



UNIVERSITAT POLITÈCNICA
DE CATALUNYA
BARCELONATECH



telecos
BCN



EY

Building a better
working world

Malware attack prevention, detection, response and recovery

A Degree Thesis Submitted to the Faculty of the Escola
Tècnica d'Enginyeria de Telecomunicació de Barcelona

Universitat Politècnica de Catalunya

by

Pol Fernández Blánquez

Department of Computer Science - Telecommunications Engineering

Under the supervision of Prof. Óscar Esparza Martin

and Laura Abellanet as EY Tutor

Barcelona, January 2022



UNIVERSITAT POLITÈCNICA
DE CATALUNYA
BARCELONATECH



Abstract

The content of this document presents an in-depth study of the main current cybersecurity threats and an automated tool for managing responses to each of them.

This study focuses on attacks in the banking sector, analysing the main entry channels of attackers, the attack vectors and the evolution of the attackers once inside the systems.

As for the tool, based on VBA and Excel macros, it will allow to present the study at the level of the MITRE Matrix which will be explained later in this document, and through input parameters it will be able to show where its main security vulnerabilities are and if it meets the appropriate requirements to avoid most threats.

Resum

El contingut d'aquest document presenta un estudi en profunditat de les principals amenaces actuals de ciberseguretat i una eina automatitzada per a la gestió de respostes a cadascuna d'elles.

Aquest estudi se centra en els atacs en el sector bancari, analitzant els principals canals d'entrada d'atacants, els vectors d'atac i l'evolució dels atacants una vegada dins dels sistemes.

En quant a l'eina, basada en macros VBA i Excel, permetrà presentar l'estudi al nivell de la matriu MITRE que s'explicarà més endavant en aquest document, i a través dels paràmetres d'entrada podrà mostrar on estan les seves principals vulnerabilitats de seguretat i si compleix els requisits apropiats per evitar la majoria de les amenaces.

Resumen

El contenido de este documento presenta un estudio en profundidad de las principales amenazas actuales de ciberseguridad y una herramienta automatizada para la gestión de respuestas a cada una de ellas.

Este estudio se centra en los ataques en el sector bancario, analizando los principales canales de entrada de atacantes, los vectores de ataque y la evolución de los atacantes una vez dentro de los sistemas.

En cuanto a la herramienta, basada en macros VBA y Excel, permitirá presentar el estudio al nivel de la matriz MITRE que se explicará más adelante en este documento, y a través de los parámetros de entrada podrá mostrar donde están sus principales vulnerabilidades de seguridad y si cumple los requisitos apropiados para evitar la mayoría de las amenazas.

Agraïments

M'agradaria donar les gràcies en primer lloc als meus companys de departament d'arquitectura de seguretat a EY, per tot el suport tant tècnic com moral, en especial a l'Andreu i l'Ainara, que m'han acompanyat en aquest procés amb un somriure en tot moment. A la Laura Abellonet, la meva mànager d'EY que ha apostat per mi en tot moment i ha donat sempre la confiança per tirar el projecte endavant.

També vull agrair al meu tutor Óscar Esparza per haver-me guiat en la confecció d'aquest treball, haver-me donat sempre bons consells i haver-me rebut sempre amb il·lusió a qualsevol hora del dia.

No puc oblidar-me de mencionar els que van començar essent els meus companys d'universitat, amics i ara part de la meva família. Especialment a en Victor i l'Àngela, el suport de tots ells ha estat essencial durant aquests anys de carrera-

Per últim però no menys important, estaré sempre infinitament agraït als meus pares Santi i Lidia i a la meva germana Clàudia per haver confiat sempre amb mi, haver viscut aquests anys amb el seu recolzament i el seu suport ha estat un luxe extraordinari. I gràcies a tu Sara, pel teu somriure, recolzament i companyia, que han fet aquests anys de carrera els millors de la meva vida amb diferència.

Contents

Abstract	3
Resum	4
Resumen	5
Agraïments	6
List of figures	9
1 Introduction	10
1.1 Involvement	11
3. State of art and fundamentals	14
3.1 Information security	14
3.2 Cybersecurity	16
3.3 Cyber threat	17
3.4 Malware	18
3.5 MITRE ATT&CK matrix	22
3.5.1 Operation of the matrix	23
3.5.2 Structure breakdown: tactics and techniques	24
3.6 Threat Modelling	29
3.6.1 Main threats identified in the banking sector	29
3.6.2 Entry channels	31
3.6.2.1 Browsing	32
3.6.2.2 Customer's channel	32
3.6.2.3 USB	32
3.6.2.4 Mail	32
3.6.2.5 Third Parties	32
3.6.2.6 Online Sharing	32
3.6.2.7 Citrix	32
3.6.2.8 API & Web Services	33
3.6.2.9 Cloud Storage	33
3.6.2.10 Endpoints (ATMs)	33
3.6.3 Entry vectors	33
4 Problem formulation and methodology	35
4.1 Challenge	35
4.2 First steps	35

5.1 Use case	41
6. Economic analysis	47
7. Conclusions and next steps	48
7.1 Conclusions	48
7.2 Next steps	49
References	50

List of figures

- 1 Cyberedge Group 2021 Cyberthreat Defence Report – a comprehensive review of 1,200 IT security professionals representing 17 countries and 19 industries [3]
- 2 Types of malware [9]
- 3 Cyber Kill Chain diagram
- 4 ATT&CK matrix breakdown
- 5 Example of a technique description in MITRE's ATT&CK
- 6 Gantt diagram of first steps
- 7 Applicable MITRE fields for Identity and Access
- 8 Figure 8. Customer Channel IaA tab
- 9 Methodology slide from the PowerPoint created
- 10 USB Status PowerPoint slide
- 11 VBA code inside the tool
- 12 USB IaA threat analysis
- 13 Data Leakage introduction slide
- 14 Data Leakage latest news slide
- 15 Applicable attack vectors for Data Leakage
- 16 MITRE ATT&ACK phases with covered(green) or partially covered(orange) techniques.
- 17 USB status, high-level rationale and high-level conclusions
- 18 Data tab inside the tool
- 19 VBA user form module for user interaction template
- 20 Cost calculation

1 Introduction

One of the most widespread threats to cyber security in today's world of unlimited Internet access is malware. In recent times, malware is designed with the ability to adapt and hide silently on the systems of unsuspecting users. Malware analysis is the process of doing a reconnaissance of malware and understanding its actions and behaviour. It is an important and relevant task, as advanced forms of malware today are often not even detectable by commonly available anti-virus software and are constantly evolving and pose an increasing risk to all internet users.

In this project we will focus on the security systems of a bank, as it is one of the main affected by this type of attack and because it is essential to strengthen the cybersecurity of these organisations in order to fight fraud in the financial sector. In this thesis, a systematic and exhaustive study of the main malware threats has been carried out and automated responses to these threats have been designed, based on the most appropriate mitigations for each of the cases and taking into account current security capabilities.

In recent times, the number of cybersecurity incidents that have come to light, and the economic, media, reputational and technological impact are increasing. Beyond the classic Crisis Management Plans, it has become clear that exceptional measures are sometimes required that go beyond the norm.

Currently, when it comes to malware, the biggest threat to state and local governments today is information held hostage. The tactic, known as ransomware, has been in use for some time now, although it has recently been gaining traction for having evolved into the most profitable type of malware in history. Also, we will enumerate and study the **3 most common threats**, which are **Ransomware, Data Breach and Identity and access**. [1]

1.1 Involvement

For the last 10 months I have been part of the consulting firm EY (Ernst & Young), one of the four largest consulting firms in the world, and I have been working in the security architecture department of a client bank, cybersecurity risk management and threat modelling. The starting point of this project was therefore to analyse the current threats and all possible vector/entry channels to the bank and to identify the need to cover the maximum of the bank's current security capabilities based on the risks detected. Given the scope of the study, the aim is to create a threat response tool that will mainly enable the mapping of the necessary capabilities with those of any bank that uses it. The methodology used will be presented in later chapters.

So far, no guidelines have been established to carry out the analysis in an orderly and efficient manner, therefore, in this project we will design and develop control guidelines to assess compliance with the minimum capabilities in the face of current threats. We will also analyse the different threats that may be able to exploit the entity's weaknesses in a more indirect way, as well as the environments in which they are applicable (this will be done by studying the different data flows that a bank has).

The ultimate goal will therefore be to create a tool that can generate a threat assessment based on the banking domain and on the cyber security matrix that we will see later in this book, based on the current capability coverage entered by the user. The tool should also be able to present the analysis results and if possible, propose recommendations for the identified problems.

Regarding the structure of this project, the main objectives to be met are given in chapter 2; chapter 3 gives a theoretical explanation of the main concepts used (especially the concepts of Information Security and Cybersecurity, Malware, Threat Modelling); the methodology followed during the project is explained in chapter 4; the results of the project (including the milestones achieved that were necessary to create the tool) are presented in chapter 5; the sixth chapter presents the economic impact of the project; the seventh chapter presents the main conclusions reached throughout the

project and explains some ideas for possible future work; finally, the last section is devoted to the citation of the main bibliographical references consulted.

2 Objectives

The main objective of this project is to carry out an exhaustive study about cybersecurity threat modelling to be able to assess compliance with the minimum-security capabilities of companies in the banking sector, necessary to counter the main cybersecurity threats in an automated way. To this end, the objective is to develop a simple tool capable of providing a report with the risks detected, given the parameters entered by a user and an in-depth study that has been developed with a security matrix that we will see in this thesis. The result of this assessment should be able to state whether or not the entity complies with the minimums and what steps need to be taken to improve it. If possible, the tool should be able to present the results of the assessment and provide recommendations and possible remedies for the deficiencies found.

In order to create such a tool, other milestones need to be met so that the tool is based on a coherent set of rules and parameterisation. It is therefore also necessary to:

- Study and fully understand the complexities, requirements and implications of the main security threats and the types of attacks that are commonly carried out.
- Study and analyse the different applicable threats and attack types in order to identify the necessary mitigating controls.
- Develop a mapping between the current security capabilities of the bank in question and the mitigations needed to repel each of the attacks studied.

In order to provide differential value, threat modelling has been carried out, with all that this entails: a better understanding of these threats allows you to learn how to protect yourself better, detect possible errors, detect vulnerabilities or things that are not being properly secured. The main attacks have been studied in depth in all their phases and in all their ways of access. In this way we can see the best practices to implement and which are the most critical parts.

Another way to add value is through the automation process with the tool and to make the whole process more efficient, the study has been done in a modular way to be scalable.

3. State of art and fundamentals

3.1 Information security

Information security is the set of measures and techniques used to control and safeguard all data handled within a company or institution and to ensure that it does not leave the system established by the company. It is also a key element for companies to currently carry out their operations, since the data handled are essential for the activity they carry out. [2]

Although the majority of companies' systems are based on new technologies, we must not confuse information security and computer security, which, although they are closely related, are not the same concept.

