PRIVACY AND SECURITY CONFERENCE 2022

PRIVACYANDSECURITYCONFERENCE.PT

Proceedings of the Digital Privacy and Security Conference 2022

19 - 20 January 2022 *Porto, Portugal*

Editors
Carla Cordeiro and Hugo Barbosa

UNIVERSIDADE LUSÓFONA DO PORTO

Copyright

Personal use of this material is permitted. However, permission to reprint or republish this material for advertising, promotional purposes, creating new collective works, resale, redistributing to servers, lists, or reuse any part of this work in other works must be obtained from the editors.

While every precaution has been taken in preparing this book, publishers and authors assume no responsibility for errors or omissions, or for damages resulting from use of the information contained herein.

1st Edition 2022

Issue EOI:10.11228/dpsc.04.01

Editors: Carla Cordeiro and Hugo Barbosa

Proceedings Design: Hugo Barbosa

Graphical Design/Website: Hugo Barbosa

E-mail: hugo.barbosa@ulp.pt

Conference Website: https://privacyandsecurityconference.pt

Conference EOI :10.11228/dpsc

DPSC2022 Proceedings EOI: http://eoi.citefactor.org/10.11228/dpsc

Universidade Lusófona do Porto
Rua Augusto Rosa, nº 24
4000-098 Porto – Portugal
Telephone: +351 222 073 230

FOREWORD

ORGANIZING AND SCIENTIFIC COMMITTEES

Digital Privacy and Security Conference 2022 Organization and Scientific Committees welcome you to the fith edition conference.

The Digital Privacy and Security Conference 2022 (DPSC2022) went back to being face-to-face despite all the limitations in complete safety and in a learning and sharing environment. In times of pandemic, we live very difficult times, but also of learning and growth as a society, together we will be able to overcome. The Organizing Committees of the DPSC2022 Conference have worked hard behind the scenes to make the 2022 edition safe and successful, considering that COVID-19 is an extraordinary global public health problem.

The main goal of a scientific event is to discuss, disseminate and create knowledge. Organizing this conference proved to be a challenging opportunity for us to achieve this goal.

Currently, we are living in a digital world, where we share all information consciously and subconsciously about our life with any one. This situation puts the people in a worrying situation. Areas such as industry, health, finance, among others are addressed at the conference taking into account the problems of each sector, also of importance and discussed throughout the presentations were the approaches to digital forensics, trust in data transactions and analysis of situations that occurred during the pandemic. Our commitment and hard work have as aims to contribute for all participants to acquire tools to better protect themselves. This area is in constant evolution and need we improved our knowledge.

The young students that devote themselves to research deserve our praise for their efforts in the search of new knowledge and better intellectual and technical skills. For some of these young people, it is the beginning of a work that intends to promote research and a better understanding of the investigated areas. Persistence and strong motivation constitute the driving force which stimulates students of Security and Audit class the Informatics Engineering degree from the Lusofona University of Porto (ULP), to the creation of scientific papers related to this field of study, to the promotion of research, and to the knowledgeable discussion and practical demonstration on a variety of issues addressed, particularly in the context of computer science, computer networks and computer forensics. The grouping of this information,which takes the shape of a book, is the natural result of these principles put into practice.

We would like to thank all those authors whose participation in this endeavor contributed to its success, hoping it will promote a better understanding of the issues that were addressed. A special thanks to all the members of the scientific committee who, with their contribution, allowed to raise the level of the conference.

Thanks to all the sponsors who made the conference possible, as well as all those who contributed to the success of DPSC2022.

Porto, January 2022

Carla Cordeiro and Hugo Barbosa

Conference Committees

ORGANIZING COMMITTEE

Carla Moreira Cordeiro – Universidade Lusófona do Porto, Portugal
Lusofona University, Portugal

Hugo Azevedo Barbosa – Universidade Lusófona do Porto, Portugal
Lusofona University, Portugal

SCIENTIFIC COMMITTEES

Hugo Azevedo Barbosa - Chair
(Lusofona University, Portugal)

José de Vasconcelos
(Lusofona University, Portugal)

Óscar Ferreira Ribeiro
(Lusofona University, Portugal)

José Lobinho Gomes
(Lusofona University, Portugal)

João Ulisses
(University of Vigo, Spain)

Günther Pernul
(University of Regensburg, Germany)

João Paulo Magalhães
(ESTG - Polytechnic Institute of Porto, Portugal)

Kiavash Satvat
(University of Illinois at Chicago, United States)

Esma Aïmeur
(University of Montreal, Canada)

Weizhi Meng
(Technical University of Denmark, Denmark)

Nader Safa
(Coventry University, United Kingdom)

Cihangir Tezcan
(Middle East Technical University, Turkey)

Antonella Santone
(University of Molise, Italy)

Tony Thomas
(Indian Institute of Information Technology and Management, India)

Nuno Santos
(IST - University of Lisbon, Portugal)

Miguel Frade
(CIIC/ESTG - Polytechnic Institute of Leiria, Portugal)

Gaurav Sharma
(Université libre de Bruxelles, Belgium)

Cristian Raventos
(National Autonomous University of Mexico, Mexico)

Ania Cravero
(University of La Frontera, Chile)

Teresa Guarda
(State University Santa Elena Peninsula, Ecuador)

Raylin Tso
(National Chengchi University, Taiwan, Republic of China)

Galvão Meirinhos
(University of Trás-os-Montes and Alto Douro, Portugal)

Tiago Pedrosa
(Polytechnic Institute of Bragança, Portugal)

Hélder Gomes
(University of Aveiro, Portugal)

Luís Antunes
(C3P, University of Porto, Portugl)

Nick Pitropakis
(Edinburgh Napier University, United Kingdom)

Evangelos Markakis
(Technological Educational Institute of Crete, Greece)

Ramoni Adeogun
(Aalborg University, Denmark)

Carlos Serrão
(ISCTE - University Institute of Lisbon, Portugal)

Mohiuddin Ahmed
(Edith Cowan University, Australia)

Rui Zhao
(University of Nebraska Omaha, United States)

Carlos Abreu
(ESTG - Polytechnic Institute of Viana do Castelo, Portugal)

Fernando Almeida
(INESC TEC | Polytechnic Institute of Gaya, Portugal)

Ladislav Beranek
(University of South Bohemia, Czech Republic)

Yahya Slimani
(University of Manouba, Tunisia)

Support Committee

Maria Oliveira (EPCJC, Portugal)

Sandro Moreira (The Fleet Kollective, Portugal)

Sponsors

Institutional Partners

ORDEM DOS ENGENHEIROS REGIÃO NORTE

IEEE University of Porto - Student Branch

ipai IIA PORTUGAL Membro de

APDSI ASSOCIAÇÃO PARA A PROMOÇÃO E DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO

Sponsors

ELION SOLUTIONS Technology is Everything

GnE gestão e engenharia

BLIP. A Flutter company www.blip.pt

Critical software

Porto Editora

Media Partner

SECURITY MAGAZINE REVISTA DOS PROFISSIONAIS DE SEGURANÇA

ENTERPRISE SECURITY

01010 01010 01010 information an Open Access Journal by MDPI

Contents

SESSION 1
Cybersecurity and Cyberattacks: Techniques, Impacts and Consequences

SESSION 2 - The Future of Risk Management in the Digital Technologies

SESSION 1

CYBERSECURITY AND CYBERATTACKS: TECHNIQUES, IMPACTS AND CONSEQUENCES

SMS-I: an Intelligent Correlation tool for Cyber-physical Systems*

Eva Maia[1 [0000−0002−8075−531X]], Norberto Sousa[1 [0000−0003−2919−4817]], Nuno Oliveira[1 [0000−0002−5030−7751]], Sinan Wannous[1 [0000−0002−9711−4850]], and Isabel Praça[1 [0000−0002−2519−9859]]

GECAD - Research Group on Intelligent Engineering and Computing for Advanced Innovation and Development, School of Engineering of the Polytechnic of Porto (ISEP), Porto, Portugal. {egm,norbe nunal,sinai,icp}@isep.ipp.pt

Abstract. Airports, like other critical infrastructures, are an attractive target for attackers, mainly due to the catastrophic impact of these attacks on society. In addition, the cyber-physical nature of airports makes them more vulnerable to cyber-physical threats, and makes detecting and investigating security attacks more difficult. Therefore, it is important to improve cyber-physical correlations and forensics investigations at airports. This work describes the SMS-I tool that allows the improvement of these two aspects at airports. Data from heterogeneous systems, over different time frames, are received and correlated. Both physical and logical security are unified and additional security details are analysed to find attack evidence. Different Artificial Intelligence (AI) methodologies are used to process and analyse the multi-dimensional data exploring the temporal correlation between cyber and physical alerts and going beyond traditional techniques to detect unusual events, and then find evidence of attacks. SMS-I's Intelligent Dashboard supports decision makers in a deep analysis of how the breaches and the assets were explored and compromised. It assists and facilitates the security analysts using graphical dashboards and alert classification suggestions. Therefore, they can more easily identify anomalous situations that can be related to possible incident occurrences. Users can also explore information, with different levels of detail, including logical information and technical specifications.

Keywords: Cyber-physical Systems· Digital Forensics · Cyber-physical Systems Forensics· Machine Learning · Rule Mining.

1 Introduction

Airports are complex critical infrastructures composed by multiple systems that allow the transit of thousands of people every day. Their importance and criticality in today's society makes them an attractive target for attackers. Therefore,

* This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 832969. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein. For more information on the project see: http://satie-h2020.eu/.

airports face daily challenges to ensure the business continuity and the passenger's safety. Despite the fact that airports are usually well protected against individual cyber threats and in some cases protected against certain physical attacks on individual systems, a remaining major issue is the vulnerability to combined cyber-physical threats. Thus, the SATIE project aims to build a security toolkit [9] in order to protect critical air transport infrastructure against combined cyber-physical threats, by improving the cyber-physical correlations, forensics investigations and dynamic impact assessment at airports.

Cyber-physical systems (CPS) combine the physical and cyber worlds, which allows an improvement of the entire operating environment by adding different promising capabilities to these environments [10]. Therefore, CPS are being used in several domains including manufacturing processes, healthcare, transportation, and commercial and residencial smart buildings [5]. This can happen because CPS use and integrate different technologies, from software systems, networks and sensors to hardware devices such as microcontrollers and actuators. However, this combination enabling interactions between cyber and physical components, not only brings new paths of attack but also increases the attack impact, since an event caused by a cyber component can have a huge impact on physical ones or vice-versa [12]. Thus, beyond damage to cyber and physical components, a cyber-physical attack can also have major consequences that may include human deaths and injuries, infrastructure damages, loss of resources, and machine breakdowns or malfunctions. These damages can have an even greater impact on critical infrastructure such as hospitals and airports. Stuxnet worm [8], the US power grid attack [17], German steel-mill incident [3], the Ukrainian power grid incident [11], and the recent Florida Water Treatment Plant [7] and Colonial Pipeline [19] attacks, are some examples of security attacks on CPS that have caused huge impacts on the normal operation of the systems.

After an attack it is crucial to understand how the attack was performed, who did the attack and why the attack happened. This will help to understand which assets were compromised but also will allow the creation of defense mechanisms for future attacks. For that security analysts need to analyse and investigate several sources of information. In CPS, this investigation process becomes much wider and complex, due to the amount of components that need to be analysed. Not only software and hardware components need to be considered but also all interactions across all CPS. Several investigations have been done to develop tools to secure CPS as well as techniques and frameworks to evaluate CPS security, however CPS forensic investigation area is still in its early stage. Mohamed et al. [14] reviewed examples of current research efforts in the field and the types of tools and methods proposed for CPS forensics. The authors also discussed some issues and challenges in the field that need to be addressed. One of the issues pointed out was the need for data analytics tools to find correlations between digital and physical evidence.

In this work we describe the SMS-I tool which deals with the analysis of data from heterogeneous systems, over different time frames and correlates them to

find evidence of the causes of an attack, allowing the improvement of the forensics investigation at airports. It analyses additional security details, providing contextual and semantic data, to identify causes for security events and threats. Machine Learning (ML) methodologies have been applied for outlier detection, exploring the temporal correlation between cyber and physical alerts, and going beyond traditional one-class algorithms, and considering ensemble methods to detect unusual events, taking into account its sequential nature, which may help to find evidence of attacks. An intelligent dashboard is also part of the SMS-I in order to support decision makers in a deep analysis of how the breaches and the assets were explored and compromised. A first overview of this tool was presented in [13].

