channels em que se rouba informação sem haver a noção que se está a ser exfiltrado?

Entrevistado: Sim, todas as instruções ao mais baixo nível do sistema operativo são analizadas, permitindo uma visibilidade que não era possível com as soluções de antivírus tradicionais.

Autor: O referencial proposto nesta tese é composto por um conjunto de Best Practices, entre os quais uma framework de atuação e ações táticas adequadas, como o uso de software próprio (Anti-virus, Anti-Malware, Anti-Steganography) para prevenir e reagir a eventuais ataques. Desta forma, e olhando para este referencial, acha que poderá ser útil para as organizações para as ajudar a combater os possíveis ameaças de segurança?

Entrevistado: No contexto actual estão a ser implementadas soluções de Advanced Threat Protection ou Endpoint Detection and Response onde estes vetores são tidos em conta .

Autor: Acha que o mercado, hoje em dia, já está dotado de soluções e do software necessário e capaz de lidar com este problema?

Entrevistado: É um mercado em crescimento existem algums bons produtos já no mercado.

Autor: Tendo em conta o que conhece da área de segurança, e entre os vetores de ataque mais comuns que tem conhecimento e que tem presenciado, o que acha que é o maior problema em termos de CiberSegurança para as empresas?

Entrevistado: As pessoas e a falta de conhecimento para comportamentos de risco na utilização dos recursos disponíveis. .

Autor: Em função do que afirmou, em que especto é que esteganografia se pode enquadrar também num desses vetores de ataque (phishing, social engineering, etc)? Ou acha que atualmente não é um problema para as empresas por não ser um vetor de ataque muito pouco usado e até com pouca capacidade de ser aplicado porque as soluções tecnológicas existentes bloqueiam e eliminam na quase totalidade este risco?

Entrevistado: Considerando o termo e a técnica de escrita oculta, nos dias de hoje é usada recorrentemente nos ataques de phishing ocultando num endereço de email, um nome legítimo, tentanto levar o utilizador a assumir que está a comunicar com uma pessoa conhecida ou entidade, phishing é uma técnica de social engineering, este é o principal vector de ataque nos dias de hoje. E também com maior taxa de sucesso, e continua a ser dos casos mais complexos de mitigar

Autor: De alguma forma, concorda com o referencial que foi proposto? Acha que se devia acrescentar alguma coisa, nomeadamente algum tipo de vulnerabilidade por onde pode ser aplicada esteganografia e que na toolbox não esteja a ser considerada?

Entrevistado: As pessoas são a maior vulnerabilidade contra técnicas de ofuscação recomendaria que fossem incluídas onde a técnica tem sucesso.

Autor: Por fim, no seu entender, acha que esta toolbox necessita de alguma melhoria, nomeadamente, de alguma Best Practice que não esteja nela incluída, ou alguma abordagem de intervenção mais tática para mitigar os riscos e as consequências de algum ataque à organização?

Entrevistado: User awareness, formação são fundamentais .

Muito Obrigado pela participação!

João Moura

Dados do Entrevistado

Nome: Luis Ramos

Cargo/Função: Security Architect

Data:27/07/2022

Autor: A tese centra-se basicamente na Cibersegurança, nomeadamente na questão da esteganografia em que a ideia principal foi criar um referencial onde fosse possível cruzar as técnicas de combate a este vetor de ataque com possíveis ataques a nível de segurança. Sendo a esteganografia uma técnica que permite ocultar informação dentro de ficheiros, de podendo até esconder código malicioso, nomeadamente, de media files, bem como a exfiltração de dados através de covert channels, foi feito um levantamento das principais ameaças que existem, que impacto podem causar, que métodos usam e quais os métodos sugeridos na literatura para os combater. Foram usados alguns artigos científicos para identificar as ameaças e foram consultados os principais sites das principais empresas de cibersegurança.

Autor: Assim sendo, tenho algumas questões que gostaria de colocar**.** Do que conhece atualmente da esteganografia, quer seja por experiência própria, quer seja pelo que já leu, considera que este é um tema que tem sido desvalorizado e que mereça alguma atenção adicional?

Entrevistado: Não considero que este tema tenha sido desvalorizado, no entanto, temos vindo a observar um elevado número de ciberataques em que a esteganografia tipicamente não foi um dos vectores de ataque. De qualquer modo é um tema relevante para os profissionais da área, mas não conhecido pela generalidade das pessoas.

Autor: Quer seja pela instalação de Malware através do carregamento de payloads vindo em ficheiros, quer seja por Covert Channels em que se rouba informação sem haver a noção que se está a ser exfiltrado?