It is important to understand that any company, regardless of its size, handles confidential data, either of its customers, its employees or both, and that it must therefore establish the necessary data protection security measures to guarantee the correct processing of this data, something which, with the entry into force first of the **LOPD**¹ and then of the **GDPR**², is not an option, but an obligation. These two regulations will be explained later in this chapter.

Based on the fact that information security may vary depending on the characteristics of each company and the sector in which it operates, we can speak of a series of common objectives that all companies share in the field of information security and data protection.

These information security objectives can be found in the **ISO 27001**³ standard. This standard provides a model for the implementation of information security management systems (ISMS), whose main purpose is the protection of information assets, i.e., equipment, users and information.

¹ **LOPD** is the Law that transposes the repealed Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

² **GDPR** (General Data Protection Regulation) on May 25, 2016, came into force.

³ **ISO 27001** is an international standard for the assurance, confidentiality and integrity of data and information, as well as the systems that process it.

In order to establish this ISO information security system, three fundamental aspects must be taken into account: integrity, confidentiality and availability. [3]

Integrity

Systems that manage information will have to ensure the integrity of the information, i.e., that the information is displayed as it was intended, without alterations or manipulations that have not been expressly authorised. The main objective is to ensure the transmission of data in a secure environment, using secure protocols and techniques to avoid possible risks.

Confidentiality

Confidentiality ensures that only authorised persons or entities have access to the information and data collected and that it is not disclosed without permission. Information security systems shall ensure that the confidentiality of information is not compromised at any time.

Availability

In this aspect, information is guaranteed to be available at all times to all persons or entities authorised to handle and know it. For this purpose, support and security measures must be in place to ensure that the information can be accessed when necessary and to prevent interruptions in services.

What are the differences between Information Security and Cybersecurity?

Although information security and cybersecurity are intertwined concepts, there are differences between them. To begin with, we can understand information security as a whole and cybersecurity as a part of that whole. That is, information security encompasses all measures and processes aimed at protecting valuable business information and data, covering both digital and physical formats. Whereas cyber security is limited to the protection of information within the company's digital environments.

Information security assesses risks and prevents threats based on defensive aspects to protect systems. Cybersecurity, on the other hand, contemplates protection

measures based on the attack against such threats (security breaches), as shown below.

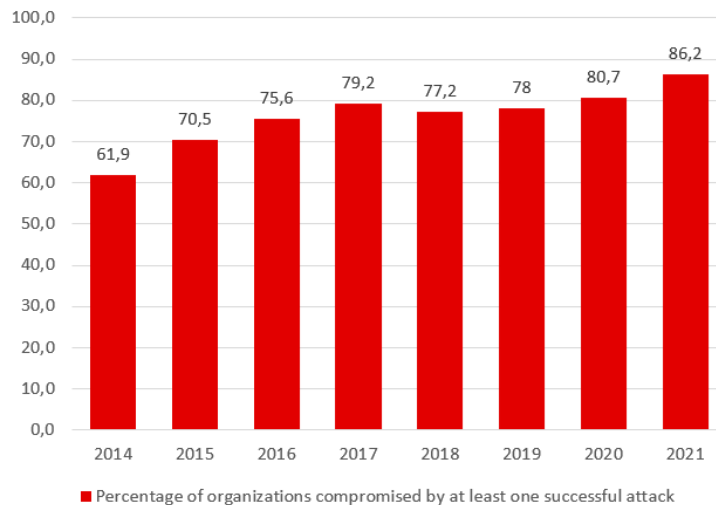


Figure 1. Cyberedge Group 2021 Cyberthreat Defence Report – a comprehensive review of 1,200 IT security professionals representing 17 countries and 19 industries

3.2 Cybersecurity

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks⁴ are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes. Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.

In today's connected world, everyone benefits from advanced cyberdefence programs. At an individual level, a cybersecurity attack can result in everything from identity theft, to extortion attempts, to the loss of important data like family photos. Everyone relies on critical infrastructure like power plants, hospitals, and financial service companies. Securing these and other organizations is essential to keeping our society functioning.

⁴ A cyberattack is a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization. Usually, the attacker seeks some type of benefit from disrupting the victim's network.

IT security should establish rules that minimise risks to information or IT infrastructure. These rules include hours of operation, restrictions to certain locations, authorisations, denials, user profiles, emergency plans, protocols and everything necessary to allow a good level of computer security while minimising the impact on the performance of workers and the organisation in general and as the main contributor to the use of programs made by programmers.

IT security is designed to protect IT assets, including the following:

- **The computer infrastructure:** this is a fundamental part of the storage and management of information, as well as the very functioning of the organisation. The function of computer security in this area is to ensure that the equipment works properly and to anticipate in the event of failures, theft, fire, sabotage, natural disasters, power failures and any other factor that may threaten the computer infrastructure.
- **Users:** these are the people who use the technological structure, communications area and manage the information. The system in general must be protected so that their use cannot compromise the security of the information or make the information they handle or store vulnerable.
- **Information:** this is the main asset. It utilises and resides in the computing infrastructure and is used by the users.

3.3 Cyber threat

Today, the term is almost exclusively used to describe information security matters. Because it's hard to visualize how digital signals traveling across a wire can represent an attack, we've taken to visualizing the digital phenomenon as a physical one.

A cyber-attack is an attack that is mounted against us (meaning our digital devices) by means of cyberspace. Cyberspace, a virtual space that does not exist, has become the metaphor to help us understand digital weaponry that intends to harm us.

What is real, however, is the intent of the attacker as well as the potential impact. While many cyberattacks are mere nuisances, some are quite serious, even potentially threatening human lives.

Cyber threats are a big deal. Cyber-attacks can cause electrical blackouts, failure of military equipment, and breaches of national security secrets. They can result in the theft of valuable, sensitive data like medical records. They can disrupt phone and computer networks or paralyze systems, making data unavailable. It's not an exaggeration to say that cyber threats may affect the functioning of life as we know it.

The threats are growing more serious, too. Gartner explains, "Cybersecurity risks pervade every organization and aren't always under IT's direct control. Business leaders are forging ahead with their digital business initiatives, and those leaders are making technology-related risk choices every day. Increased cyber risk is real — but so are the data security solutions."

3.4 Malware

Malicious software, or malware, plays a part in most computer intrusion and security incidents. Any software that does something that causes harm to a user, computer, or network can be considered malware, including viruses, trojan horses, worms, rootkits, scareware, and spyware. While the various malware incarnations do all sorts of different things, as malware analysts, we have a core set of tools and techniques at our disposal for analysing malware. [10]

Malware analysis is the art of dissecting malware to understand how it works, how to identify it, and how to defeat or eliminate it. And you do not need to be an uber-hacker to perform malware analysis. With millions of malicious programs in the wild, and more encountered every day, malware analysis is critical for anyone who responds to computer security incidents. [5]

Types of malware

These are the main types of malware that can be found across the web.

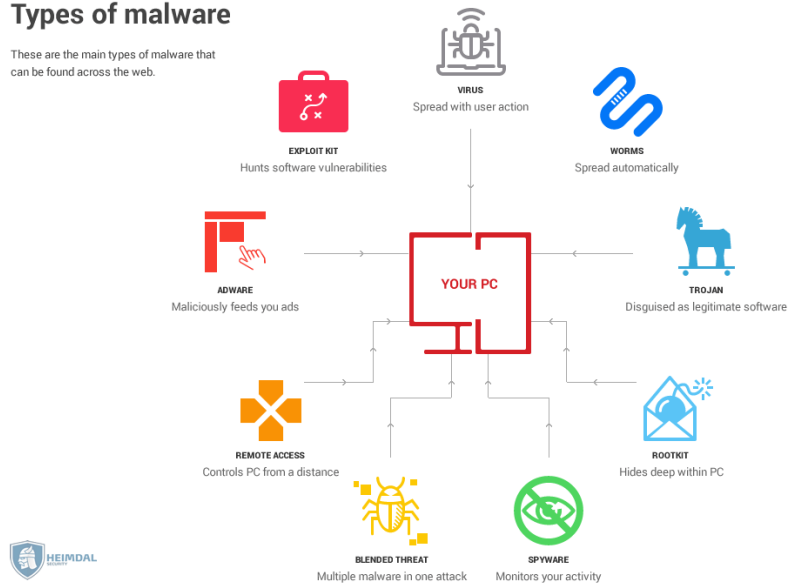


Figure 2. Types of malware [9]

Malware breaches a network through a vulnerability, typically when a user clicks a dangerous link or email attachment that then installs risky software. once inside the system, malware can do the following:

- Blocks access to key components of the network (ransomware)
- Installs malware or additional harmful software
- Covertly obtains information by transmitting data from the hard drive (spyware)
- Disrupts certain components and renders the system inoperable

3.5 Security in the banking sector at present and trend in recent years

Before the rise of the digital economy, only physical barriers and computer firewalls were needed to protect customer resources and information. Today, money and associated data move around the world in a matter of milliseconds, in many cases without human interaction, so complexity is greatly increased. For banks, insurers and other financial services companies, it is critical that their technologies deliver what customers need, while addressing security issues and complying with regulations.[6]

Companies in the financial services industry are responsible for holding and managing their customers' money and financial information. They must comply with federal, state and local regulations governing almost every aspect of the industry to ensure that financial data is as secure as possible.

Customers have unprecedented access to their financial information from a variety of devices, which is also a risk factor. Protecting customer data from fraud, complying with government regulations and, at the same time, developing more convenient and intuitive financial products and services is no easy task. Adding to this complex challenge is **the need to adapt to changing criminal threats**.

To respond to this trend, government agencies around the world are updating existing laws, regulations and technology standards, as well as implementing new ones to adapt to a rapidly evolving digital economy.

Why are IT security and data regulation important?

The way money and data are managed and stored today is very different from 20 years ago. Millions of people use the Internet to communicate, shop, work and play. Companies around the world have adapted their business models in response to this shift in consumer focus. While the Internet allows information to be accessed, stored and transferred quickly and conveniently, some unscrupulous individuals use it to exploit any vulnerabilities they find for their own gain. Data breaches are becoming increasingly serious, highlighting the need for stronger measures to protect information. Regulatory compliance and financial security represent a constant effort to stay ahead of criminals, who will continue to look for ways to infiltrate, so no system can guarantee total and permanent security. However, with advances in security technologies, the adoption of new standards and a change in attitudes towards digital financial services, businesses will be able to stay one step ahead of intruders.

How do security and compliance in financial services work? The way in which the financial services sector approaches security and compliance varies depending on a number of factors. However, there is one constant: governments and companies around the world are investing heavily in updating security and compliance measures to meet

the needs of the digital economy. Technological innovations, in addition to the application of lessons learned from past developments, improve the receipt, management, dissemination, storage and access to data. Many of the features listed below are available in most countries:

Encryption

Sensitive information is encrypted and converted into a code that can only be accessed with the correct decryption key. However, in order to encrypt, verify and decrypt the data, more time and processing power is required. To speed up the processing of the ever-increasing data, banks upgrade and expand existing IT infrastructures or implement new, more flexible and robust systems that enable faster and more easily expandable data encryption.