2 SMS-I Tool Overview

SMS-I is a forensics investigation system that is a part of the SATIE security toolkit. In the SATIE security environment, cyber and physical sensors are scattered across the whole airport's infrastructure collecting vast amounts of events related to the airport system's activity. These events are sent to the CEngine, a pattern matching mechanism that contains expert written rules which are periodically reviewed and updated under a strict protocol, to possibly identify abnormal behaviour. When a set of events trigger a specific rule, an alert is originated and sent to the incident Management Portal (IMP). In the IMP, after investigating the alert occurrence, the security operator classifies alerts as either incidents or not, triggering a security response. SMS-I tool inspects these incident and alert occurrences to provide a deeper analysis of an attack. For that, the system periodically fetches data from the CEngine and the IMP using HTTP(S) requests to obtain alerts and incidents generated by the SATIE Toolkit. This data is parsed into predefined formats and stored into specific indexes of the SMS-I Database. This is a crucial part of the SMS-I tool since it allows the system to keep track with the new data that is generated within the SATIE Environment. Then, the SMS-I ML Engine gets this new data and executes the ML models capable of determining, for each alert, the probability of it being an incident based on its own features, features of related events and the features of other alerts of a regarded time window. The employed models are expected to grow smarter over time with system usage. Additionally, using the Association Rule Mining (ARM) Engine, the SMS-I ML Engine provides an API endpoint for executing rule mining algorithms on the SMS-I Database data according to a set of parameters specified in the request header. It retrieves the list of association rules to identify probable relationships between alerts for a given timeframe. Finally, the SMS-I Intelligent Dashboard provides a Graphical User Interface of all this data that handles the interaction with the security analyst. It encapsulates Kibana dashboards and allows the operator to make use of several functionalities such as consulting alert lists, performing filtering, mining new association rules, managing association rule base and consulting alert details. An overview of the SMS-I architecture can be seen in Fig. 1.

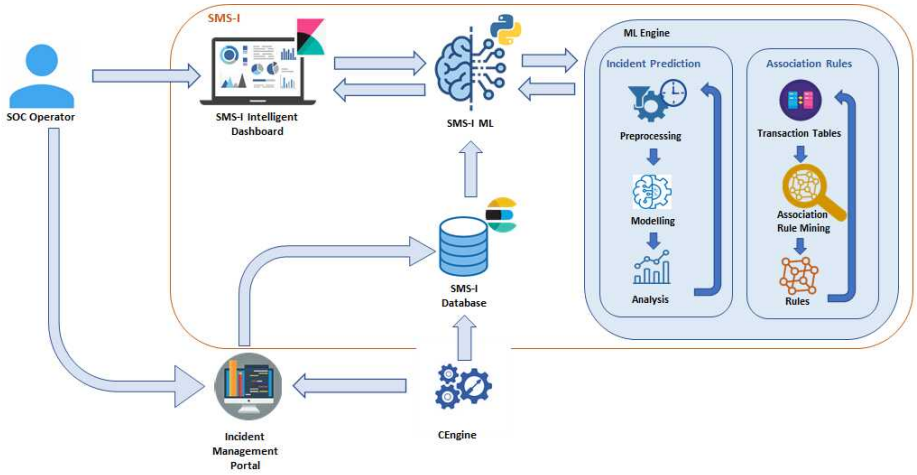


Fig. 1. SMS-I architecture overview

3 SMS-I Machine Learning Engine

The ML methods present in the SMS-I can be categorized into two groups: incident probability prediction and association rule mining. For the first, supervised algorithms were trained on the sequential data of cyber and physical alerts to predict the probability of a given alert to be an incident based on previous occurrences. On the other hand, the second group of methods uses the same data to derive new correlation rules between alerts that can be analysed to understand the complex pattern inherent to such data. Both will be described in the following sections.

3.1 Incident Probabilities

There are many approaches for building ML models that can efficiently detect anomalies in time series data. To properly investigate and explore state of the art methods for such task a study on public datasets was performed. One of the difficulties of this study was to find an appropriate testbed for testing the employed methods performance. The lack of good and reliable datasets has been appointed in the literature as one of the main obstacles in intrusion detection research [18]. However some datasets have been recently introduced to solve this issue, NSW-NB15 [15], CICIDS2017 [21] and CIDDS-001 [18]. From all the previously mentioned, CIDDS-001 was the one selected to be used for several reasons such as the number of records, the recording period duration and the considered attack types. Therefore, anomaly detection for the CIDDS-001 dataset, considering the AttackType label, was addressed using two different approaches: single-flow and multi-flow. The first regards individual flows as separate records and attempts to find differences between normal and attack related ones. The

later, considers a given window of flows performing an analysis on the entire data sequence to detect anomalies. For each approach three ML algorithms were experimented and compared: Random Forest (RF), Multi-player Perception (MLP) and Long-Short Term Memory (LSTM). The results [16] shown that considering the single-flow approach the best performing model was the RF with an F1-score of 85.04%. For the multi-flow approach, the best f1-score value, 91.66%, was obtained by the LSTM model for a window size of 70. Although the performance of the RF considerably drops with the increase in sequence length, for a window size of 10, it achieved a f1-score of 89.82%, which is relatively close to the best recorded value. From the results, it can be concluded that learning sequential relationships between flows seem to improve anomaly detection considerably. The LSTM has proven to be a very reliable model for capturing these sequential patterns, and its performance appears to get better for bigger flow sequences.

After the training using a public dataset, a SATIE dataset was used to fine tune the incident probability algorithm. The normal use of the SATIE Toolkit and the scenario simulations generated allowed the creation of the SATIE dataset. All the alerts related to incidents, 368, were labelled as malicious while the remaining ones, 9215, were marked as normal. Despite this dataset is not large in terms of data volume and has a high-class imbalance since more than 96% of records are benign, these experiments were important to understand which approaches are better for the SATIE data and how well can the algorithms distinguish between malicious alerts, which were tagged as incidents, and false positive alerts. However, these dataset characteristics made the application of deep learning approach such as MLP and LSTM unviable. Additionally, there were multiple challenges regarding data quality such as alerts related to incidents that were not manually labelled in the IMP, alerts with a lot of empty fields that were only generated to test SATIE Tools and many repeated entries due to simulations that are executed daily. To mitigate these problems, every feature with over 60% missing values were discarded as well as all the alerts related to the repeated daily executions. Furthermore, an oversampling method, Synthetic Minority Oversampling Technique was used to produce synthetic examples of incidents to minimize the class imbalance. The data, after being pre-processed, was split into two sets: 70% for training and 30% for test. Then, a RF model was used as classifier (RF-1), obtaining an accuracy of 98.08%. However, the value of F1-score, 60.94%, indicated that the model was performing poorly on the minority class, failing to classify most of the incidents. In an attempt to improve the obtained results, three time-based features were engineered for a given window of time (30 minutes), the number of alerts, the number of distinct sensors and the most common sensor. With the new features, both accuracy and F1-score of this new classifier (RF-2) improved significantly, 98.54% and 76.60% respectively. These results lead to believe that an approach which combines both individual alert features and time-based engineered features can work quite well on the SATIE data.

3.2 Association rule mining

Apriori is a very popular algorithm for data mining focusing on association rules, developed by Agrawal and Srikan in 1994 [1]. It identifies the items or patterns in a transactional dataset and then relates frequent occurrences to those patterns, generating association rules to describe them [6]. These rules are comprised of statements that describe the relationships between seemingly unrelated items inside a transaction. Let $X = \{i_1, 1_2, \ldots, i_m\}$ be the set of all items concerned in a dataset, and $T = \{t_1, t_2, \ldots, t_m\}$ be a set of transactions, where each transaction is a set of items. The association rule, noted as $X \Rightarrow Y$ indicates a certain relation between two itemsets X and Y. An association rule $X \Rightarrow Y$ is supported if the percentage of transactions that contain both itemset X and Y in T exceeds a certain threshold, called support thresholdFurthermore, the confidence for the association rule $X \Rightarrow Y$ is defined by the percentage of transactions that contain itemset Y among transactions containing itemset XThe support represents the usefulness of the discovered rule and the confidence represents certainty of the rule. Lift is a simple correlation measuring whether X and Y are independent or dependent and correlated events. If a rule has a lift of one, X and Y are independent and no rule will be generated containing either event. If a rule has a lift greater than one, X and Y are dependent and correlated positively.

To build the association rule mining for SMS-I tool, using the apriori algorithm, the sequences of alerts in a mineable database were grouped by using a certain criterion to form transactions. That criterion is a time window, and the focus will be the name of the sensor that originated the alert. In order to compile the transactional dataset, for each alert the selected window was subtracted to its "detect_date" field. From the obtained time range, all alerts that fell inside that interval were joined and a list with their sensor's name was created, performing this operation to all entries, obtaining the set of transactions. Using this set of transactions several rules are generated to be allow the user to understand the correlation of the different sensor alerts in an attack.

4 SMS-I Intelligent Dashboard

SMS-I allows the analysis of data from heterogeneous systems, over different time frames. To provide this information regarding the system's events, alerts, and incidents in a useful way, it implements a visualization tool - the SMS-I Intelligent Dashboard. It assists and facilitates the security analyst's work using graphical dashboards and alert classification suggestions, which derive from the SMS-I ML Engine previously presented. For that, two different detailed dashboards were accessible: alerts and incidents dashboards. Both were developed using Elasticsearch and Kibana technologies. Elasticsearch is responsible for the analysis, normalization, enrichment and storage of alert and incident data, as well as data provided by ML algorithms. Then, this data is the accessed by Kibana to create these two dashboards, which allows the user to search and visualize airport security related data.

The Alerts Dashboard includes all data related to airport security alerts generated by the different cyber and physical Threat Detection Systems available in the SATIE Toolkit. One of the main goals of this dashboard is to monitor the quantity, nature, and severity of alerts, considering their incident prediction probability, which is calculated by the SMS-I ML Engine. More than 70% of security analysts feel overwhelmed with the number of alerts and incidents they need to investigate for a day [2]. More than 50% of organizations receive over 10,000 alerts daily, which can lead to alert fatigue and neglect. So, to maintain SOC efficiency and reduce the impact of the investigation on the responsible personnel, it is essential to control the quantity of received alerts and incidents. Therefore, a set of graphics and metrics were added to this dashboard (see Fig. 2) to monitor the quantity of alerts received to help avoid a sudden overload of alerts by monitoring the total number of cyber and physical alerts. The severity of

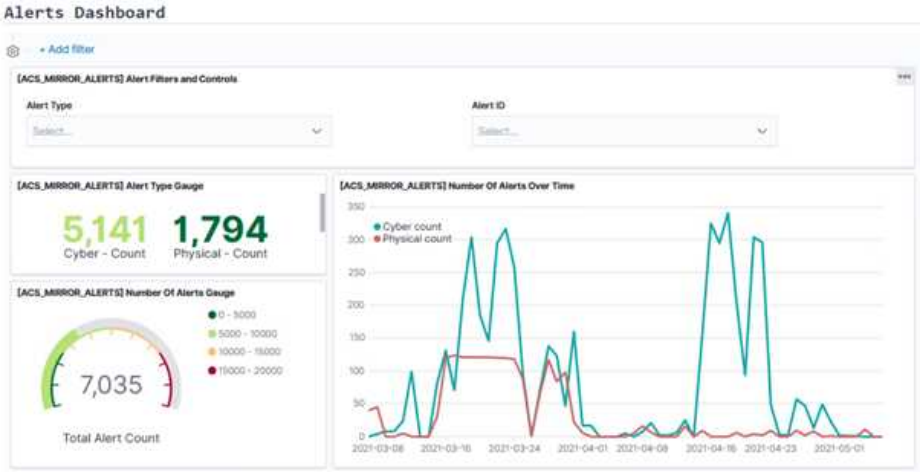


Fig. 2. SMS-I Intelligent Dashboard: Alert quantity monitoring visualizations

alerts is another important parameter that needs to be monitored by security analysts, since alert's severity defines if the alert should be ignored or if there is a need to carry out a more thorough investigation. For the SATIE project, four severity levels were defined: high, medium, low, and info. Besides controlling the number of alerts for each severity level, to avoid the overburdening of security analysts, using alerts dashboard is also possible to monitor the date of occurrence of alerts.This is useful to perform pattern and trend identification and to study previous incidents and preceding alerts. The results provided by the ML engine regarding the incident prediction probability, in other words the probability of an alert representing an incident, can also be visualized in the alerts dashboard. The most common source and target IPs and ports are also displayed to the user in the Alerts Dashboard. This information can be very valuable for the security analyst, as it helps to discover information about the attacks, namely where they come from and what the targets are.