Entrevistado: Em organizações que têm uma política de classificação de informação, os dados considerados confidenciais têm um tratamento diferente, sendo alvo de controlos técnicos e procedimentais específicos, desde a nível de imagem ou a nível de rede utilizando firewalls de layer7 que têm a capacidade de ver os pacotes e perceber se os fluxos de dados são fidedignos ou não; ou inclusive perceber se existem dados/pacotes a sair por portos ou protocolos não comuns. Tipicamente pequenas e médias organizações têm a protecção que é facultada via a solução de endpoint, que pode ou não dar protecção das diferentes técnicas de esteganografia; no entanto são é comum existirem soluções especificas para esteganografia em organizações de menor dimensão.

Autor: O referencial proposto nesta tese é composto por um conjunto de Best Practices, entre os quais uma framework de atuação e ações táticas adequadas, como o uso de software próprio (Anti-virus, Anti-Malware, Anti-Steganography) para prevenir e reagir a eventuais ataques. Desta forma, e olhando para este referencial, acha que poderá ser útil para as organizações para as ajudar a combater os possíveis ameaças de segurança?

Entrevistado: É sempre útil existir uma Framework de resposta a incidentes que permitam às organizações detectar, conter e remediar rapidamente ameaças. No entanto, a Framework deve ser única e aplicada não apenas a temas de esteganografia, mas a todos os eventuais incidentes que venham a surgir. Isto faz com que não se dupliquem processos ligados às Frameworks. Exemplo disto é a Framework da NIST.

Autor: Acha que o mercado, hoje em dia, já está dotado de soluções e do software necessário e capaz de lidar com este problema?

Entrevistado: Existem diversas soluções no mercado para endereçar muitos problemas. Muitas das vezes o problema não é a tecnologia em si mas identificar as fragilidades e posteriormente identificar que controlos o podem mitigar. A nível de software existe sempre necessidade de melhoria continua.

Autor: Tendo em conta o que conhece da área de segurança, e entre os vetores de ataque mais comuns que tem conhecimento e que tem presenciado, o que acha que é o maior problema em termos de CiberSegurança para as empresas?

Entrevistado: O maior problema de cibersegurança para as empresas são as pessoas. Faz falta existir uma cultura de cibersegurança dentro das organizações. Hoje em dia já não se protegem computadores, mas a sociedade como um todo. É importante existir uma maior sensibilização para os riscos do digital pois todas as organizações estão muito dependentes da tecnologia (transformação digital) e podemos e devemos tirar o melhor partido tendo consciência dos riscos inerentes.

Autor: Em função do que afirmou, em que especto é que esteganografia se pode enquadrar também num desses vetores de ataque (phishing, social engineering, etc)? Ou acha que atualmente não é um problema para as empresas por não ser um vetor de ataque muito pouco usado e até com pouca capacidade de ser aplicado porque as soluções tecnológicas existentes bloqueiam e eliminam na quase totalidade este risco?

Entrevistado: Na minha perspetiva, tudo o que possa colocar em causa a confidencialidade da minha informação deve ser alvo de uma análise de risco e posteriormente o seu plano de mitigação. A verdade é que acaba por não ser um tema "quente", que se oiça falar todos os dias – isto aliado ao facto de soluções de Endpoint Security, Email, Web, entre outras já terem capacidades de detecção e bloqueio deste tipo de ataques faz com que seja um pouco descurado. No entanto, organizações com uma boa gestão de risco e que implementem um plano sólido de ciberataques certamente vão olhar também para este vector.

Autor: De alguma forma, concorda com o referencial que foi proposto? Acha que se devia acrescentar alguma coisa, nomeadamente algum tipo de vulnerabilidade por onde pode ser aplicada esteganografia e que na toolbox não esteja a ser considerada?

Entrevistado: O referencial, regra geral, tem os principais pontos alinhados com uma NIST que é o referencial do mercado e as vulnerabilidades estão em linha com as técnicas mais comuns dentro deste vector de ataque.

Autor: Por fim, no seu entender, acha que esta toolbox necessita de alguma melhoria, nomeadamente, de alguma Best Practice que não esteja nela incluída, ou alguma abordagem de intervenção mais tática para mitigar os riscos e as consequências de algum ataque à organização?

Entrevistado: Existe sempre um ponto que acho muito importante, mas muitas vezes descurado que são as "Lesson Learned" – no último ponto do processo devemos olhar para o que correu bem e menos bem e optimizar o processo com base no que aprendemos ao por em vigor este referencial. No entanto reforço a importância de uma Framework global de resposta a incidentes alinhados à tecnologia, processos e pessoas.

Muito Obrigado pela participação!

João Moura