Multi-factor authentication

Logging in with multiple forms of authentication is becoming a popular option, and not just for financial services websites. The user enters a password or key. This triggers a request to send a code by text message to a pre-registered device. The code is a randomly generated set of characters that the user enters to complete the login process. While this adds a step to the initial process, it is a major impediment to criminals who want to log in to the site. The Second Payment Services Directive (PSD2) requires EU banks to apply multi-factor authentication to all transactions, including those that cross international borders.

Data distribution and storage

The influence of the GDPR extends beyond the EU and drives the policies of financial institutions around the world in relation to data storage, distribution and access. Storing data in one place is no longer a secure option for businesses, even those that rely on cloud services to store digital information. Reliance on a single provider creates a concentration risk that leaves data vulnerable to leakage. Distributing storage and functions in separate parts across multiple providers reduces risk and makes it harder for intruders to access.

Artificial intelligence (AI)

Predefined algorithms can identify transactions that do not fit a normal pattern; for example, a transaction made in London by a customer living in the US. But if the customer visits London several times a year and makes legitimate trades from there, the algorithm will always send alerts about them. AI can be applied to learn and adapt to the customer's behaviour. It also updates algorithms so that alerts are no longer sent for future transactions that match usage patterns. AI also uses biometrics, which is a method of identifying customers using their unique characteristics to gain access to account information. Eye, facial and fingerprint recognition are features of many smart devices. More and more banks are offering these options in their mobile applications. This adds another layer of security, making it more difficult for criminals to break into systems.

3.5 MITRE ATT&CK matrix

MITRE is a non-governmental corporation founded in 1958 whose mission is to try to solve problems that contribute to a safer world, so in this opportunity we will analyse its MITRE ATT&CK (Tactics, Techniques and Adversary Common Knowledge) framework, a platform that organises and categorises the different types of attacks, threats and procedures carried out by different attackers in the digital world and that allows identifying vulnerabilities in computer systems. The ATT&CK [7] knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

MITRE has ATT&CK distributed in a few different matrices: Enterprise, Mobile and PRE-ATT&CK. Each of these matrices contains various tactics and techniques associated with the content of the matrix.

- The Enterprise matrix is composed of techniques and tactics that apply to Windows, Linux or MacOS systems.
- Mobile contains tactics and techniques that apply to mobile devices.

- PRE-ATT&CK contains tactics and techniques related to what attackers do before attempting to breach a particular network or system.

In this project we will work with the Enterprise matrix.

3.5.1 Operation of the matrix

MITRE's ATT&CK™ matrix is closely related to the well-known Cyber Kill Chain® framework developed by Lockheed Martin.

The Cyber Kill Chain [11] framework was developed as an advanced method to detect and prevent any cyber intrusion. MITRE's ATT&CK matrix uses this model to understand the logic of an attacker.

To better understand the principles of the MITRE ATT&CK matrix, let us consider the Cyber Kill Chain framework in detail.

The framework contains the following seven steps that adversaries have to follow to achieve their malicious intentions:

Reconnaissance — Choose a target and get as much information about it as possible.

Weaponization — Based on the information acquired during reconnaissance, choose the best tools for carrying out the attack.

Delivery — Deliver the weaponized bundle to the target's environment.

Exploitation — Exploit the vulnerability to execute code in the target's system.

Installation — Install a persistent backdoor to maintain remote access to the target's environment.

Command and Control (C&C) — Establish a command channel to enable the adversary to remotely manipulate the victim.

Actions on Objective — Take the planned illegal action, such as data destruction, exfiltration, or encryption.

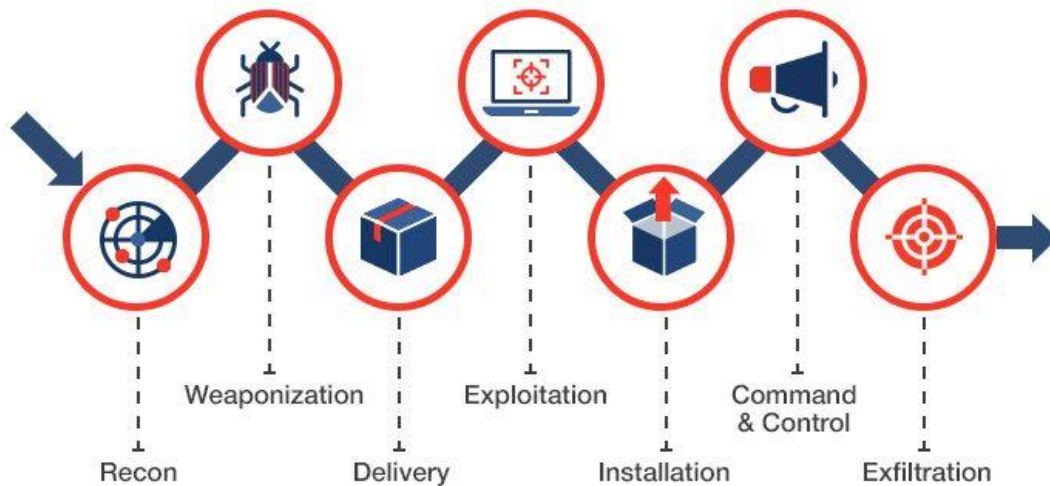


Figure 3. Cyber Kill Chain

The Cyber Kill Chain is a systematic process for an attacker to achieve the desired effect. Using the **ATT&CK** matrix and keeping in mind the attack stages the adversary has to undertake, cybersecurity developers, testers, and officers get a powerful method to create and emulate various attack scenarios to verify the reliability of an enterprise platform or company's defensive systems.

This matrix does not replace the Cyber Kill Chain, but simply clarifies what is behind the last three stages of the matrix.

3.5.2 Structure breakdown: tactics and techniques

When looking at ATT&CK in matrix form, the column headings at the top are **tactics** and, basically, categories of techniques. The tactics correspond to what the attackers are trying to accomplish, while the individual techniques correspond to how they accomplish those steps or objectives.

Let's review the eleven tactics of the current version of the ATT&CK matrix.

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Active Scanning (012)	Acquire Infrastructure (016)	Drive-by Compromise (016)	Command and Scripting Interpreter (018)	Account Manipulation (014)	Abuse Elevation Control Mechanism (014)	Abuse Elevation Control Mechanism (014)	Brute Force (014)	Account Discovery (014)	Exploitation of Remote Services (014)	Archive Collected Data (013)	Application Layer Protocol (014)	Automated Exfiltration (017)	Account Access Removal (017)
Gather Victim Host Information (014)	Compromise Accounts (012)	Exploit Public-Facing Application (012)	Exploitation for Client Execution (012)	BITS Jobs (012)	Access Token Manipulation (013)	Access Token Manipulation (013)	Credentials from Password Stores (013)	Application Window Discovery (014)	Internal Spearphishing (014)	Audio Capture (014)	Communication Through Removable Media (014)	Data Transfer Size Limits (017)	Data Destruction (017)
Gather Victim Identity Information (012)	Compromise Infrastructure (016)	External Remote Services (016)	Inter-Process Communication (012)	Boot or Logon Autostart Execution (017)	Boot or Logon Autostart Execution (017)	Deobfuscate/Decode Files or Information (013)	Exploitation for Credential Access (013)	Browser Bookmark Discovery (014)	Lateral Tool Transfer (014)	Automated Collection (014)	Data Encrypted for Impact (017)	Data Manipulation (013)	Data Encrypted for Impact (017)
Gather Victim Network Information (016)	Develop Capabilities (014)	Hardware Additions (014)	Native API (014)	Boot or Logon Initialization Scripts (013)	Boot or Logon Initialization Scripts (013)	Direct Volume Access (013)	Forward Authentication (013)	Cloud Infrastructure Discovery (014)	Remote Service Session Hijacking (017)	Data from Cloud Storage Object (014)	Data Encoding (012)	Exfiltration Over Alternative Protocol (013)	Data Encrypted for Impact (017)
Gather Victim Org Information (014)	Establish Accounts (012)	Phishing (013)	Scheduled Task/Job (013)	Browser Extensions (012)	Browser Extensions (012)	Execution Guardrails (017)	Input Capture (014)	Cloud Service Dashboard (014)	Remote Services (016)	Data from Configuration Repository (012)	Data Obfuscation (012)	Exfiltration Over C2 Channel (013)	Defacement (012)
Phishing for Information (013)	Obtain Capabilities (016)	Replication Through Removable Media (016)	Shared Modules (016)	Compromise Client Software Binary (016)	Create or Modify System Process (014)	Exploitation for Defense Evasion (017)	Man-in-the-Middle (012)	Domain Trust Discovery (014)	Replication Through Removable Media (016)	Data from Information Repositories (012)	Dynamic Resolution (013)	Exfiltration Over Other Network Medium (017)	Disk Wipe (012)
Search Closed Sources (012)	Supply Chain Compromise (013)	Software Deployment Tools (013)	System Services (012)	Create or Modify System Process (014)	Event Triggered Execution (017)	File and Directory Permissions Modification (012)	Modify Authentication Process (014)	File and Directory Discovery (014)	Network Service Scanning (014)	Fallback Channels (014)	Encrypted Channel (012)	Exfiltration Over Physical Medium (017)	Endpoint Denial of Service (014)
Search Open Technical Databases (017)	Trusted Relationship (014)	User Execution (012)	User Execution (012)	Exploitation for Privilege Escalation (017)	Group Policy Modification (017)	Group Policy Modification (017)	OS Credential Dumping (013)	Network Sniffing (014)	Software Deployment Tools (014)	Data from Local System (014)	Ingress Tool Transfer (014)	Exfiltration Over Web Service (012)	Firmware Corruption (014)
Search Open Websites/Domains (012)	Valid Accounts (014)	Windows Management Instrumentation (014)	External Remote Services (014)	Hijack Execution Flow (017)	Hijack Execution Flow (017)	Hide Artifacts (017)	Steal Application Access Token (014)	Network Share Discovery (014)	Taint Shared Content (014)	Data from Network Shared Drive (014)	Non-Application Layer Protocol (014)	Scheduled Service Stop (017)	Resource Hijacking (017)
Search Victim-Owned Websites (012)	Hijack Execution Flow (017)	Process Injection (017)	Implant Container Image (016)	Scheduled Task/Job (013)	Scheduled Task/Job (013)	Impair Defenses (017)	Steal or Forge Kerberos Tickets (014)	Password Policy Discovery (014)	Use Alternate Authentication Material (014)	Data from Removable Media (014)	Non-Standard Port (014)	Transfer Data to Cloud Account (017)	System Shutdown/Reboot (017)
	Office Application Startup (016)	Indirect Command Execution (016)	Pre-OS Boot (013)	Modify Authentication Process (014)	Modify Authentication Process (014)	Indirect Command Execution (016)	Steal Web Session Cookie (014)	Peripheral Device Discovery (014)	Man in the Browser (014)	Data from Staged (012)	Protocol Tunneling (014)	Service Stop (017)	System Shutdown/Reboot (017)
	Scheduled Task/Job (013)	Masquerading (016)	Server Software Component (013)	Modify Cloud Compute Infrastructure (014)	Masquerading (016)	Two-Factor Authentication Interception (016)	Unsecured Credentials (016)	Query Registry (014)	Man in the Browser (014)	Remote System Discovery (014)	Remote Access Software (014)	Service Stop (017)	System Shutdown/Reboot (017)
								Process Discovery (014)	Man in the Browser (014)	Screen Capture (014)	Traffic Signaling (017)	Service Stop (017)	System Shutdown/Reboot (017)
								Software Discovery (011)	Man in the Browser (014)	Video Capture (014)	Web Service (013)	Service Stop (017)	System Shutdown/Reboot (017)

Figure 4. ATT&CK matrix breakdown

Gaining initial access

The adversary is trying to get into your network. Initial access consists of techniques that use multiple entry vectors to obtain their initial foothold within a network. Footholds gained through initial access may allow for continued access, like valid accounts and use of external remote services, or may be limited-use due to changing passwords.