The Incidents Dashboard aggregates all detected incidents related to airport security. This dashboard follows the structure of the Alerts Dashboard by monitoring the quantity, nature, and severity of incidents. Thus, similar to what happens with the Alerts Dashboard, it has similar visualizations available to the user, displaying information regarding incident quantity monitoring and incident severity monitoring.

SMS-I intelligent dashboard also makes available a set of different visualizations. Events timeline is one of them. It provides ability to security analysts to preview a timeline of events within the system. Events are displayed in the form of an ordered timeline, with summarized info of each event (Fig. 3). Filters can be applied to customize the timeline, such as: maximum alerts number, minimum incident probability, and time range. A Watch List section is also

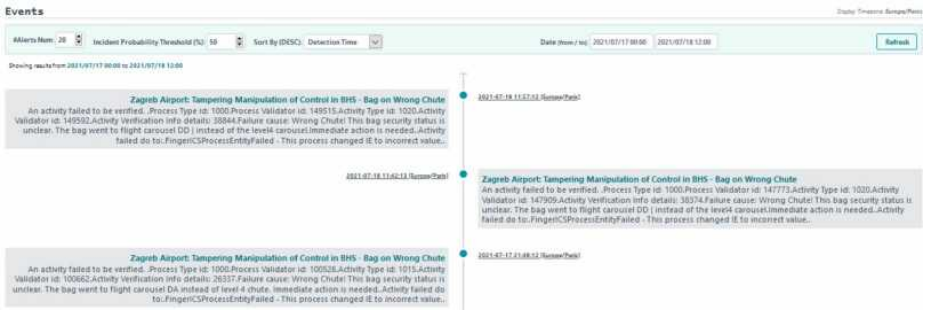


Fig. 3. SMS-I Intelligent Dashboard: Events timeline

available and allow users to preview a list of the latest alerts within the system. Alerts in this list are being displayed in the form of aligned cards, with summarized info of each alert within the corresponding card. The list can be sorted by detection time or incident probability, and filtered by maximum alerts number, minimum incident probability, and time range. Each card within the list has highlights of the alert details. Users can click on any card to display the full details of the corresponding alert (Fig. 4). Furthermore, cards are displayed using indexed colours that reflect the severity level of each alert (red for High, orange for Medium, and Green for low). When the user clicks on a specific alert Card, the corresponding alert details will be displayed. Details include the alert title and description, information identifying the alert, the source and target details, and the probability of this alert being an incident. If the card is a specific incident Card, the corresponding incident details as well as the related alerts will be displayed (Fig. 4).

Another important part of SMS-I Intelligent Dashboard is the Association Rules functionality (Fig. 5) which allows security analysts to automatically generate rules that can help them understand, using historical data, the correlation of the different sensor alerts in an attack. The security analyst can customize the parameters, namely the time window, the support and confidence, to generate different rules.

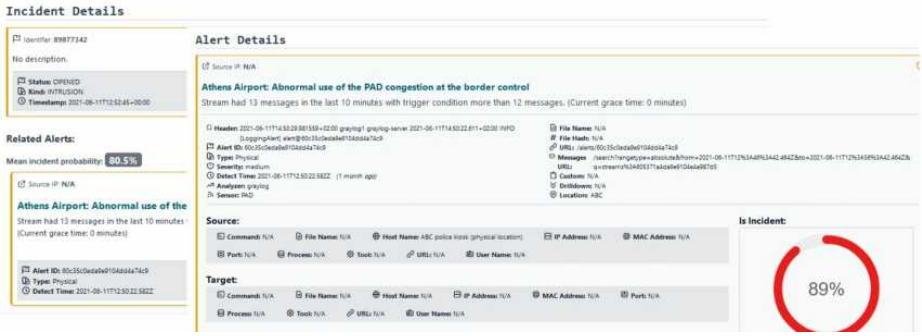


Fig. 4. SMS-I Intelligent Dashboard: Incident and Alert details example

Fig. 5. SMS-I Intelligent Dashboard: Association rules visualization

5 SMS-I Demonstration

Three different airports from three different countries are part of the SATIE project to ensure that SATIE security toolkit is scalable and adaptable to the operational needs, and compliant with the emerging regulations and standards at national and European levels. For that, the entire SATIE Solution was embedded into a validation environments. First, a simulated environment where the SATIE solution and the airport and ATC systems are fully virtualized was used. Then three demonstrations at the airport sites were made, where the SATIE solution implemented in the simulated environment was connected with the actual airport systems (as far as possible). Five different threat scenarios were defined to be performed in the validation environments. They were fine-tuned to take into account the technical performances and configurations of the actual airports' systems and operational requirements. The scenarios were also customized to be feasible on the simulation platform and in each airport environment.

During the two different validation phases, using the the simulation platform and in the pilot sites, different security analysts used SMS-I tool, through the SMS-I Intelligent Dashboard. This interaction allowed the fine tuning of the tool, gathering more data to refine the SMS-I ML engine, but it also highlighted the need to have tools, like SMS-I, that correlate the different cyber and physical security alerts. IBM stated that it took an average of 287 days to identify and contain a data breach in 2020 [20]. This detection time demonstrates how difficult is for companies to detect and mitigate cyber atacks [22]. Moreover, the analytic tasks conducted by security analysts rely heavily on a cognitive decision-making process that can differ between analysts, depending on their technical knowledge or level of experience [4]. This is why it is so important to have intelligent tools to support security analyst decisions. In one of five different threat scenarios used to perform validation of the SATIE Toolkit, an attacker seeks to perform cyber attacks on the Airport Operation Control Center (AOCC) system to manipulate the information displayed in the Flight Information Display System (FIDS) to trigger odd passenger movements to cause an ideal hostage situation, and odd plane movements on the platform to create a fatal collision. For that the attacker sends a spear-phising email to a computer with administrator privileges in the AOCC room. An AOCC employee opens the email on that computer and clicks on the link which allows the malware to be downloaded and executed. This malware allows the attacker to take remote control of the computer. Then, the attacker performs a network scan to determine the network address and port of the Airport Operation Database server – his main target. From a security analyst's perspective, it is important to correlate both events and understand that they are steps of the same attack. However, during the demonstration of this scenario the security operator reported the corresponding alerts as two different incidents (Fig. 6). Moreover, the port scanning alert was classified as a low severity incident, which should not be the case since it is already the second stage of the attack. Using the SMS-I Intelligent Dashboard, after the reporting of the incident by the security operator, the security analyst can observe that, despite this was an incident that was reported as a low severity incident, it is related with an alert that has a 69% probability of being an incident (Fig. 6), thus it should be reported with higher severity. Furthermore, using association rules, the security analyst can understand that malware alert and the network scan alert are correlated and should be reported as being part of the same incident. This is just a "real" and very simple example that illustrates the need of intelligent tools that can help security analysts in their decision-making process.

6 Conclusion

This work describes the SMS-I tool that allows the improvement of the forensics investigation at airports. It is a complex system composed by multiple components with specific functions, namely periodic data synchronization, incident probability, association rule mining, dashboard visualization and a several other functionalities involving different lists and filters. Several AI approaches were

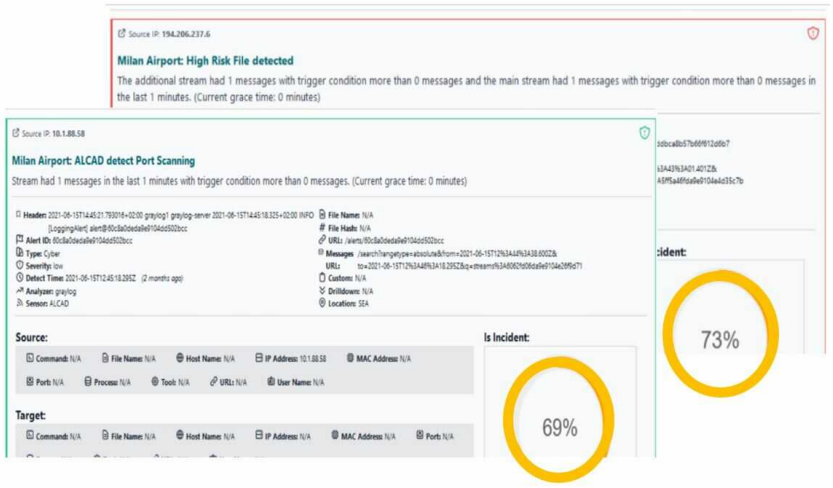


Fig. 6. SMS-I Intelligent Dashboard: Malware Detection by Malware Analyser and Network Scan detection by ALCAD system (part of SATIE toolkit)

used to process and analyse the multi-dimensional SATIE platform data exploring the temporal correlation between cyber and physical alerts. Supervised algorithms were trained on the sequential data of cyber and physical alerts to predict the probability of a given alert to be an incident based on previous occurrences. The results obtained suggest that the multi-flow approach outperforms the single-flow-based one and that the LSTM is a robust algorithm to understand complex patterns in sequential data, in particularly, network traffic data. Also, several association rules can be created applying different ML techniques, that allows the user to understand the correlation of the different data in an attack.

All the information can be visualized in the SMS-I Intelligent Dashboard. Several graphical dashboards, with different level of detail, can be used to easily identify anomalous situations that can be related to possible incident occurrences. Also, the information provided by the ML algorithms, namely the incident probability can be analysed on SMS-I intelligent dashboard. Moreover, for an additional insight about the association rules, a management of the association rules by the security analysts can also be done.

SMS-I tool was tested in three different European airports: Milano Malpensa Airport, Athens International Airport and Zagreb Airport. The tests allowed the improvement of the AI modules and the fine-tuning of the different visualizations. In this work, a very simple and authentic example demonstrated the convenience and usefulness of the SMS-I tool in the decision-making process of security analysts. As future work, we plan to test SMS-I in other airports as well as try to adapt it to other cyber-physical systems.

References

1. Agrawal, R., Srikant, R.: Fast algorithms for mining association rules in large databases. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA (1994)
2. Casey, T.: Survey: 27 percent of it professionals receive more than 1 million security alerts daily (May 2018), https://www.imperva.com/blog/27-percent-of-it-professionals-receive-more-than-1-million-security-alerts-daily/
3. Colatin, S.D.T.: Steel mill in germany (May 2014), https://cyberlaw.ccdcoe.org/wiki/Steel_mill_in_Germany_(2014)
4. Daniel, C., Gill, T., Hevner, A., Mullarkey, M.: A deep neural network approach to tracing paths in cybersecurity investigations. In: ICDMW. pp. 472–479 (2020)
5. Gunes, V., Peter, S., Givargis, T., Vahid, F.: A survey on concepts, applications, and challenges in cyber-physical systems. KSII TIIS **8**, 4242–4268 (2014)
6. Han, J., Kamber, M., Pei, J.: Data mining concepts and techniques, third edition
7. Kardon, S.: Florida water treatment plant hit with cyber attack (Feb 2021), https://www.industrialdefender.com/florida-water-treatment-plant-cyber-attack/
8. Karnouskos, S.: Stuxnet worm impact on industrial cyber-physical system security. IECON 2011 pp. 4490–4494 (2011)
9. Köpke, C., *et al.*.: Impact propagation in airport systems. In: CPS4CIP. pp. 191–206. Springer International Publishing, Cham (2021)
10. Lee, E.A.: Cyber physical systems: Design challenges. In: 2008 11th IEEE ISORC. pp. 363–369 (2008). https://doi.org/10.1109/ISORC.2008.25
11. Lee, R.M., Assante, M.J., Conway, T.: Analysis of the cyber attack on the ukrainian power grid. E-ISAC (2016)
12. Loukas, G.: Cyber-physical attacks: A growing invisible threat (2015)
13. Macedo, I., Wanous, S., Oliveira, N., Sousa, O., Praça, I.: A tool to support the investigation and visualization of cyber and/or physical incidents. In: Rocha, Á., *et al.*. (ed.) WorldCIST. Springer International Publishing (2021)
14. Mohamed, N., Al-Jaroodi, J., Jawhar, I.: Cyber–physical systems forensics: Today and tomorrow. Journal of Sensor and Actuator Networks **9**(3) (2020)
15. Moustafa, N., Slay, J.: Unsw-nb15: a comprehensive data set for network intrusion detection systems (unsw-nb15 network data set). In: 2015 MilCIS. pp. 1–6 (2015). https://doi.org/10.1109/MilCIS.2015.7348942
16. Oliveira, N., Praça, I., Maia, E., Sousa, O.: Intelligent cyber attack detection and classification for network-based intrusion detection systems. Applied Sciences **11**(4) (2021)
17. Plumer, C.: It's way too easy to cause a massive blackout in the us (Apr 2014), https://www.vox.com/2014/4/14/5604992/us-power-grid-vulnerability
18. Ring, M., Wunderlich, S., Grüdl, D., Landes, D., Hotho, A.: Flow-based benchmark data sets for intrusion detection (2017)
19. Sanger, D.E., Krauss, C., Perlroth, N.: Cyberattack forces a shutdown of a top u.s. pipeline (May 2021), https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html
20. Security, I.: Cost of a data breach report 2021 (July 2021)
21. Sharafaldin., I., Habibi Lashkari., A., Ghorbani., A.A.: Toward generating a new intrusion detection dataset and intrusion traffic characterization. In: Proceedings of the 4th ICISSP,. pp. 108–116. INSTICC, SciTePress (2018)
22. Vielberth, M., Böhm, F., Fichtinger, I., Pernul, G.: Security operations center: A systematic study and open challenges. IEEE Access **8**, 227756–227779 (2020)

Cybersecurity and Cyberattacks in Organizations: a Case Study

Ricardo Martins

Lusófona University, Porto – Portugal
ricardoolimart2001@gmail.com

Abstract. Nowadays technologies are an increasingly an indispensable factor for the daily life of an organization. Currently these are used to store the most sensitive data of an organization such as login data, banking information and personal data of employees, in addition to the storage function, these are also used to optimize tasks, increase productivity and product quality. Therefore, the increase in attacks has been having an exponential growth in recent years because of these factors mentioned above it is becoming more profitable for the attacker to carry out attacks against organizations either for their own benefit, or to sell the information obtained illicitly to competitors or in the market or even just to cause damaged. This paper presents different types of cyber-attacks that can be carried out against organizations and will be analyzed at the World panorama, in Europe and in Portugal, and later will be addressed a case of study for each of them, also reports the cybersecurity issues that should be addressed by the organizations.

Keywords: Cyberattacks, Cybersecurity, Technologies, Organizations, Threats

1 Introduction

Technologies increasingly play a more important role in companies, and for many of them, the use of technologies is essential for the proper functioning of the organization and, therefore, we have been witnessing an exponential increase in cases of cyberattacks on organizations as they stop attackers are increasingly profitable to make these attacks as technologies increasingly represent something of high importance, but many organizations devalue security issues related to technologies as somehow an investment in the security area will not bring financial return and moreover it requires a possibly high investment [1]. As organizations devalue investment in the security area, they become vulnerable to cyber-attacks and, especially, these are successful. Nowadays, intruders have several techniques and tools to carry out cyberattacks and, therefore, companies should try as much as possible to be careful, that is, they should take measures to avoid suffering attacks of this kind since the occurrence of these attacks on a company, can be devastating for the company whether for ransom or reputation issues [1]. The purpose of this document is to investigate the ways most used by hackers to carry out attacks on organizations and describe how these attacks work, it also aims to investigate the cybersecurity policies adopted by

organizations and finally it will be investigated the evolution of cyberattacks and cybersecurity at global, European and national level. In general, this paper will describe the main objectives by which cyberattacks are carried out, then the most frequent threats in the organizational environment will be mentioned, then what a security policy should contain and the importance of cybersecurity it has i nowadays, that is to say, the points that must be specified in it, afterwards and related to the security policies, some good practices that must be carried out by the organizations will be described and finally the evolution of cyberattacks and cybersecurity will be detailed in the world, in Europe and in Portugal and a case study of a real cyberattack will be presented for these three. The first chapter (introduction) outlines the topics from which this document will be implemented. The second chapter presents the description of the focal terms of this paper, such as cyberattack, cybersecurity, and politics. The third chapter introduces the objectives of executing cyberattacks, that is, the purposes of executing these crimes against organizations, since this will focus on the main methods of attacks against organizations and will include a description of the modus operandi of each of these methods. In the fourth paragraph, an effective analysis of how organizations can protect themselves from the attacks mentioned in the previous point will be carried out, in addition to this, it will also describe the best practices for drawing up a correct and objective security policy. The fifth paragraph will scrutinize the way in which cyberattacks, and cybersecurity is evolving at a global, European, and national level, then a case study will be described for each of these three, that is, a case of a cyberattack will be detailed. and the way the organization mitigated and dealt with it. In the sixth paragraph, the writing of the document will be concluded, and a detailed opinion will be presented in a succinct manner on how cyberattacks and cybersecurity have evolved in the World, European and national panorama, and the opinion will be presented in line with the points elaborated in this document.

2 Definition of cyberattack, cyber security and security policy

Cyberattacks are attacks carried out in the technological context, in other words, it is an act of modifying, destroying, exposing, stealing sensitive information and data and obtaining unauthorized access to a certain medium [2]. Cybersecurity is the measures defined by the organization to protect its technologies against cyberattacks, these include the development of policies and guidelines, analysis of risk management, awareness and training of employees and definition of the best tools and technologies to protect the organization's technology against attacks, on the other hand, protection measures are good practices aimed at all organizations and must be implemented by them to obtain a secure organizational technological environment[3].

3 Targets of cyberattacks

In short, cyberattacks have four main purposes, these being [4]:

Intrusion -The intrusion has the function compromise the integrity, confidentiality or availability of a system resource. This type of attack can irreversibly change information.

Access to confidential information - Towards of an attack, attackers may have access to certain information considered sensitive.

Loss or theft of information Following an attack, information may be erased, or information may be stolen by the attacker.

Personification- Occurs when the attacker tries to impersonate someone else.

3.1 Most frequent attacks

This section will present the main attacks by hackers against organizations and will also present the main ways to mitigate them and the main measures by which organizations should be guided to protect themselves from these attacks.

Some examples of the most frequently executed attacks are:

3.1.1 Distributed denial of service (DDoS)

DoS (Denial of Service) is an attack whose function is to interrupt a service or completely prevent the use of the system by legitimate users [5]. Regarding the attacks themselves, there are eight attacks that are used most frequently, these are [6]:

Sin Floods (SYN Flood) -This attack aims to flood the network by sending a high volume of packets (500-589 million packets per second).

WS-Discovery - It is a multicast discovery protocol and therefore it is used by IoT devices to discover the different nodes in a network.

Reflected and Amplified Attacks-These attacks have the method of sending a message to users to present the possibility of delivering a larger payload than usual.

BIT-AND-PIECE These attacks affect the telecommunications sector and the services that provide the internet and aim to overload a service.

Multi-Vector DDoS Attacks - This attack combines different types of existing DDoS attacks to cause more impact.

Some actions to mitigate these attacks are: the use of DDoS protection services, use of methods to quickly identify infections, use and cloud services and frequently carry out risk analyzes to assess security techniques, technologies and network services [6].

3.1.2 Spam

Spam is the mass sending of unsolicited messages. Spam is not itself a means of attack, it is used as a means to distribute attacks such as ransomware and trojans [7].

Some ways to avoid receiving spam emails are: implementing a method to filter content and locate existing malicious content, keep hardware, firmware and software up to date, not log in via links received by email, develop procedures to handle sensitive data, use secure email gateway and perform filters maintenance frequently, implement security techniques and finally frequently update the whitelist, reputation filters and blacklist. [8]

3.1.3 Phishing attack

Phishing is a technique used to trick people into sharing their confidential data unlawfully [9]. We can organize phishing attacks into two categories [10]:
Make the attack-To carry out an attack, several ways can be used, such as email spoofing, sending attachments, URL spoofing, website spoofing and spear phishing.
Collect the data obtained in that attack-The techniques used to collect the data obtained in the attack can be divided automatically into two groups, the collection is performed by filling out false forms by the victim, keyloggers (records and sends to the attacker the keys clicked by the victim) and manual collection which is performed through human observation (social engineering) and social network analysis.

To mitigate phishing attempts, simply educate staff to learn how to deal with phishing attempts, implement standards to reduce spam emails, verify website domains, and verify forms before filling in personal data [9].

3.1.4 Web based attacks

Services provided by the Web are subject to different types of attacks such as [11]:
SQL Injection - This attack has the function of executing queries/changes on websites in an improper way.
XML Injection Attack - This attack's main function is to change the XML logic of an application/site.
XPath Injection Attack - This attack occurs when user input data is used maliciously.

The most frequent attack in this category is SQL Injection. This is a technique used by hackers to perform improper SQL queries/changes on the database server [12].

To mitigate these attacks, developers must take into account the security of the application while developing it, as attacks often occur due to design flaws, it is also important to implement web application firewalls, use input validation methods, encrypt communication and API binding. provide correct authentication mechanisms, authorization and perform vulnerability assessments on applications. [12]

3.1.5 Malware

Malware is a general term used to describe all malicious software intended to wreak havoc on a computer system. [13]

The best-known different types of malwares are [13]:

3.1.5.1 Trojan Horse

This type of malware disguises itself in the system together with a legitimate program and so the victim installs the program thinking that he is installing something legitimate and after all he is installing something legitimate with a virus attached and once installed and given permissions can perform activities in the background.

3.1.5.2 Virus

This type of malware attaches itself to a legitimate program or system document and spreads from one computer to another via internet downloads or email attachments for example.

3.1.5.3 Worm

Worm is very similar to a virus, it only has the particularity of spreading from computer to computer without human interference, unlike the virus, it can be executed through a keylogger or through activity monitoring programs.

3.1.5.4 Ransomware

Ransomware is the most prevalent type of cyberattack currently, this type of attack has as its main objective to hijack the files and resources of the victim's machine and then ask for a ransom, in order for the latter to regain access to those resources or files. Ransomware can be differentiated into three distinct categories such as [14]:

Locker -This ransomware's main function is to block the computer's functions.
Crypto- Crypto encrypts files on the victim's device but does not interfere with computer functions. This can use three different schemes to encrypt documents, namely: symmetric encryption, where the key to encrypt documents is included in the ransomware, then we have asymmetric encryption, but this has a condition given that it is slower than the previous one and that's why it becomes a problem to encrypt large files, finally we have hybrid encryption, this uses symmetric and asymmetric encryption.
Scareware- Scareware uses pop-up ads as a means of attacking, as a way to trick users into downloading certain software.

Some actions to mitigate these attacks are: keep backups that follow the 3-2-1 rule (3 copies in two different formats and one of those copies off site), have cyber insur-

ance policy, have a security operations center in the organization, implement content filtering to filter out unwanted attachments, invest in employee training, and perform frequent antivirus tests [15].

4 Security Policies for Organizations

We have witnessed a growth in the importance of technology in organizations and therefore they must pay special attention to the care they must take and transmit to the organization's technology users. A security policy is intended to delineate and regulate the rules by which people belonging to it must obey whenever they are IT. use the systems. A good security policy must comply with certain requirements such as: information security policies, ie the way in which information must be managed according to existing laws, regulations and the business, the organization of information, in other words, the levels of access for which a certain type of information will be available, the management of human resources that is related to the organization of information and also contains the levels of access to computer systems, asset management, ie, the organization must have someone who is responsible for the computer field and this must be documented, physical security and environment, that is, it must contain the rules for the physical use of the computer components, security of operations, that is, rules must be defined on how the organization's network should be used and, finally, the management of security incidents, that is, it must be documented how to act before, during and after a cyber-attack [4].