Execution

The adversary is trying to run malicious code. Execution consists of techniques that result in adversary-controlled code running on a local or remote system. Techniques that run malicious code are often paired with techniques from all other tactics to achieve broader goals, like exploring a network or stealing data.

Persistence

The adversary is trying to maintain their foothold. Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access.

Privilege escalation

The adversary is trying to gain higher-level permissions.

Privilege Escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network. Adversaries can often enter and explore a network with unprivileged access but require elevated permissions to follow through on their objectives. Common approaches are to take advantage of system weaknesses, misconfigurations, and vulnerabilities.

Defense Evasion

The adversary is trying to avoid being detected. Defense Evasion consists of techniques that adversaries use to avoid detection throughout their compromise. Techniques used for defense evasion include uninstalling/disabling security software or obfuscating/encrypting data and scripts.

Credential Access

The adversary is trying to steal account names and passwords. Credential Access consists of techniques for stealing credentials like account names and passwords.

Discovery

The adversary is trying to figure out your environment. Discovery consists of techniques an adversary may use to gain knowledge about the system and internal network. These techniques help adversaries observe the environment and orient themselves before deciding how to act.

Lateral movement

The adversary is trying to move through your environment. Lateral Movement consists of techniques that adversaries use to enter and control remote systems on a network. Following through on their primary objective often requires exploring the network to find their target and subsequently gaining access to it.

Collection

The adversary is trying to gather data of interest to their goal. Collection consists of techniques adversaries may use to gather information and the sources information is collected from that are relevant to following through on the adversary's objectives. Frequently, the next goal after collecting data is to steal (exfiltrate) the data.

Command and Control

The adversary is trying to communicate with compromised systems to control them. Command and Control consists of techniques that adversaries may use to communicate with systems under their control within a victim network. Adversaries commonly attempt to mimic normal, expected traffic to avoid detection.

Exfiltration

The adversary is trying to steal data. Exfiltration consists of techniques that adversaries may use to steal data from your network. Once they've collected data, adversaries often package it to avoid detection while removing it. This can include compression and encryption.

A **technique** is a specific behaviour that seeks to achieve a goal and is often a single step in a series of activities employed to complete the attacker's overall mission. ATT&CK provides various details on each technique, including a description, examples, references, and suggestions for mitigation and detection.

Drive-by Compromise

A drive-by compromise is when an adversary gains access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is targeted for exploitation. This can happen in several ways, but there are a few main components:

Multiple ways of delivering exploit code to a browser exist, including:

- A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, cross-site scripting.
- Malicious ads are paid for and served through legitimate ad providers.
- Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content).

Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted attack is referred to a strategic web compromise or watering hole attack. There are several known examples of this occurring.^[1]

Typical drive-by compromise process:

1. A user visits a website that is used to host the adversary controlled content.
2. Scripts automatically execute, typically searching versions of the browser and plugins for a potentially vulnerable version.

<p>ID: T1189</p> <p>Tactic: Initial Access</p> <p>Platform: Windows, Linux, macOS</p> <p>Permissions Required: User</p> <p>Data Sources: Packet capture, Network device logs, Process use of network, Web proxy, Network intrusion detection system, SSL/TLS inspection</p> <p>Version: 1.0</p>

Figure 5. Example of a technique description in MITRE's ATT&CK

ATT&CK is valuable in a variety of everyday situations. Any defensive activity that references attackers and their behaviours can benefit from the application of the ATT&CK taxonomy. In addition to providing a common lexicon for IT defenders, ATT&CK also provides a basis for penetration testing and red teaming. This provides a common language for defenders and red teams when referring to adversarial behaviour.

Examples of cases where the ATT&CK taxonomy may be useful to apply:

Mapping defensive controls

Defensive controls may have an understood meaning in comparison to the ATT&CK tactics and techniques to which they are applied.

Threat search

Mapping defences to ATT&CK generates a roadmap of defensive breaches that provide threat seekers with the perfect locations to find possible missed attacker activity.

Detections and investigations

The Security Operations Centre (SOC) and incident response team can reference ATT&CK techniques and tactics that have been detected or discovered. This helps understand where defensive strengths and weaknesses lie, and validates mitigation and detection controls, and can uncover misconfigurations and other operational issues.

Reference actors

Actors and groups can be associated with specific, definable behaviours.

Tool integrations

Disparate tools and services can be standardized into ATT&CK tactics and techniques, bringing cohesion to a defence that often lacks it.

Sharing

When sharing information about an attack, an actor or group, or defensive controls, defenders can ensure a common understanding through the use of ATT&CK techniques and tactics.

Red team/penetration testing activities.

Red team, purple team, and penetration testing activities planning, execution, and reporting can use ATT&CK to speak a common language with defenders and report recipients, as well as with each other.

3.6 Threat Modelling

Threat modelling (TM) is a fundamental security practice in any software development process. One of its main differentiators with respect to other practices is that TM is one of the activities with the best return on investment, as it allows identifying and managing security flaws at the design level, before they are implemented in the source code, where the cost of mitigation would be exponentially higher. Its main objective is to identify the attacks to which an application could be susceptible, as well as the security controls that will allow the software to achieve the desired level of security.

3.6.1 Main threats identified in the banking sector

Ransomware

Ransomware is the hijacking of information by malicious software that encrypts the contents of a drive or hard disk. In this computer attack, the user receives an alert message asking for a ransom in order to recover their "hijacked" information. Payment is usually requested in cryptocurrency, in order to remove any trace that can be investigated. [1]

Like other types of malware, ransomware is usually distributed through phishing emails that contain links to malicious content or dangerous attachments. In addition, users may unknowingly download it when they visit infected websites that install malicious software on their computer without their consent. Nowadays, ransomware is also distributed through social networks and instant messaging applications.

This type of cyber-attack has been going on for years, mostly targeting businesses. With changes in encryption algorithms becoming increasingly complicated, Ransomware is growing and is difficult to combat. According to the company Panda Cloud Antivirus, it is estimated that by 2021 it had reached 6 billion dollars in data ransomware. Different types currently exist:

- **Police virus.** This type of ransomware attack displays a message warning that the machine has been blocked for accessing illegal sites. This message pretends to be sent by the police in an attempt to trick as many people as possible into paying the requested fine.
- **Filecoder.** This ransomware encrypts files, preventing their access. If the user pays the ransom in cryptocurrencies, he will be provided with the key to unlock the files. There is a variant of this ransomware, Wiper, which once the ransom is paid, the code does not unlock the files, but deletes them.
- **Lockscreen.** This ransomware blocks access to the computer, preventing it from performing any function unless the ransom is paid and the code for its deactivation is received.
- **Hoax.** This ransomware technique does not actually lock files like Filecoder, but pretends to do so, forcing victims to pay out of fear.

Data Breach/Leakage

A data breach is an incident where information is stolen or taken from a system without the knowledge or authorization of the system's owner. A small company or large organization may suffer a data breach. Stolen data may involve sensitive, proprietary, or confidential information such as credit card numbers, customer data, trade secrets, or matters of national security. The effects brought on by a data breach can come in the form of damage to the target company's reputation due to a perceived 'betrayal of trust.' Victims and their customers may also suffer financial losses should related records be part of the information stolen.

Most data breaches are attributed to hacking or malware attacks. Other frequently observed breach methods include the following:

- **Insider leak:** A trusted individual or person of authority with access privileges steals data.
- **Payment card fraud:** Payment card data is stolen using physical skimming devices.
- **Loss or theft:** Portable drives, laptops, office computers, files, and other physical properties are lost or stolen.

- **Unintended disclosure:** Through mistakes or negligence, sensitive data is exposed.

Identity and access

Identity management and access control is the discipline of managing access to enterprise resources to keep systems and data secure. As a key component of your security architecture, it can help verify your users' identities before granting them the right level of access to workplace systems and information. While people might use the terms' identity management, authentication, and access control interchangeably, each of these individually serve as distinct layers for enterprise security processes. Within that scope, both authentication and access control—which regulates each user's level of access to a given system—play vital roles in securing user data.

According to Okta's Business at Work 2019 [8] report, nearly 40% of employees use the same two to four passwords to access over 100 apps on average. In the workplace, this means corporate IT administrators have their hands full managing user credentials for multiple systems. As organizations embrace cloud-based tools for a mix of on-prem and online services, IT admins have become responsible for securing access to many platforms with varying identity management and access control solutions. This can be challenging for IT teams and can also lead to a frustrated user base that needs to stay on top of multiple logins.

3.6.2 Entry channels

We will consider as possible entry channels any point of the bank's architecture where corrupt information is allowed to be uploaded, downloaded directly from the internet or any compromised source of entry. Main channels are presented below:

3.6.2.1 Browsing

General Internet navigation, by using compliant browsers.

3.6.2.2 Customer's channel

A channel we have to interact directly with customers, it includes access to the bank's application or online banking, where the user can view all his data and accounts and can carry out all kinds of transactions remotely.

3.6.2.3 USB

Use of removable devices for data transfers, software installation. May refer to devices for personal use, e.g., mobile phones or USB.

3.6.2.4 Mail

Bank's mail server, where users access corporate and personal mailboxes.

3.6.2.5 Third Parties

Especially VPN or MPLS, SFTP. Includes:

- Subsidiaries
- Business customers
- Service providers
- SaaS

3.6.2.6 Online Sharing

Online repositories where users can share documents and files.

3.6.2.7 Citrix

Citrix XenApp is an on-demand application delivery solution that allows you to virtualize, centralize and manage any Windows® application in the data centre, and deliver it instantly as a service to users, wherever they are and whatever device they use.