After the security policy is elaborated, it must be ensured that some measures are complied with, such as [16]:

Assign management responsibility-Someone within the organization should have the role of ensuring that adequate resources are used.

Gaining Employee Acceptance- Communication with employees about cybersecurity issues by administrators.

Carry out cybersecurity audits -Audits should be carried out regularly by people with adequate knowledge and experience.

Data Protection- Make employees and suppliers work in accordance with the RGPD

Publish cybersecurity policies - Cybersecurity rules and policies for OS employees should be defined and published

Provide Appropriate Training - Provide cybersecurity awareness training to all employees.

Ensure effective third-party management - Ensure that all providers with access to data or sensitive parts of systems respect the agreed security levels.

Develop an incident response plan - An incident response plan must be developed, this plan must contain clear and documented guidelines, roles and responsibilities.

Protect access to systems - Encourage employees to use passwords with at least 3 random words combined in a sentence, this must be long, with upper and lower case

letters, must also have numbers and special characters and must not contain personal information. At passwords must not be reused elsewhere, cannot be shared with peers, and must use 2-factor authentication.

Secure devices - Use firewalls, ensure remote access software is up to date, ensure remote access only to verified IP addresses, restrict remote personnel access to only necessary systems, and ensure monitoring and alerts are enabled to alert you to suspicious activities. Improve physical security - Encourage users of company devices to be careful with them such as being careful where they leave them and using strong passwords.

Secure backups - Backup should be done regularly and automatically whenever possible, kept outside the organization's environment, should be encrypted especially if moved between locations, and the ability to restore data from backups should be regularly tested.

Working in the cloud - When choosing a cloud service, you must obtain information about it, such as how it complies with European Union regulations and the type of treatment used with personal data.

5 Cyberattack analysis

In this chapter, an analysis of the evolution of cyberattacks in the World, European and Portuguese panorama will be carried out. Three real cases of executions of cyberattacks against organizations will also be described.

5.1 Analysis of the World Panorama

Regarding the global scenario, cyber-attacks have experienced an exponential growth in relation to the values of previous years and a lot because of the COVID-19 pandemic, which the whole world has faced. The pandemic is indirectly related to the increase in cases of attacks, since the technological area, with the progression of the pandemic, became a very important and indispensable factor in the daily lives of organizations and, therefore, it became a profitable business for the hackers. The most performed attacks worldwide are through malware, ransomware, spear-phishing and spam emails, these attacks lead to violations of the organization's privacy, affect the company's reputation, lead to lost revenue, and generally lead to interruption of the services of the organization. company., then there is website theft, which is based on the hacker gaining administrative control of the website, which can lead to service disruption, loss of reputation, loss of customer confidence, and loss of revenue. As the pandemic came on suddenly and so organizations had to adapt very quickly and they had to make technology an indispensable factor for the proper functioning of the organization, and that is why we have been witnessing an increase in importance and increasing cybersecurity measures worldwide [17].

5.1.1 Cyberattack on Colonial Pipeline (USA)

Colonial Pipeline is a company that contains the largest pipelines in the US [18]. The type of attack used in this case was through a Ransomware, more specifically the hackers used a Trojan called DarkSide [19]. This type of Trojan is created by DarkSide and then sold to people interested in buying it, and a fee is charged either for the executed attack or a monthly fee. Darkside is a ransomware-as-service (RaaS) in other words, it is an organization in which they develop ransomware and then deliver it to cybercriminals to carry out attacks on organizations, the hackers who developed it receive an income [20]. Regarding the attack itself, this took place on May 7, 2021, the actors of the coup encrypted the data and demanded payment in cryptocurrencies, they also stole 100GB of company information to use as blackmail [21]. Regarding the modus operandi of the attack, the hackers used a password from a VPN service account that was no longer in use but still had active access, this password was made public along with a set of other passwords on the darkweb. The data breach happened on April 29 and was only discovered on May 7, when it was communicated to the company that they had been attacked, the company decided to pay the attackers approximately 3.8 million euros (US$ 4.4 millions) in cryptocurrencies right after the attack for the attackers to return the stolen data by them [21]. In terms of impact, the company lost part of the money it paid, the US government was later able to recoup a part, but in addition to this, it restricted the availability of fuel, which led to prices increasing enormously at gas stations and furthermore it caused embarrassments in the gasoline stations. This attack could have been avoided if the company in question gave more relevance to security issues, given that a policy for the use of multifactor authentication was in place [21]. Basically, multifactor authentication involves adding one more level of protection to a login, as for the login to be executed, the user who intends to do so will have to use two pieces of information found in different places [22].

5.2 Analysis of the European panorama

In relation to cyber-attacks that occurred in the European space between 2020 and 2021, these increased mainly due to the pandemic state in which we live. Between 2020 and 2021 we observe that attack through Ransomware continues to dominate the list of attacks preferred by attackers on the other hand, malware continues to decline even though in 2021 its affluence has increased compared to the year 2020, since the attack by DDoS became more "competent" and targeted in the year 2021. The pandemic forced the adoption of technology on a large scale, and so cybersecurity experts needed to adapt existing defenses to a new infrastructure paradigm being that the main objective was to minimize the organizations' exposure to cyber-attacks. In addition, specialists had to deal with the adaptation of organizations to a new modus operandi as they had to adapt and modify all their work patterns, and IT security professionals had to respond very quickly to the challenges introduced by the pandemic [23].

Between 2020-2021 cyber threats did not affect a single industry, that is, attacks were made to systems that are used by different industries, but targeted attacks were also carried out, that is, attacks aimed at harming an organization in concrete [23].

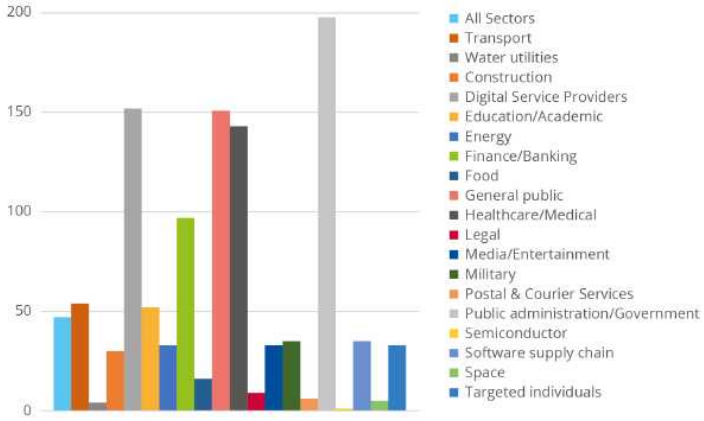


Fig. 1. Incidents by sector between 2020 and 2021 [23]

5.2.1 Cyberattack on Oloron Sainte-Marie (France)

Oloron Sainte-Marie is a hospital located in the Pyrénées-Atlantiques region and on March 8, 2021, was the target of a ransomware attack [24]. The attack carried out by the hackers encrypted the hospital's data and demanded a payment of 44120 euros (approximately 50000 dollars) in Bitcoin. The attack executed by the hackers encrypted the hospital's data and demanded a payment of 44120 euros (approximately 50000 dollars) in Bitcoin. Regarding the attack itself, the screens went blank, and a message appeared on them with a ransom demand of 12000 euros (approximately 13600 dollars), the municipality decided not to pay the ransom and a part of the data was erased from the disk [25]. This attack ended up affecting the proper functioning of the hospital because the computer system was down and, therefore, the users' data and prescriptions were no longer available and had to be executed on paper, this attack affected the medical interventions performed to the users [26]. To mitigate this attack, the hospital managers conducted an audit of the hospital's computer systems [26].

5.3 Analysis of the Portuguese panorama

Regarding the national panorama, we can say that we have been witnessing an increase in threats and conflicts in cyberspace in Portugal, in 2020 the number of cybersecurity incidents underwent a large increase compared to the values of 2019, and the exponential growth of these incidents occurred to from March 2020, which coincides with the beginning of the COVID - 19 pandemic. During the year 2020 there was an increase in phishing/smishing attempts, but there was also an increase in other forms of swindling. people being more isolated and also because of the growing need for people to use more technological means due to the pandemic. The main attack is the malware infection since the fact that people have to use more technological means

due to the fact that they are telecommuting favored the attackers to the point that they were able to take advantage of the technical vulnerabilities that arose from it. Despite the increased risks, national cyberspace managed to increase or at least managed to maintain capacity in 2021 in compared to the year 2020, but it is possible to state that in the year 2021 threats continue with an emerging trend compared to the year 2020. It is inevitable to talk about cyber-attacks without mentioning the influence that the pandemic situation had on their increase. For this increase there are two reasons being these, the social confinement, and the mandatory mass adoption of digital technologies. During the period of confinement, phishing was the most used cyber-tack by attackers. In Portugal, the main victims of cyber-attacks are SMEs (small-medium enterprises), Sovereignty Bodies, Public Administration and the sectors of Banking and Education and Science, Technology and Higher Education [27].

5.3.1 Cyberattack on Portugal Energy (EDP)

EDP Comercial is a company belonging to the EDP Group that operates in the free energy market, both nationally and internationally [28]. The type of attack used in this case was through a Ransomware, more specifically the attackers used a Trojan called by Ragnar Locker which is intended for cyber-attacks against organizations [29]. Regarding the modus operandi of this ransomware, it starts by implementing Windows XP virtual machines to encrypt the victim's files, the implementation of the virtual machine allows attackers to prevent the Trojan from being detected by security mechanisms, after closing the barriers of the company's security and device management services, then it warns the company that it was attacked and publishes evidence of the attack on the dark web to show the company in question that it has very important documents belonging to it, and then the attackers present it to the injured a ransom value in Bitcoin and a deadline [30]. Regarding the attack itself, this one took place on April 13, 2020. This attack encrypted part of the company's servers and in addition apparently, 10TB of sensitive company data was stolen. The attackers exposed evidence on dark web that they had sensitive company data and gave it 20 days to proceed with the payment of 1580 bitcoins (approximately 10 million euros at the time), if the company did not make the payment, they threatened to return public documents and deliver the information to the competition. EDP did not pay the attackers the 1580 bitcoins and therefore, and surprisingly, they eliminated the decryption keys from the company's servers and computers, that is, the attackers in doing this gave up trying to profit from the attack since made it impossible to recover the assets affected by the attack. In terms of impact, the company lost much of its reputation as it lost sensitive data, which contained government information, customer data, investor data, among others and in addition there is still a risk that hackers have sensitive information in their hands and may still try to take advantage of them. In addition to the aforementioned impacts, the company still had to replace the hacked servers. Regarding security issues, an investment of 50 million euros was made in computer security, to make mitigations, "maximum permissible downtimes for applications" were implemented, redundant disaster recovery systems, creation of a team to monitor the

security of the company, cyber-attack insurance, and employee training in security principles [29].

6 Conclusion

To conclude, throughout this paper the main attacks carried out against organizations were described, a set of measures by which companies can be guided to mitigate the occurrence of cyber-attacks was also presented, and a global, European, and national analysis of the evolution was presented. of cyber-attacks and finally three case studies of cyber-attacks were presented. Regarding the analyzes presented, we can observe that these all focus on a factor called COVID-19, in the three scenarios presented, the pandemic factor led to an exponential growth of attacks and therefore it is noticeable that organizations did not give much relevance to more technologies. specifically in the area of cybersecurity, mainly in the training of its employees, which only happened when they had to perform more functions virtually, if they had been trained before in the technological areas, the number of incidents would probably be lower, on the other hand we can say that attacks orchestrated by hackers are evolving and so it will become increasingly difficult to defend against them as there are several ways to exploit system vulnerabilities and also, for a hacker, just find a small vulnerability to be able to breach the system while, on the other hand, the team that takes care of the organization's computer field has to look for and fix several vulnerabilities that may exist, so the attacker's job will always be easier than the work of the defense. Organizations will always be able to try their best to prevent the occurrence of attacks, for that they have to create a good security policy and encourage technology users to follow them. In short, organizations should invest in cybersecurity investment since, increasingly, the most important and confidential information is stored in digital format and therefore care must be increased since the occurrence of a cyberattack can completely ruin an organization either in monetary terms or in matters of customer trust.

7 References

1. Astani, M., Ready, K.J.: Trends and Preventive Stratregies For Mitigating Cybersecurity Breaches in Organizations. Issues in Information Systems.Volume 17, Issue II. pp. 208-214 (2016)
2. Iakovakis, G., Xarhoulacos, C.G., Giovas, K., Gritzalis, D.: Analysis and Classification of Mitigation Tools against Cyberattacks in COVID-19 Era. Hindawi. Volume 2021, 1-21 (2021)
3. G. Cains, M., Flora, L., Taber, D., King, Z., S. Henshel, D.: Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation. Wiley Online Library. Risk Analysis, 1-27 (2021)
4. Oliveira, V, dos Santos, V.D.: Cibersegurança e Inteligência Artificial: Como garantir a segurança de um Sistema de Informação. NOVA Information Management School – Instituto Superior de Estatísitca e Gestão de Informação, 1-91 (2021)

5. Ivaki, N.: A comprehensive taxonomy of DDOS attacks and defense mechanism applying in a smart classification. WSEAS Transactions on Computers. 1-11, (2008)
6. ENISA, "Distributed deniel of service- ENISA Threat Landscape" (2020)
7. Spinello, R.A.: Ethical reflections on the problem of spam. Ethics and Information Technology. 1. 185-191 (1999)
8. ENISA, "Spam – ENISA Threat Landscape", (2020)
9. ENISA, "Phishing – ENISA Threat Landscape", (2020)
10. Basit, A., Zafar, M., Liu, X., Javed, A.R., Jalil, Z., Kifayat, K.: A comprehensive survey of Al- enabled phishing attacks detection techniques. Telecommunication Systems (2021) 76, 139-154 (2020)
11. Mouli, V., Jevitha, KP.: Web Services Attacks and Security – A Systematic Literature Review. Procedia Computer Science. 93. 870-877 (2016)
12. ENISA, "Web-based attacks", (2020)
13. Mat, S.R.T., Razak, M.F.A., Kahar, M.N.M., Arif, J.M., Mohamad, S., Firdaus, A.: Towards a systematic description of the field using bibliometric analysis: malware evolution. Scientometrics (2021) 126, 2013-2055 (2021)
14. Beaman C., Barkworth A., Akande, T.D, Hakak, S., Khan, M.K.: "Ransomware: Recent advances, analysis, challenges and future research directions. Computers & Security, Volume 111, pp. 1-22 (2021)
15. ENISA, "Ransomware – ENISA Threat Landscape" (2020)
16. ENISA, "Cybersecurity guide for SMEs – 12 steps to securing your business", (2021)
17. Okereafor K,. Adelaiye O.: Randomized Cyber Attack Simulation Model : A Cybersecurity Mitigation Proposal for Post COVID-19 Digital Era. IJRERD. Volume 05 – Issue 07, pp. 61-72 (2020)
18. Colonial Pipeline, https://sr2448.colonialresponse.com, last accessed 2021/10/20
19. Kaspersly, https://www.kaspersky.com/blog/pipeline-ransomware-mitigation/39907, last accessed 2021/10/20
20. CISA, https://us-cert.cisa.gov/ncas/alerts/aa21-131a, last accessed 2021/10/20
21. Bloomberg, https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password, last accessed 2021/10/20
22. Microsoft, https://www.microsoft.com/pt-pt/security/business/identity-access-management/mfa-multi-factor-authentication, last accessed 2021/10/21
23. ENISA, "Enisa Threat Landscape 2021" (2021)
24. LaChaîneTV7, https://www.sudouest.fr/pyrenees-atlantiques/oloron-sainte-marie/bearn-l-hopital-d-oloron-sainte-marie-victime-d-une-cyberattaque-1558161.php, last accessed 2021/11/02
25. TECHVAIR https://www.techvair.com/2021/09/oloron-sainte-marie-sanitation-service.html, last accessed 2021/11/15
26. Insider Paper, https://insiderpaper.com/frances-oloron-sainte-marie-hospital-cyberattack/ last accessed 2021/11/02
27. CNCS, "O relatório em 15 minutos – Cibersegurança em Portugal" (2021)
28. EDP, https://www.edp.pt/quem-somos/, last accessed 2021/11/10
29. Expresso, https://expresso.pt/economia/2020-04-18-EDP-imune-a-crise-mas-nao-aos-hackers, last accessed 2021/11/11
30. National Cyber Security Center Hungary, https://nki.gov.hu/en/it-biztonsag/hirek/virtualis-geppel-tamad-a-ragnar-ransomware/, last accessed 2021/11/15

A Comparative Study of Different Data Encryption and Decryption Techniques

Sérgio Oliveira [21907522]

[1] Lusofona University of Porto,Portugal
a21907522@mso365.ulp.pt

Abstract. We all know the online world is getting more and more powerful and we all connected to it, in a way or another. The interconnection of computer networks is increasing and with it, the cyber-attacks are getting more and more sophisticated. With that being said, we need to find a way to keep the data safe and Cryptography is one of the ways. What Cryptography does is find a way to keep the confidentiality, integrity, authentication, and we can maintain the identification of the data user all secure and sealed, and the only people to have authorization are the user or an associate. Symmetric keys and public keys are well known in the Cryptography world. Symmetric key cryptography is a technique which secures an immense capacity of confidentiality and data security, using a communication channel with a common key to encrypt and decrypt. I tis also important to mention the Fundamentals of Cryptography and its algorithms and concepts. In this project I will focus on symmetric data encryption methods that are Data Encryption Standard (DES), Triple Data Encryption Algorithm (TDEA), Advanced Encryption Standard (AES) and adding up I will mention blowfish and twofish tactic. On the side of asymmetric data encryption, I will mention about RSA(Rivest-Shamir-Adleman) and TEA (Tiny Encryption Algorithm).

I will talk about their ability to secure data and efficiency to encrypt as well.

Keywords: Cryptography, DES, TDEA, AES, RSA, Symmetric key, Encrypt, Decrypt, Data, Blowfish

1 Introduction

Over the years, computer network and internet are more and more involved in our modern society. Online banking services, payment of bills, exponential growing of some applications on the network need a safe environment that guarantees privacy and confidentiality.

We can't leave these transactions and growing applications without security and control because it makes them vulnerable to violations, so, when we are dealing with transactions and applications that are carried throughout the public sector or wireless networks, we need to secure the network management and monitor the process to prevent any violations, so we need to make sure that we guarantee data authentication, integrity, privacy and integrity of data.

This makes us able to guarantee precision and consistency throughout the information lifecycle and it's critical to any system that stores, processes, or retrieves data. This is very important to confirm someone as authentic, that is, claiming the veracity of something or someone.

The act of transferring data through the internet is that there are many security aspects that we need to be aware of, from secure commerce and online payments to private communications and password protection. So that's when we include cryptography to make all this safe and secure. We use cryptography when we need to secure privacy during several online transfers as well as data [1].

Cryptography uses an algorithm that helps us prevent and secure the information against violations. This algorithm can classify into a symmetric key, which is also called a private key, and an asymmetric key, also called a public key [2]. This are used to prevent or delay unauthorized access so sensitive information with the purpose of secure and hiding information. When you use the same cryptography keys to encrypt and decrypt a message it's called symmetric key but when you use a different key to encrypt and decrypt a message it's called asymmetric key.

Today we need to connect cryptography to the open networks, where it will be used to keep the information confidential, because of the information transfer that goes on between people or organization [3].

2 Fundamentals of Cryptography

Cryptography is a fundamental information security system that as several important uses that guarantees confidentiality and integrity of the information or data. Actuality is a technique that aims to the point that every message sent is current, which is that it doesn't allow intruders to repeat old messages over and over, which also prevents the overflow of the system.

Cryptography also aims for the authentication that the sender and the receiver must have an account authenticated, integrity of data that the message sent and received is the same (not modified), confidentiality which is that the message cannot be read or understood by unauthorized people and neither the sender nor the receiver can deny that the information was sent by them.

2.1 Redundancy

Redundancy is usually referred as a technique aimed at preventing an intruder from trying to send data that could usually be considered valid by the recipient in a transmission.

We can ask ourselves: "Is redundancy a bad thing?". The answer is: "no", it isn't. Although not the most linguistically correct way, redundance somehow tries to force the user to focus on a certain idea, word or somewhat information.

An example of redundancy is the use of the word new, for example “new innovation”, we are reenforcing the idea of an innovation when an innovation is already something new [4].

The graph below shows an experiment made by Vox that consists in rewriting old articles and turning them in new posts [5].

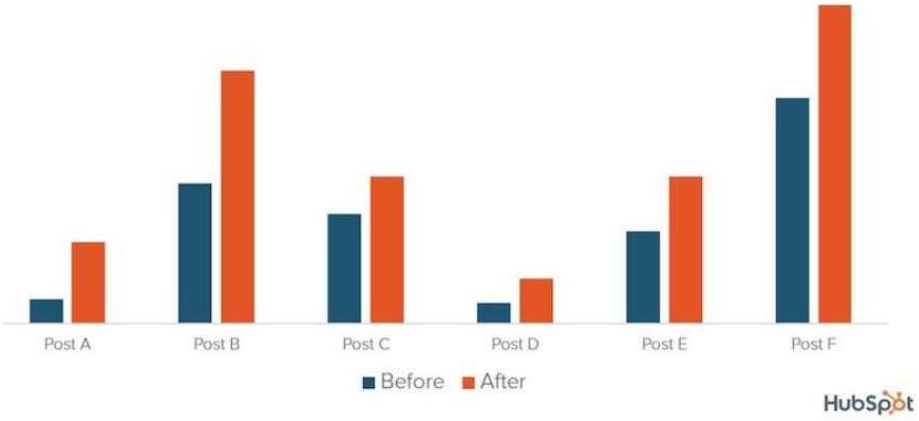


Fig.1- Monthly views from organic search before and after the update in 2015 made by Vox.

3 Cryptography Techniques

The most general security system in the online world is cryptography that secures and prevents unauthorized accesses.

3.1 What is the meaning of Cryptography?

The importance of not revealing secrets to the “outside world” started to intrigue people to develop a way to share messages that, only the person that sent and the person that received, be able to read its content.

Cryptography is also referred as secret writing. We use this term when we mean the transformation of messages using the mechanism of symmetric and asymmetric keys.

3.1.2 Symmetric and asymmetric keys

Symmetric keys and asymmetric keys serve the same purpose but in different ways. Starting with symmetric keys, they use the same key to encrypt and decrypt a message, making this a more secure and fast way. In the other hand, asymmetric keys use a

different key to encrypt and decrypt a message. In this case, as there are two different keys, the one used to encrypt is a public key and to decrypt. Another difference between this to encryption methods are that asymmetric algorithms are much slower than symmetric ones and it's not very effective to use them unless we have a big amount of data. As they are sometimes used together some experts call it hybrid encryption [6].

4 Cypher concept

When we talk about cryptography, a word that we hear a lot is cypher, but what is cypher? Cypher is an algorithm that is used to encrypt and decrypt messages to create a secret writing. There are different types of cyphers but what is common between most of them, is their ability to numbers or symbols for letters which is needed a key to decipher.

4.1 Plaintext

Plaintext is the input of a message, that is, the way that when you read a message it makes sense. This algorithm makes plaintext being transformed in ciphertext. The process is algo called encrypt and decrypt.

4.2 Ciphertext

Ciphertext is the transformation of the plaintext, which is, the transformation of the original message into an encrypted message. Ciphertext can't be read until it's converted back into plaintext, or in other words, being decrypted.

4.3 Substitution Cypher

The substitution cypher is a pre-defined system that are deciphered by inverse substitution. There are some types of cypher substitution such as:

- Simple substitution- Each letter is filtered one by one.
- Polygraphy replacement- Filtering is made from a group of letters.
- Monoalphabetic- Uses a single fixed substitution in the entire message.
- Polyalphabetic- Uses more than

Example of plaintext being transformed into ciphertext through substitution cypher:

Plaintext: GRAY FOX HAS ARRIVED
Ciphertext: UKQN YGB IQL QKKOCT

4.4 Transposition Cipher

Transposition Cipher proceeds to change the letter of the text to be ciphered to another letter. An example of this is columnar transposition where each character is written horizontally with specified alphabet width.