3.6.2.8 API & Web Services

A web service is a means of intercommunication and interoperability between machines connected in a network. An API or application programming interface is a set of definitions and protocols used to design and integrate application software.

3.6.2.9 Cloud Storage

Channel where data is stored in the cloud for remote access.

3.6.2.10 Endpoints (ATMs)

Physical terminals where you physically interact with the bank and where you can make direct transactions.

3.6.3 Entry vectors

In cybersecurity, an attack vector is a path or means by which an attacker can gain unauthorized access to a computer or network to deliver a malicious result. In my study, it is directly related to the MITRE Matrix, for each of its columns (phases of the attack) many of them apply but they are not always the same, depending on the threat and the entry channel through which it is transmitted.

The term itself comes from the military domain; an attack vector is usually referred to as a hole or flaw present in the established defence. Such flaws can be the leaking of information by a double agent; a weakness in the transmission of a top-secret message; etc.

In this way, cybersecurity attack vectors exploit network weaknesses such as applications, computers and e-mail, as well as personnel weaknesses through social engineering practices.

For these reasons, it is advisable to have technical solutions in computer security designed specifically for each possible failure, as well as to train personnel who could be affected by various types of computer attacks.

For example, in the technique “*Drive-by Compromise*” adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behaviour such as acquiring Application Access Token. This attack vector appears in the Ransomware threat and the entry channels involved are the following: Browsing, Customers Channel, Third parties, Online Sharing and Cloud Storage.

4 Problem formulation and methodology

In this chapter we will formulate the challenge and set out both the problem and the methodology that will be used to solve it.

4.1 Challenge

The problem we have tackled with this project is that of having vulnerabilities not foreseen or even contemplated in a bank's security architecture, due to insufficient defence against certain attack vectors and not having a clear mapping with what capacity covers what recommended mitigation.

This makes it possible to exploit vulnerabilities that initially may not even seem relevant, or to generate a dangerous attack from an apparently non-critical input channel.

The challenge will therefore be to do this study/analysis efficiently and in depth, in order to see as many possibilities as possible given the characteristics of each attack.

Taking into account the channels of entry to the bank, the phases of the attacks and the variant techniques of each attack, hundreds of different possibilities emerge, which are grouped together with the corresponding mitigations. The focus is therefore to map the mitigations currently in place in the bank with different groupings of attacks to see what is covered and to identify key risks.

4.2 First steps

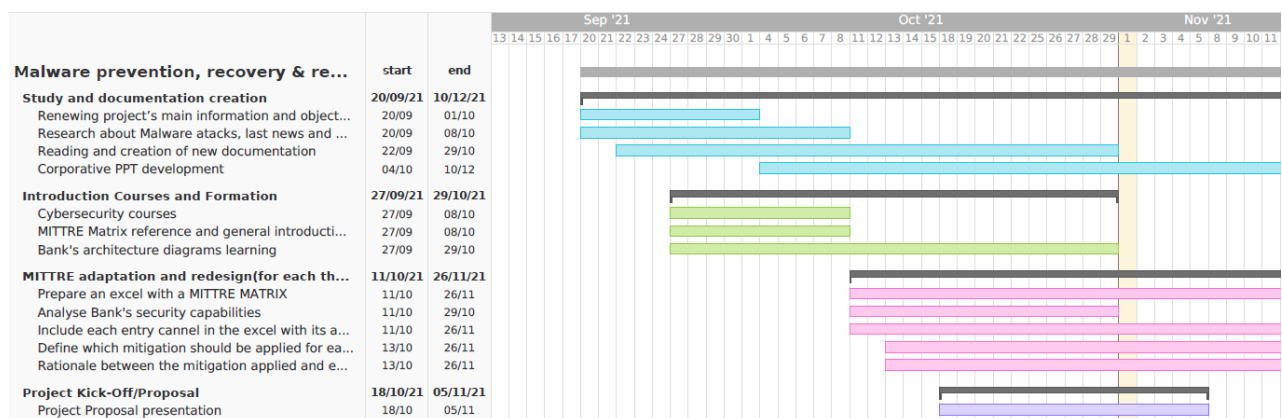


Figure 6. Gantt diagram of first steps

First, an in-depth study of the current cybersecurity situation was carried out, all the bases of the project that we have seen in chapter 3 were documented and the 2021 cybersecurity reports were reviewed, in order to recognise the main threats detected, see the evolution of attacks and review the main incidents.

Trainings were held at EY in the first weeks to study all the capabilities of the client bank and its security architecture, cyber security trainings and introduction to the ATT&CK MITRE matrix.

Once this part was completed, three Excel documents were generated with an adaptation and redesign of the ATT&CK matrix for each of the three main security threats; Ransomware, Data Leakage and Identity and Access. In each document there is a tab with the applicable part of the matrix according to the threat, where the fields used for each individual study are highlighted.

1	Mitre column applicable	Attack vectors applicable
2	Initial Access	Trusted Relationship
3	Initial Access	Valid Accounts
4	Initial Access	Phishing
5	Execution	System Services
6	Persistence	Accounts (creation or manipulation)
7	Persistence	Create or Modify System Process
8	Privilege Escalation	Abuse Elevation Control Mechanism
9	Privilege Escalation	Access Token Manipulation
10	Privilege Escalation	Create or Modify System Process
11	Privilege Escalation	Domain Policy Modification
12	Privilege Escalation	Scheduled Task/Job
13	Privilege Escalation	Valid Accounts
14	Defense Evasion	Abuse Elevation Control Mechanism
15	Defense Evasion	Access Token Manipulation
16	Defense Evasion	Domain Policy Modification
17	Defense Evasion	File and Directory Permissions Modification
18	Defense Evasion	Impair Defenses
19	Defense Evasion	Modify Authentication Process
20	Defense Evasion	Modify Registry
21	Defense Evasion	Use Alternate Authentication Material
22	Defense Evasion	Valid Accounts
23	Credential Access	Brute Force
24	Credential Access	Credentials from Password Stores
25	Credential Access	Exploitation for Credential Access
26	Credential Access	Forced Authentication
27	Credential Access	Forge Web Credentials
28	Credential Access	Modify Authentication Process
29	Credential Access	OS Credential Dumping
30	Credential Access	Steal Application Access Token
31	Credential Access	Steal Web Session Cookie
32	Credential Access	Steal or Forge Kerberos Tickets
33	Credential Access	Two-Factor Authentication Interception
34	Credential Access	Unsecured Credentials
35	Discovery	Account Discovery
36	Discovery	Password Policy Discovery
37	Lateral Movement	Remote Service Session Hijacking

Figure 7. Applicable MITRE fields for Identity and Access

Then there is a tab for each input channel of the bank, the ten we saw in chapter 3, and for each tab we had the following structure:

Mitre column applicable	Attack vectors applicable	Mitigations applicable	Gap analysis result	Rationale
Initial Access	Valid accounts	Application Developer Guidance	Covered	
Initial Access	Valid accounts	Password Policies	Covered	
Initial Access	Valid accounts	Privileged Account Management	Covered	
Persistence	Accounts (creation or manipulation)	Multi-factor Authentication	Covered	
Persistence	Accounts (creation or manipulation)	Network Segmentation	Partially Covered	
Persistence	Accounts (creation or manipulation)	Privileged Account Management	Covered	
Privilege Escalation	N/A	N/A	N/A	
Defense Evasion	N/A	N/A	N/A	
Credential Access	Brute Force	Account Use Policies	Covered	
Credential Access	Forced Authentication	Password Policies	Covered	
Credential Access	Exploitation for Credential Access	Exploit Protection	Covered	
Credential Access	Exploitation for Credential Access	Update Software	Covered	
Credential Access	Exploitation for Credential Access	Threat Intelligence Program	Covered	
Credential Access	Steal Application Access Token	User Training	Covered	
Credential Access	Steal Web Session Cookie	User Training	Covered	
Credential Access	Steal Web Session Cookie	Software Configuration	Partially Covered	

Figure 8. Customer Channel IaA tab

As can be seen in the example Figure 8, we see the column of the ATT&CK matrix affected, the column with the applicable attack vectors, the column with the applicable mitigations, the column where it is assessed whether it is covered, partially covered or not covered and finally the rationale where the mapping between the attack and the mitigation covered by the bank is explained; which has been omitted for confidentiality reasons. When a row does not apply for this control, it is defined N/A and we do not take it into account in the report. Let's take a look at the tab in detail again:

Once we have considered all the possible entries and all the attack vectors, we must analyze what security capabilities we have in the bank exhaustively to find out what possibilities we still have to cover or what capabilities are not sufficient to ensure that a vulnerability is prevented. Possible mitigations have been proposed for each of the cases in the study. We must take into account that each of the more than 750 possibilities that have emerged in the study of the 3 threats, 10 entry channels and about 50 attack vectors; has a more or less concise or customized mitigation.

Once the scenario is clear, a gap analysis exercise must be carried out to see whether all the possible risks posed by the bank's current security are covered, not covered or partially covered. For each of them, all the bank's policies involved, low-level architecture diagrams and specific documentation for each of the threats and entry

channels had to be consulted, which translates into a very extensive task with many details to take into account.

A rationale has been generated for each of the attack possibilities, which allows to see which security capabilities cover such an attack (whether protocols, software or tools), which cover them partially and if there is any that is not covered, the need for implementation has been highlighted. The idea is to have a technical conclusion on which vulnerabilities are detected or which risks are potentially critical, so that they can be consulted quickly and concisely

From here the project is divided into two parts (a, b), the main one is the study, analysis and modelling of threats and the second is the design of a tool to automate the response to threats and streamline the mapping process by means of user forms.

a. Threat modelling

Goals were the following:

- a.1 Identify and analyse the main threats in the financial/banking sector.
- a.2. Identify and study entry channels
- a.3. Identify and study attack vectors
- a.4. Identify and study current capabilities
- a.5. Gap analysis (bank capabilities)

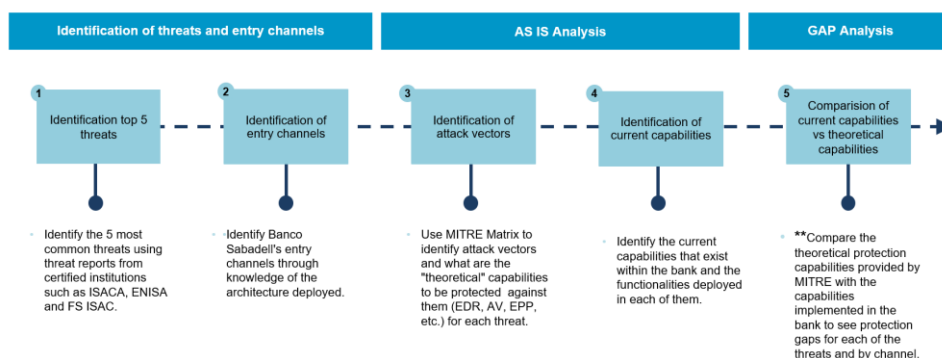


Figure 9. Methodology slide from the PowerPoint created

Concretely, I have made a first version of the whole study that has been reviewed weekly by my team and together with a colleague we have made a PowerPoint presentation in order to generate the complete report. The report has an introduction to the MITRE matrix, a breakdown of the three main threats (Ransomware, Data Leakage and Identity and Access), where each has a specific analysis of its entry channels and has a customised MITRE matrix generated by me, tailored according to the applicable mitigations. In addition to the proposed mitigations in each input channel of each threat, I have made a slide with all the gap analysis at a high level in order to quickly identify the least covered capabilities and see where the main security risks are. At the end of each threat, I made a slide with final conclusions where the impact of the risk is specifically measured.