The following image shows an example of a transposition cipher where the message is written out in rows of a pre-defined length. The example is the word HACK (length 4).

The alphabetical order in this case will be "3 1 2 4" and in the end the message is read off in columns.

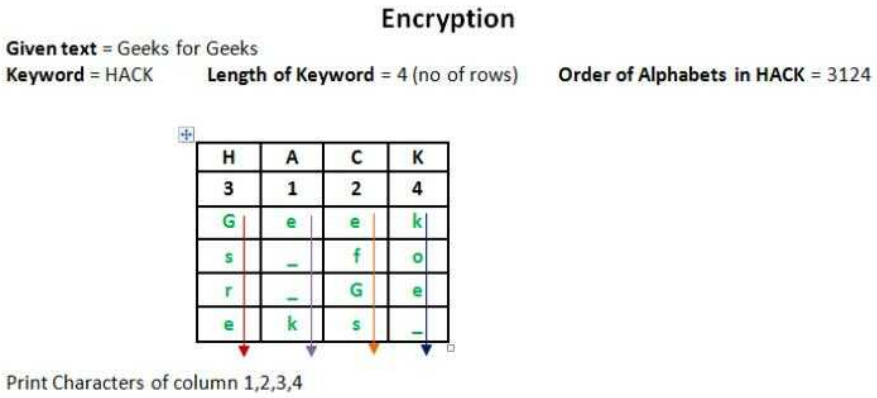


Fig.3- Example of encryption of the word "HACK" through transposition cipher

The final text after encryption will be: "e kefGsrekoe_"

4.5 Caesar's Cipher

Is one of the most used ciphers but is simple as well. It consists in choose a letter of the common alphabet and replace that same letter by its corresponding three places ahead, and that's it [7].

For example, the letter R is replaced by the letter Q, the letter D is A is replaced by the letter D, etc.

6

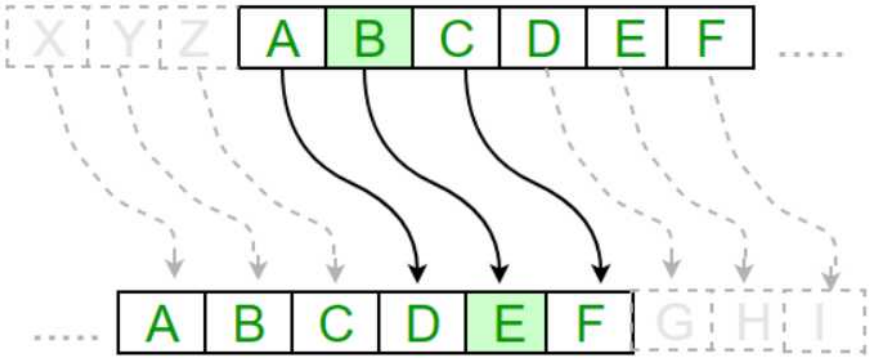


Fig.2- Example of Caesar's Cipher with a shift of three.

Although it's predefined as a shift of three it can also shift an integer between 0 to 25.

4.6 Vigenère Cipher

This cipher is based on Caesar's Cipher because it's based on the letters of the regular alphabet just as Caesar's Cipher. This works as the following explanation: If the number of characters in the key is lower than the number of characters of the message, the key will be repeated until both have the same number of characters.

Example:

Plaintext: attackatdawn
Keyword: LEMON ➔LEMONLEMONLE (after the length is equal)
Ciphertext: LXFOPVEFRNHR

4.7 The Vermam Cipher

The Vermam Cipher uses the Boolean system "XOR" (represented by "⊕") to cypher and decipher, and it's much stronger when used in numbers.

A	B	A ⊕ B
1	0	0
0	1	1
1	0	1
1	1	0

Fig.4- Table referring to the Vermam Cipher

Example of Vermam Cipher:

Plaintext: Hi! 1001000 1101001 0100001
Key: 0l;@ XOR 0110000 1101100 0111011 1000000
Ciphertext: 1111000 0000101 0011010 1000000

Only the symmetric key can decrypt the example.

5 Encryption Algorithms

5.1 Data Encryption Standard (DES)

Data Encryption Standard is an Algorithm that encrypts and decrypts data in 64-bit blocks using a key of 56 bit. Data encryption standard uses plaintext and ciphertext with both using inputs and outputs of 64-bit blocks, always operating in equal size.

.

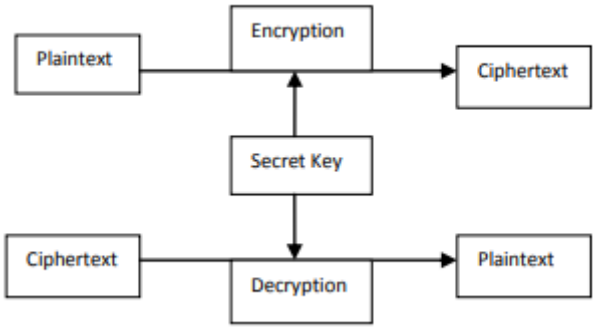


Fig.5- DES Encryption Process [8].

5.2 Triple Data Encryption Standard (TDES)

Triple Data Encryption Standard is a successor of Data Encryption Standard. It's also a symmetric encryption which applies the same algorithm as Data Encryption Standard but doing it three times each data block. This method is using to encrypt passwords and pins.

8

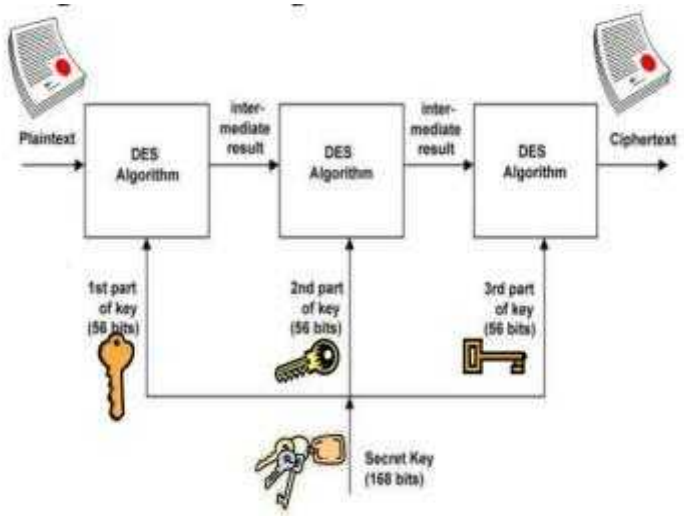


Fig.6- 3DES Encryption Process Block Diagram [9].

5.3 Advanced Encryption Standard (AES)

This is an algorithm that uses a 128-bit form, a 192-bit form and a 256bit-form for the most challenging encryption purposes.
This algorithm is known for his ability to block every attack except the attacks using brute force.

5.4 Blowfish

Blowfish is also an algorithm made to replace DES. This tool can break the message that is being sent into 64-bit blocks and encrypts each of them individually. It's used most for secure passwords and payments duo his speed and flexibility.

5.5 Twofish

Twofish is blowfish's successor that deciphers 128-bit data blocks and encrypts it in 16 rounds not depending on key size. It's known for his speed in software and hardware environments.

5.6 Rivest-Shamir-Adleman (RSA)

This is a slow asymmetric encryption algorithm that factorizes the product of two large prime numbers and the only way to decode the message in a successful way is having the knowledge of these two numbers.

5.7 Tiny Encryption Algorithm (TEA)

This is a simple, safe and effective algorithm that works using a 64-bit block that divides in two 32bit-blocks and uses a 128 bit-block key that divides itself in four smaller 32bits-key that is used in each one of four sub cycles [10].

```
void code(long* v, long* k)  {
      unsigned long y=v[0],z=v[1], sum=0,     /* set up */
                  delta=0x9e3779b9,   /* a key schedule constant */
                  n=32 ;

      while (n-->0) {                         /* basic cycle start */
            sum += delta ;
            y += ((z<<4)+k[0]) ^ (z+sum) ^ ((z>>5)+k[1]) ;
            z += ((y<<4)+k[2]) ^ (y+sum) ^ ((y>>5)+k[3]) ;
       }                                  /* end cycle */
      v[0]=y ; v[1]=z ; }
```

Fig.7- TEA Encryption Function

6 Simulation Analysis

"For encryption, the best solution is to combine public- and secret-key systems in order to get both the security advantages of public-key systems and the speed advantages of secret-key systems" [11]. The next table will show how much faster blowfish algorithm to encrypt when all the algorithms (DES, 3DES, AES, Blowfish) with different text file sizes.

10

Text File Size (in Kbytes)	AES	3DES	Blowfish	DES
20	42	34	25	20
48	55	55	37	30
108	40	48	45	35
242	91	82	46	51
322	115	115	48	47
780	165	170	65	85
910	213	230	68	145
5501	260	310	120	250
7200	210	286	109	260
7838	1240	1470	122	1280
22335	1370	1800	155	1720
42000	1530	2300	165	2100
99000	1720	2750	190	2600
Average Time	542.38	742.31	91.92	663.31

Table 1- Comparative Encryption times (in ms) of various algorithms with different packet size

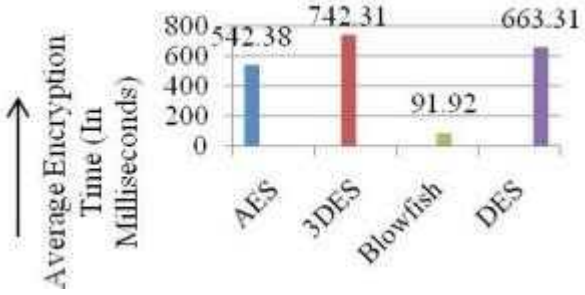


Fig.8- Encryption time of each Algorithm (in ms)

After analyzing both the table and the figure we can conclude that the algorithm with the fastest Encryption time is blowfish by far and the slowest one is 3DES with DES not far behind. We can see that in the beginning with the lighter files DES Encryption was faster than Blowfish but over 780kb the blowfish became faster. For last, the average time is much lower on blowfish algorithm than on AES, DES and 3DES.

Input size in (Kbytes)	AES	3DES	Blow fish	DES
49	63	53	38	50
59	58	51	26	42
100	60	57	52	57
247	76	77	66	72
321	149	87	92	74
694	142	147	89	120
899	171	171	102	152
963	164	177	80	157
5345.28	655	835	149	783
7310.336	882	1101	140	953
Average Time	242	275.6	83.4	246

Table 2- Comparative Decryption times (in ms) of various algorithms with different packet size

From this table we can easily see that Blowfish is a better option to decrypt than the other algorithms. We can also tell that AES is faster than 3DES and DES, and even though 3DES is a successor of DES it is still slower than it [12].

The values of the AES, 3DES and DES decryption time is similar, but once again blowfish is much lower than the others. We can see that from the beginning blowfish "leads" from the beginning the timer, making it faster and more efficient. AES starts with the most time to decrypt but over 899kb it is equal to 3DES but slower than DES.

When we get to the 5345.28kb, AES surpasses 3DES and DES, making it the second one with the lowest time to decrypt, so we conclude that decryption process is a little influenced by size.

7 Conclusion

This paper above presented is a Comparative Study of Different Data Encryption and Decryption Techniques. For this to happen it was explained first what cryptography was and how was this concept important for this study. It was studied how these methods work and how can they be useful to a society that is more and more dependent of the internet and online services. It was shown how their algorithms operate and their performance. The algorithms that were compared are AES, 3DES, Blowfish and DES and it was concluded that Blowfish is the most effective algorithm in terms of performance and sometimes is the most needed to serve a certain job. In the other hand, 3DES was shown as the least effective one, taking more time than the other to encrypt and decrypt. The speed and power of this symmetric algorithm is amazing. On the other hand, on the asymmetric side, RSA is the most used on online network duo his speed and security. The goal is to find an algorithm that is secure, fast and effective.