USB Status

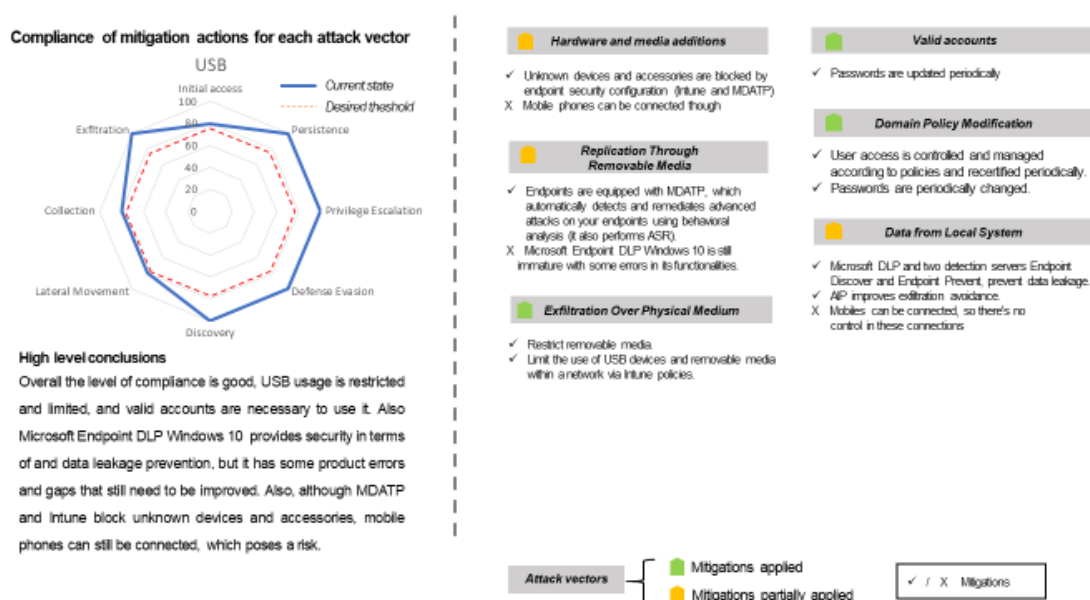


Figure 10. USB Status PowerPoint slide

As can be seen in Figure 10 is presented one of the slides with the compliance level of the example bank for the USB input channel made for this project. We see a radar diagram showing the levels of compliance, a breakdown of the most relevant attack techniques for the report in orange when mitigations are applied that partially cover and

in green when mitigations fully cover. Finally, at the bottom left, there is a high-level conclusion to quickly understand the results obtained and to be able to remedy them.

b. Automate the response process

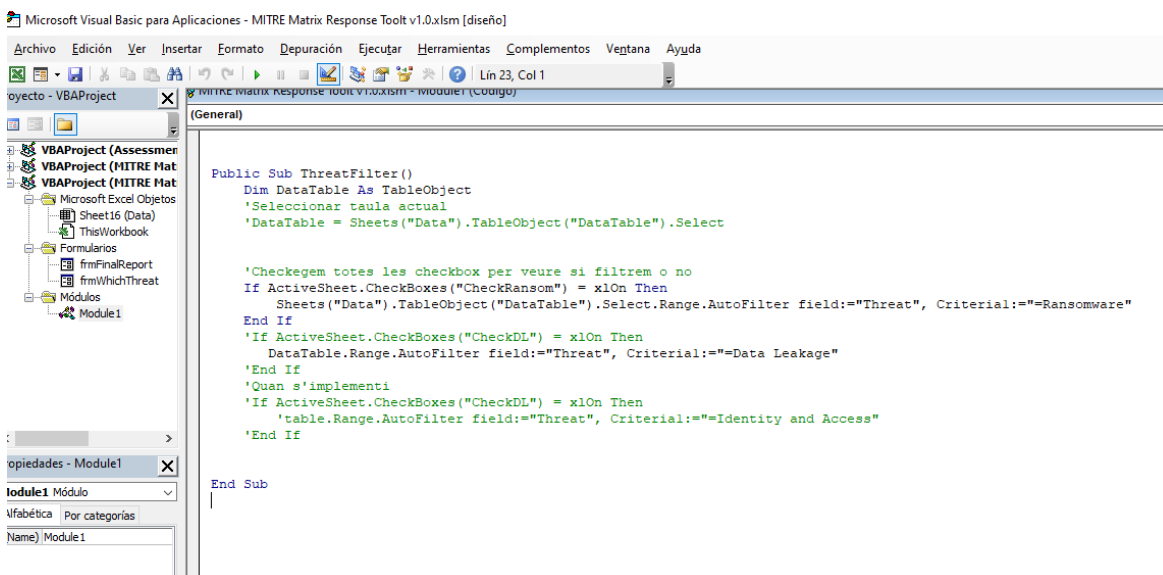
The tool has been created from scratch by me and developed in the last weeks.

b.1. The appropriate action is sought according to the type of threat detected.

The automated response can be, for example, to contact the security managers of different entities via automated emails to speed up the resolution of the problem, to have scripts to enable/disable system features such as firewall rules, to isolate the systems via VPN or sandboxing or to run some Macros previously programmed.

b.2. Modular architecture in order to avoid interferences between responses and create synergies appropriately.

It consists of a VBA Excel based tool where the user can filter by threat and entry channel depending on which study is currently carried out and introduce whether a mitigation is covered or not. Finally, a report is generated with identified risks and generates graphs in a dashboard where the results are presented.



```

Microsoft Visual Basic para Aplicaciones - MITRE Matrix Response Tool v1.0.xlsm [diseño]
Archivo  Edición  Ver  Insertar  Formato  Depuración  Ejecutar  Herramientas  Complementos  Ventana  Ayuda
Lin 23, Col 1
VBAProject - VBAProject
(VBProject)
  VBAProject (Assessment)
  VBAProject (MITRE Mat)
  VBAProject (MITRE Mat)
  Microsoft Excel Objects
    Sheet16 (Data)
    ThisWorkbook
  Formularios
    frmFinalReport
    frmWhichThreat
  Módulos
    Module1

Public Sub ThreatFilter()
    Dim DataTable As TableObject
    'Seleccionar taula actual
    'DataTable = Sheets("Data").TableObject("DataTable").Select

    'Checkegem totes les checkbox per veure si filtrem o no
    If ActiveSheet.CheckBoxes("CheckRansom") = xlOn Then
        Sheets("Data").TableObject("DataTable").Select.Range.AutoFilter field:="Threat", Criteria:="=Ransomware"
    End If
    'If ActiveSheet.CheckBoxes("CheckDL") = xlOn Then
        DataTable.Range.AutoFilter field:="Threat", Criteria:="=Data Leakage"
    End If
    'Quan s'implementi
    'If ActiveSheet.CheckBoxes("CheckDL") = xlOn Then
        'table.Range.AutoFilter field:="Threat", Criteria:="=Identity and Access"
    End If

End Sub
  
```

Figure 11. VBA code inside the tool

5 Results

In this section it will be presented the results of this study and the advantages identified in the process.

As seen in chapter 4, a very structured methodology has been followed to achieve all the objectives and to achieve a meaningful, well-defined in-depth study of significant value for the project and for the company. The idea is that this study and this tool can be used in any company in the sector in a fast, optimal and case-specific way, through the interaction of a user of the bank in question.

For this study we have worked mainly with Excel where we have sorted, classified and prepared all the data collected from the bank's security architecture, the parameters and data of the MITRE ATT&CK matrix and the security parameters previously established. For each threat raised in this project, a separate Excel document has been created, as we have seen in the last chapter, where each of the tabs referring to the bank's entry channels has a column with the corresponding rationale. This rationale or conclusion aims to give a complete and detailed view of which security technologies/capabilities comply and to what degree the proposed mitigation covers.

5.1 Use case

We will now look at an anonymised example to analyse it as a use case, for the example we will use the **USB entry channel** of an **invented bank** for the **Data Leakage threat** and we will see an example of analysis and the slides that are generated after studying Excel briefly.

Mitre column applicat ⁵	Attack vectors applicabl ⁶	Mitigations applicabl ⁶	Gap analysis resu ⁶	Rationale
Initial access	Hardware and media additions	Limit Hardware Installation	Partially covered	Unknown devices and accessories are blocked by endpoint security configuration (Intune and MDATP). It is not fully covered as for instance mobile phones can be connected though.
Initial access	Valid accounts	Password Policies	Covered	Passwords policy states that passwords shall be updated periodically.
Initial access	Valid accounts	Privileged Account Management	Covered	Domain and local accounts as well as their permission levels are routinely audited to look for situations that could allow an adversary to gain wide access by obtaining credentials of a privileged account.
Persistence	Account (creation, disposal or manipulation)	Multi-factor Authentication	Covered	MFA is not required for each login but it is demanded at the firsts logins and periodically. Also, it is asked if some parameters change (location, for instance)
Persistence	Account (creation, disposal or manipulation)	Network Segmentation	Partially Covered	Some segmentation is in place (between tenants, for instance), but not as much as
Persistence	Account (creation, disposal or manipulation)	Privileged Account	Covered	There are not too many administrator accounts, intended to be avoided for day-to-day
Persistence	Account (creation, disposal or manipulation)	Operating System Configuration	Covered	By ensuring proper security configuration for critical servers to limit access by potentially unnecessary protocols and services, such as SMB file sharing, domain controllers are protected.
Persistence	External remote services	Disable or Remove Feature of Program	Partially covered	Disable or block remotely available services that may be unnecessary.
Persistence	External remote services	Multi-factor Authentication	Covered	MFA is not required for each login but it is demanded at the firsts logins and
Persistence	External remote services	Network Segmentation	Partially Covered	Some segmentation is in place (between tenants, for instance), but not as much as
Privilege escalation	Domain Policy Modification	User account management	Covered	User access is controled and managed according to policies, and recertified periodically to ensure its validity. Passwords must also be periodically changed.
Privilege escalation	Domain Policy Modification	Audit	Covered	User access is controled and managed according to policies, and recertified periodically to ensure its validity. Passwords must also be periodically changed.
Privilege escalation	Domain Policy Modification	Privileged Account Management	Covered	Tools in use are correctly managed to ensure privileged accounts (Safeguard, PIM, TACACS...)
Privilege escalation	Valid accounts	Password Policies	Covered	Passwords policy states that passwords shall be updated periodically.
Privilege escalation	Valid accounts	Privileged Account Management	Covered	Domain and local accounts as well as their permission levels are routinely audited to look for situations that could allow an adversary to gain wide access by obtaining credentials of a privileged account.
Defense Evasion	Domain Policy Modification	User account management	Covered	User access is controled and managed according to policies, and recertified periodically to ensure its validity. Passwords must also be periodically changed.
Defense Evasion	Domain Policy Modification	Audit	Covered	User access is controled and managed according to policies, and recertified periodically to ensure its validity. Passwords must also be periodically changed.
Defense Evasion	Domain Policy Modification	Privileged Account Management	Covered	Tools in use are correctly managed to ensure privileged accounts (Safeguard, PIM, TACACS...)
Defense Evasion	Impair defenses	User account management	Covered	User access is controled and managed according to policies, and recertified periodically to ensure its validity. Passwords must also be periodically changed.
Credential Access	N/A	N/A	N/A	N/A
Discovery	Network Service and Share Scanning	Multi-factor Authentication	Covered	MFA is not required each time to browse but it is periodically asked in order to access the account that allows browsing (both Citrix and NGW/P)
Lateral Movement	Replication Through Removable Media	Disable or Remove Feature of Program	Covered	Unknown devices and accessories are blocked by endpoint security configuration (Intune and MDATP). It is not fully covered as for instance mobile phones can be connected though. Disable or block remotely available services that may be unnecessary.
Lateral Movement	Replication Through Removable Media	Limit Hardware Installation	Partially Covered	Unknown devices and accessories are blocked by endpoint security configuration (Intune and MDATP). It is not fully covered as for instance mobile phones can be connected though.
Lateral Movement	Replication Through Removable Media	Behavior Prevention on Endpoint	Covered	Endpoint is equipped with Microsoft Defender for Endpoint, which automatically detects and remediates advanced attacks on your endpoints using behavioural analysis (It also performs security

Figure 12. USB IaA threat analysis

As can be seen in the figure, we can see the different columns that we discussed in chapter 4, especially column 4 and 5 where we have the view of which mitigations are sufficient and which are not sufficient to cover the attack. In the rationale we can see the technologies used as security capabilities, for example when we want to prevent an attacker, once inside the system, in the “Persistence”⁵ phase from accessing other applications or services externally, a multi-factor authentication⁶ is implemented to give a double layer of security to the simultaneous access to other parts of the system. And that in each of the rows, resulting in this tab from which we will extract the high-level data to be able to formulate the slides as a report, which we will see below.

⁵ Explained in chapter 2

⁶ Explained in chapter 3.5

Introduction: Data Leakage

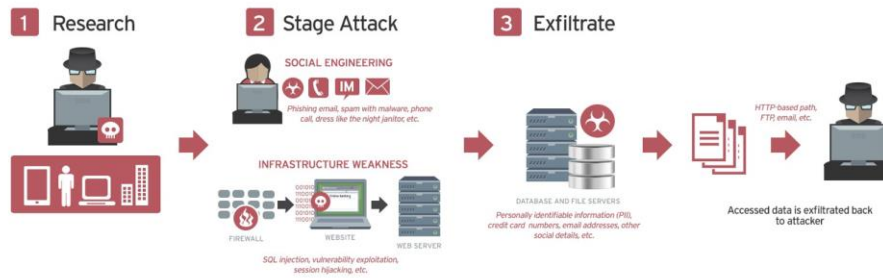


What is Data Leakage?

Data leakage describes a **data loss** of sensitive information that results in unauthorized personnel access to valuable data assets. The sensitive data can be company information, financial details or other forms of data that puts the company name or its financial situation at risk.



How does it work?



The majority of data breaches are rooted in three main areas:

1. Malicious attacks, which involve cybercriminals or insiders
2. Human error, such as careless employees or contractors
3. Systems glitches, including business process failures

Common cyberattacks used in data breaches include the following: **Spyware**, **Phishing** and **Broken or misconfigured access controls**.

Figure 13. Data Leakage introduction slide

First, we have introductory slides explaining the threat and its scope, then we have a slide with the latest news on the threat and then we have the 3 summary/report slides of the analysis.

Data Leakage as a current threat

The image shows a collage of news headlines from BBC News:

- Hack Brief: An Adult Cam Site Exposed 10.88 Billion Records**
CAM4 has taken the server offline, but not before it leaked 7TB of user data.
- Yahoo 2013 data breach hit 'all three billion accounts'**
© 3 October 2017
- Twitch confirms massive data breach**
By Joe Tidy & David Molloy
BBC News
© 6 October
- Robinhood trading app hit by data breach affecting seven million**
© 9 November

Figure 14. Data Leakage latest news slide

MITRE Matrix Data Leakage - Applicable Attack Vectors

Initial access	Persistence	Privilege escalation	Defense evasion	Credential Access	Discovery	Lateral movement	Collection	Command and control	Exfiltration
Exploit Public-Facing Application	Server Software Component	Access Token Manipulation	Access Token Manipulation	Brute Force	Network Service and Share Scanning	Remote Services (Exploitation and Hijacking)	Data from Cloud Storage Object	Application layer protocol	Data transfer size limits
External Remote Services	Accounts (creation, disposal or manipulation)	Exploitation for Privilege Escalation	Deobfuscate/Decode Files or Information	Forced Authentication	Remote System Discovery		Data from Information Repositories	Data encoding	Exfiltration over alternative protocols
Valid accounts	External remote services	Valid accounts	Files or Information	Input Capture	Cloud Discovery		Data from Local Systems	Encrypted channel	Exfiltration over physical medium
Phishing			Exploitation for Defense Evasion	Man-in-the-Middle	Network Discovery and Sniffing		Data from Network Shared Drive	Fallback channel	Exfiltration over Web Service or Cloud Account
			Domain Policy Modification	Network Sniffing	System Discovery		Email Collection	Non-standard port	
			Impair defenses	Unsecured Credentials	Password Policy Discovery		Man in the middle	Proxy	
			Indicator Removal on Host						
			Masquerading						

Figure 15. Applicable attack vectors for Data Leakage

Data Leakage – USB (I)

Initial access	Persistence	Privilege escalation	Defense evasion	Credential Access
<p>Valid accounts Access by usage of existing accounts (e.g. compromised credentials)</p> <p>Hardware and media additions Adversaries may introduce computer accessories, computers, or networking hardware into a system or network that can be used as a vector to gain access.</p>	<p>Accounts (creation or manipulation) Adversaries may manipulate accounts to maintain access to victim systems or do any action that preserves adversary access to a compromised account.</p> <p>External Remote Services Techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access.</p>	<p>Domain Policy Modification Domains provide a centralized means of managing how computer resources (ex: computers, user accounts) can act, and interact with each other, on a network.</p> <p>Valid accounts Access by usage of existing accounts (e.g. compromised credentials)</p>	<p>Domain Policy Modification Domains provide a centralized means of managing how computer resources (ex: computers, user accounts) can act, and interact with each other, on a network.</p> <p>Impair defenses To maliciously modify components of a victim environment in order to hinder or disable defensive mechanisms.</p>	
Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
<p>Network Service and Share Scanning Listing of services running on remote hosts, including those that may be vulnerable to remote software exploitation</p>	<p>Replication Through Removable Media Moving onto systems, by copying malware to removable media and taking advantage of Autorun features when the media is inserted into a system and executes.</p>	<p>Data from Local Systems Sensitive data can be collected from local system sources, such as the file system or databases of information residing on the system.</p>		<p>Exfiltration Over Physical Medium Adversaries may attempt to exfiltrate data over a USB connected physical device.</p>

Figure 16. MITRE ATT&ACK phases with covered (green) or partially covered (orange) techniques

USB Status

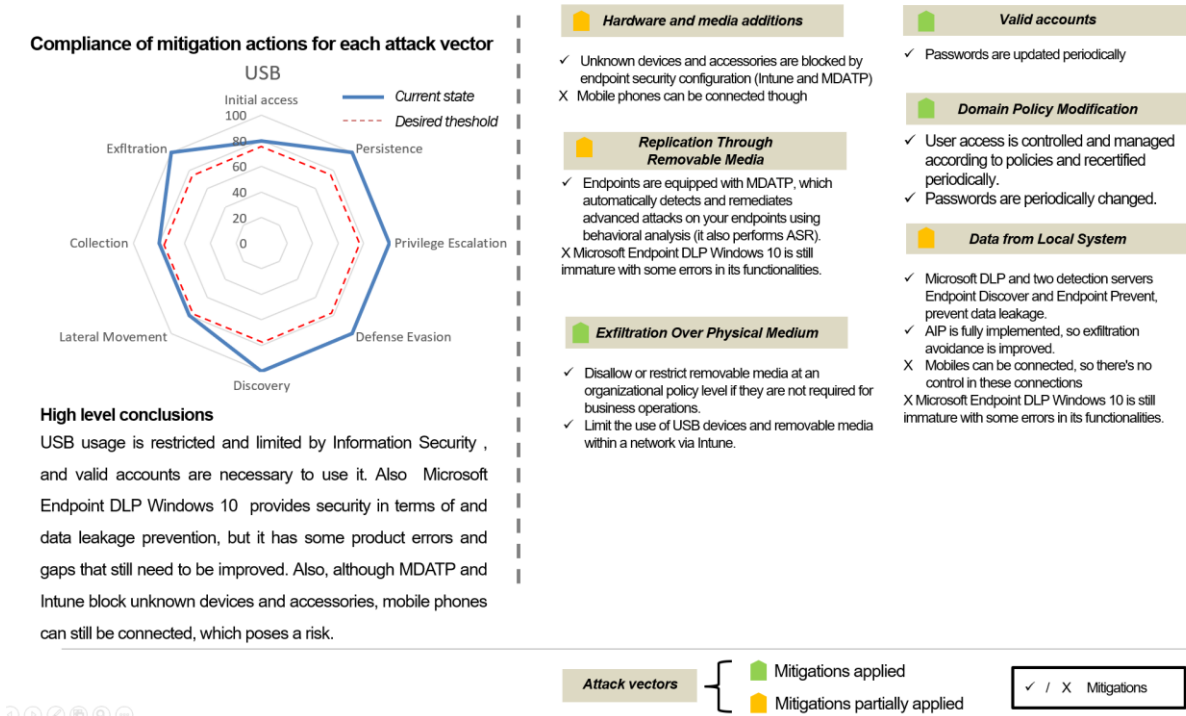


Figure 17. USB status, high-level rationale and high-level conclusions

In this last figure, a clear and concise overview of the status of the USB channel in the analysed bank can be seen in a clear and concise manner. The idea is precisely that, to be able to consult these results in an agile way so that anyone can understand it and use it as reference material. This report can streamline the scalability of the risks detected by analysts and give details of which capabilities are most vulnerable or which attack techniques are least prevented.

We can see in this case in figure 17 that the use of USB is limited or restricted, as it is one of the most dangerous channels in data leakage. Any user could access their laptop and download anything they want if these mitigating measures were not implemented.

On the other hand, we have the tool, which allows through the interaction of a user responsible for the security of the bank in question, to make use of a checklist to enter which controls apply and which do not, for all threats, one in particular or only a few specific cases that allows you to do given the flexibility of the response tool.

Threat	Entry channel	Mitre column applicab	Attack vectors applicable	Mitigations applicable	Gap analysis resu
Ransomware	Browsing	Initial access	Drive-by compromise	Application Isolation and Sandbox	
Ransomware	Browsing	Initial access	Drive-by compromise	Restrict Web-Based Content	
Ransomware	Browsing	Initial access	Drive-by compromise	Update Software	
Ransomware	Browsing	Initial access	Drive-by compromise	Exploit Protection	
Ransomware	Browsing	Execution	User Execution	Antivirus/Antimalware	
Ransomware	Browsing	Execution	User Execution	Software Configuration	
Ransomware	Browsing	Execution	User Execution	Network Intrusion Prevention	
Ransomware	Browsing	Execution	User Execution	Restrict Web-Based Content	
Ransomware	Browsing	Execution	Exploitation for Client Execution	Application Isolation and Sandbox	
Ransomware	Browsing	Execution	Exploitation for Client Execution	Exploit Protection	
Ransomware	Browsing	Persistence	Browser extensions	Execution Prevention	
Ransomware	Browsing	Persistence	Browser extensions	User training	
Ransomware	Browsing	Persistence	Browser extensions	Limit software installation	
Ransomware	Browsing	Defense Evasion	Domain Policy Modification	User account management	
Ransomware	Browsing	Defense Evasion	Domain Policy Modification	Audit	
Ransomware	Browsing	Defense Evasion	Domain Policy Modification	Privileged Account Management	
Ransomware	Browsing	Defense Evasion	Impair defenses	User account management	
Ransomware	Browsing	Defense Evasion	Masquerading	Execution Prevention	
Ransomware	Browsing	Defense Evasion	Masquerading	Code Signing	
Ransomware	Browsing	Discovery	Network Service and Share Scanning	Encrypt Sensitive Information	
Ransomware	Browsing	Discovery	Network Service and Share Scanning	Multi-factor Authentication	
Ransomware	Browsing	Lateral Movement	Remote Services (Exploitation and Hijacking)	Application Isolation and Sandbox	
Ransomware	Browsing	Lateral Movement	Remote Services (Exploitation and Hijacking)	Network Segmentation	
Ransomware	Browsing	Lateral Movement	Remote Services (Exploitation and Hijacking)	Vulnerability Scanning	
Ransomware	Browsing	Lateral Movement	Remote Services (Exploitation and Hijacking)	Multi-factor authentication	
Ransomware	Browsing	Lateral Movement	Remote Services (Exploitation and Hijacking)	Update Software	
Ransomware	Browsing	Lateral Movement	Remote Services (Exploitation and Hijacking)	Privileged Account Management	
Ransomware	Browsing	Command and Control	Proxy	Filter Network Traffic	
Ransomware	Browsing	Command and Control	Proxy	Network Intrusion Prevention	
Ransomware	Browsing	Command and Control	Proxy	SSL/TLS Inspection	
Ransomware	Browsing	Command and Control	Remote Access Software	Network Intrusion Prevention	
Ransomware	Browsing	Impact	Data (Encryption and wiping)	Data Backup	
Ransomware	Browsing	Impact	Inhibit System recovery	Data Backup	

Figure 18. Data tab inside the tool

In this figure you can see some of the more than 750 possibilities that comprise the study, which can be filtered according to the desired analysis and column 6 which is used as a checklist to enter the data on whether or not to implement it.

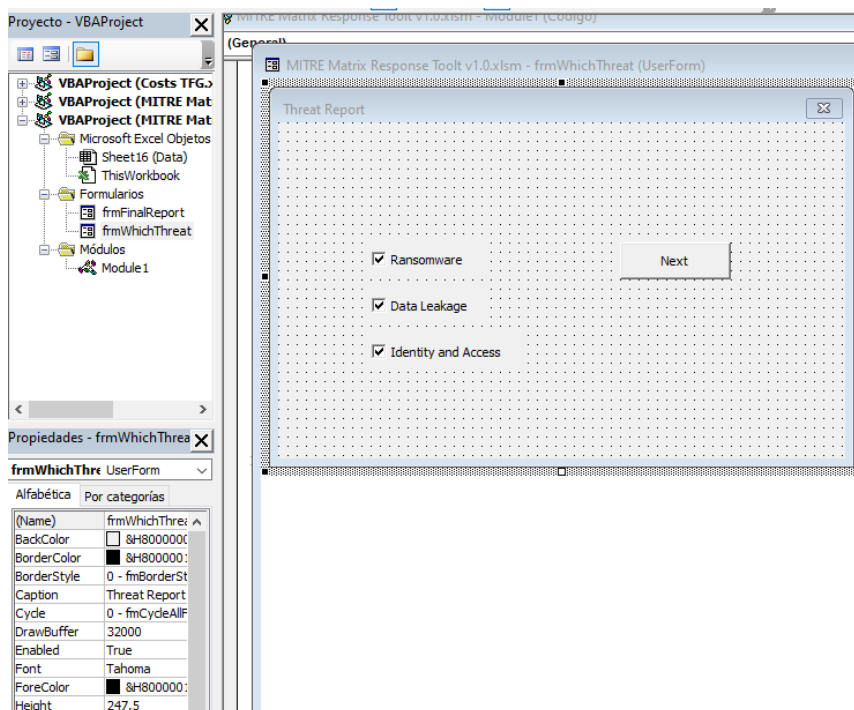


Figure 19. VBA user form module for user interaction template

Once the user enters the data and the appropriate filters, a dashboard is generated with the results seen in the PowerPoint slide in excel format to be able to visualise in detail at any time.

6. Economic analysis

The economic analysis of this project isn't complex, all of the code has been programmed during the thesis or is Open Source (Excel and LaTeX).

All of the thesis has been done on a personal computer, and the data has been stored too in the computer and the EY cloud service.

Adding up the usual materials such as paper, pens, chair and desk, with the average salary of a junior engineer from UPC and the utilities the result is a total cost of 5.940 euros.

Item	Cost per month
Computer	20,00 €
Desk	5,00 €
Chair	3,00 €
Pens	10,00 €
Paper	20,00 €
Utilities	50,00 €
Junior Engineer	1.080,00 €
Total cost	5.940,00 €

Figure 20: Cost calculation

7. Conclusions and next steps

The goal of this section is to make a review of the results and a comparison with similar projects to create some context for the thesis as well as defining the next steps that can be made to further develop a better tool and improve the study that may help a lot of clients.

7.1 Conclusions

After having carried out this exhaustive study on threat modelling and created the automated response tool, it can be seen at the end that it has been possible to fulfil the objectives set out at the beginning of this thesis. It has been possible to break down the complex approach to cybersecurity threats in detail, in an orderly and classified manner for ease of reference and ease of development of the study and the tool; thus, it can be concluded that all objectives have been successfully achieved. The mapping has been accurate, taking into account the security capabilities of the client bank, which has allowed the study to be generalised to all clients in the sector.

The three main threats studied account for millions of dollars in losses each year and cyber-attacks are becoming increasingly common, with thousands being carried out daily on all types of companies, servers and computers. The project developed in this thesis brings a fundamental value in the fight for the prevention of security in banking systems and gives a fundamental insight into how these attacks are carried out, where the most dangerous vulnerabilities are, how to mitigate and respond to all types of threats and which mitigations are the most important for each control.

With regard to the automated response tool, the objective has been achieved, through user interaction that will mark the different controls that apply in the form of a form, to generate results in the form of a dashboard to be able to see in detail the level of compliance with each of the mitigations provided by the client bank's security policies and capabilities.

Speaking more personally now, it has been a very enriching experience to do this thesis project because I have been able to learn different technologies used in the security capabilities and architectures of banking institutions, deepen my knowledge in cybersecurity, learn about the MITRE ATT&CK matrix and the great value it brings to threat modelling, understand the importance of mitigating controls for all types of vulnerabilities and finally I have been able to expand my knowledge with Excel software, get into the programming language of Macros and be able to make a tool that works properly with a certain degree of complexity. In addition, I have been able to do it together with an excellent work team in which, despite being an internship student, my work has always been valued and they have always trusted me to improve it. For me, it is a priceless fact that they have encouraged me to continue, and it is very gratifying to be able to say this about a place of work.

7.2 Next steps

In addition to continuing to work on and expand the project for more threats, the aim is to improve the automated response tool programmed to have more functionalities such as generating an automatic report in pdf format to be able to present it directly to the corporate level, which can automatically send emails to those responsible for security in the entity when risks are detected, and which could even be used in real time, perhaps using other programming languages and unifying the experience in a more complex and complete tool. The aim is to unify the study with a dynamic environment that allows the information to be constantly expanded and to incorporate more and more security policies, new parameters and new data.

References

- [1] The Rise of Ransomware CISCO
<https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/ransomware-defense/rise-of-ransomware.pdf>
- [2] Information Security. <https://ayudaleyprotecciondatos.es/2020/07/14/seguridad-de-la-informacion/>
- [3] Integrity, confidentiality and availability <https://www.pmg-ssi.com/2021/03/que-es-la-seguridad-de-la-informacion-y-cuantos-tipos-hay/>
- [4] Retarus statistics blog <https://www.retarus.com/blog/en/alarming-cybersecurity-statistics-for-2021-and-the-future/>
- [5] Michael Sikorski and Andrew Honig. *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software*. No Starch Press, 2012
- [6] IT security and regulation in the financial sector
<https://www.redhat.com/es/topics/security/security-and-compliance-financial-services>
- [7] MITRE ATT&CK <https://attack.mitre.org>
- [8] Okta's Business at Work 2019 <https://www.okta.com/businesses-at-work/2019>
- [9] 3.3 Type of malware: Heimdal <https://heimdalsecurity.com/blog/wp-content/uploads/hs-Types-of-malware-1.png>
- [10] Attack vectors <https://www.optical.pe/blog/vectores-de-ataque-ciberseguridad/#:~:text=Los%20vectores%20de%20ataque%20en%20ciberseguridad%20son%20las%20formas%20o,propósito%20de%20obtener%20beneficios%20económicos.>
- [11] Cyber Security Kill Chain <https://www.netskope.com/es/security-defined/cyber-security-kill-chain>