12

References

1. Kumar, A.Y. (2013) Comparative Study of Different Symmetric Key. International Journal of Application or Innovation in Engineering & Management, 2, 204-206
2. Abd Elminaam, D., Abdual Kader, H.M. and Hadhoud, M.M. (2010) Evaluation of the Performance of Symmetric Encryption Algorithms. International Journal of Network Security, 10, 216-222.
3. Avithra, S. and Ramadevi, E. (2012) Study and Performance Analysis of Cryptography Algorithms. International Journal of Advanced Research in Computer Engineering & Technology, 1, 84
4. Nenchev, Dragomir N. "Redundancy resolution through local optimization: A review." Journal of robotic systems 6.6 (1989): 769-798.
5. Sarik,Marko (2015), Blogging Strategy That Works: Reduce, Reuse, Recycle Content To Attract A New Audience
6. Stallings, W. (2014) Cryptography and Network Security Principles and Practice. Sixth Edition, Prentice Hall, Upper Saddle River.
7. William Stallings (2003), Cryptography and Network Security, 3rd edition, Pearson Education
8. Thakur, Jawahar, and Nagesh Kumar. "DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis." International journal of emerging technology and advanced engineering 1.2 (2011): 6-12.
9. Adhie, Roy Pramono, et al. "Implementation cryptography data encryption standard (DES) and triple data encryption standard (3DES) method in communication system based near field communication (NFC)." Journal of Physics: Conference Series. Vol. 954. No. 1. IOP Publishing, 2018.
10. Williams, Derek. "The tiny encryption algorithm (tea)." Network Security (2008): 1-14.
11. Mitali, Vijay Kumar, and Arvind Sharma. "A survey on various cryptography techniques." International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) 3.4 (2014): 307-312.
12. Kansal, Shaify, and Meenakshi Mittal. "Performance evaluation of various symmetric encryption algorithms." 2014 international conference on parallel, distributed and grid computing. IEEE, 2014.

The importance of Ethical Hacking tools and techniques in Software Development Life Cycle

Avito Da Silva

Lusófona University, Porto. Rua Augusto Rosa n24 4000-098 Porto-Portugal
alexandreavito@gmail.com

Abstract. When developing software, it is important to develop secure software before deploying and most of the time developers inject vulnerable code into the software without realizing it. It is very hard to have perfectly secure software, but it is possible to minimize most of the risks and vulnerabilities. For instance, a hacking attack on a company's information system for example can generate a lot of expenses and problems like leaking or losing meaningful data, reports, and sensitive client information.

Over the years, technology has been increasing its presence all around the world and now we use the software in almost every place like hospitals, local shops, supermarkets, in the industry, and many more. So ethical hackers use a variety of tools and techniques to simulate a hacking attack to try to find risks and vulnerabilities and minimize them if they find any to protect the software so that a company or user can use it safely.

In this paper, we are going to discuss what is ethical hacking, who is an ethical hacker, the tools, and the techniques ethical hackers use, and how they can interact with the software development life cycle.

Keywords: Ethical Hacking, Software Development, SDLC, Software Security, Software Vulnerabilities, Mobile Applications, Web Application, Embedded System

1 Introduction

Developing software is not the easiest task and takes a lot of resources like developers, managers, designers, analysts, hardware, money, and time. The most difficult resources to manage to develop a secure software are time and money because the longer it takes to develop the software the more expensive it gets and customers most of the time try pay the minimum possible which sometimes takes the time of the software testing because developers are more focused on implementing all the requirements that when it comes to testing phase there isn't not too much time to make all the tests. Einstein once said "A clever person solves problems. A wise person avoids it" and when it comes to software security, we should avoid all possible vulnerabilities during the development because after the deployment it will be more expensive and could also lead to some serious problems, for instance hacking an embedded sys-

tem such as aircraft can be used as an act of terrorism by taking it down and consequently arm people.

The remainder of this paper is organized as follows: Section 1 “Software development” is talked about what are processes of software development and is life cycle, the risks associated with not developing a secure software now a days and costs of data breaching.

In section 3 “Ethical Hacking” is addressed what is ethical hacking, who is an ethical hacker, tools and techniques used in the ethical hacking phases and importance of ethical hacking in mobile applications, web applications and embedded software.

2 Software development

Software Development refers to a set of computer science activities dedicated to the process of creating, designing, deploying, and supporting software. Development involves the tools, methodologies, and processes necessary to create software, it also concerns the code and algorithms that physicists, device fabricators, service scientists, chemists, and hardware makers need to write in the course of doing their work. Software development also involves the activities of skilled individuals who develop project-specific software code even though they themselves are not primarily software developers [6].

All software projects go through the phases of requirements gathering, business analysis, system design, implementation, and quality assurance testing.

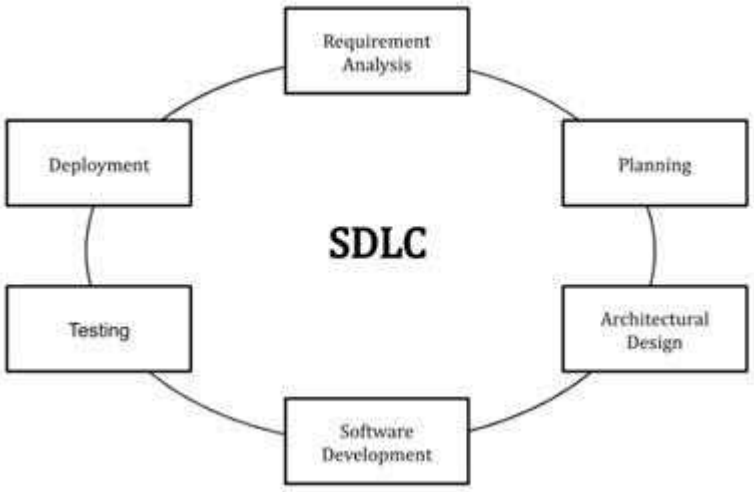


Fig. 1. Software development life cycle [2]

2.1 The risks of developing a non-secure software now a days

We live in a digital era where we use software almost all day from the simplest applications like online shopping, social media, listening to an audiobook or music through most complex ones like hospital systems, organization portals, business process management tools or software to control devices or even industries machine. These software or applications capture and generate a lot of data and most people need this critical data available and secure for their day-to-day activities or jobs.

The total amount of data created, captured, copied, and consumed globally increased rapidly over the years reaching 64.2 zettabytes in 2020. Over the next five years up to 2025, global data creation is projected to grow to more than 180 zettabytes [4].

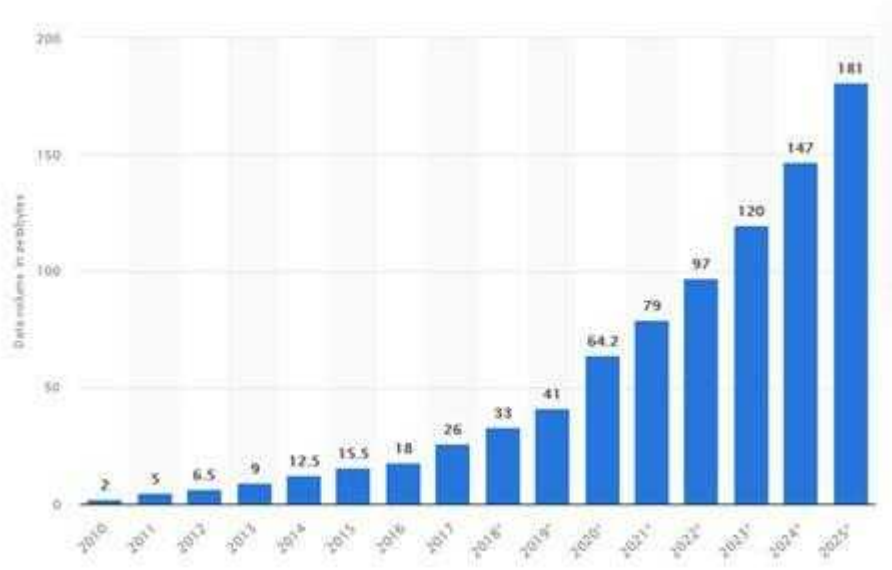


Fig. 2. Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2025

As we can see in the figure 2, with the amount of data increasing every year the necessity of securing and maintaining the integrity of this data is increasing and below in figure 3 is a report of the data breach cost in euros during the years of 2014 – 2019.

4

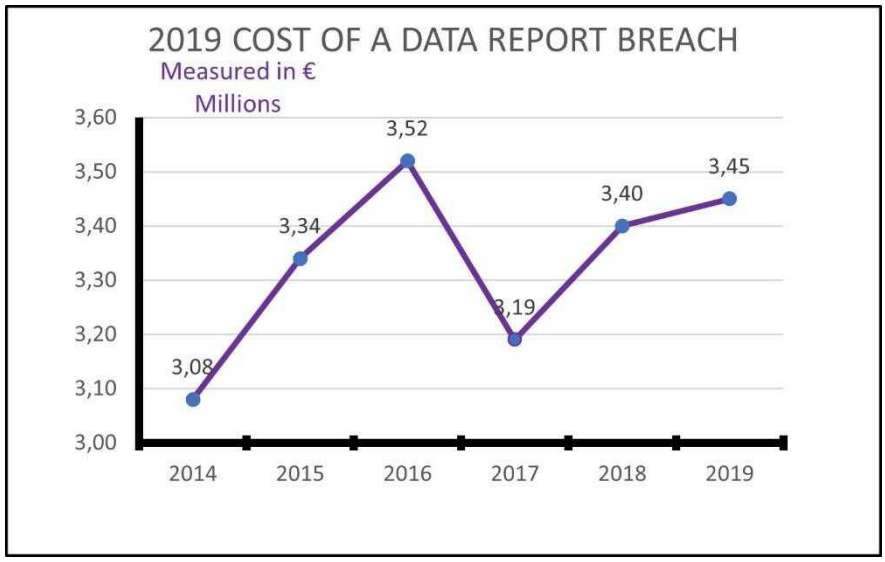


Fig. 3. Cost of a data breach report [1]

A malware, or malicious software, is any piece of software that was written with the intent of doing harm to data, devices, or to people. Types of malwares include computer viruses, trojans, spyware, ransomware, adware, worms, file-less malware, or hybrid attacks. Recent malware attacks have become more sophisticated with the advent of machine learning and targeted spear-phishing emails [1].

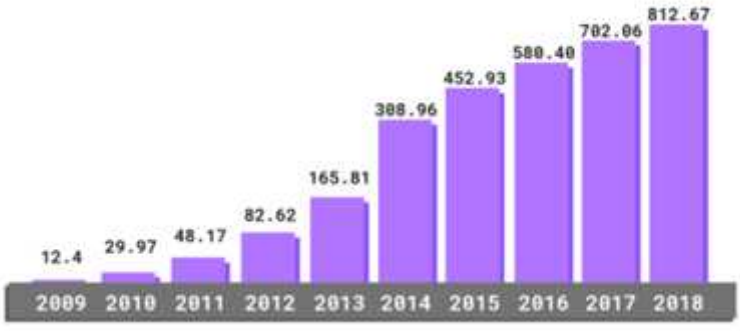


Fig. 4. Total malware infection growth rate in millions

Some vulnerabilities can come from a bad database design, weak implementation (both frontend and backend) and weak testing.

The testing phase is very important and should always be scheduled so he goes as planned that is why is very important to develop a testing report where all the tests

that are going to be applied to the software should be documented. Is also a good idea to have a maintenance plan report, in this report it should be documented how the software will be maintained and things to do if something happened for instance if an hacker gained access to system it should be documented what the organization should do to minimize the impact or solve this particular issue or any other possible issues.

3 Ethical hacking

Is an authorized attempt to do penetration testing on a company's system before the attempt is written a contract where the company specifies what the ethical hacker can attempt to hack, and the ethical hacker should not try to hack any component outside the ones specified in the contract.

Who is an ethical hacker?

The EC-Council, the leading cyber security professional certification organization, defines an ethical hacker as "an individual who is usually employed with an organization and who can be trusted to undertake an attempt to penetrate networks and/or computer systems using the same methods and techniques as a malicious hacker." Sometimes ethical hackers come from the "dark side" after repaying their debt to society, but you can also learn ethical hacking skills in a classroom setting and become certified [8].

3.1 Ethical hacking phases and tools

Are the phases and tools an ethical hacker can follow to perform the hacking attack. They are like the hacking phases the only difference is that an ethical hacker after performing the attack it should analyze the test result and produce to the organization an improvement plan to minimize the risks if they exist. It is not required to sequentially follow these phases.

In this phase it will be shown the tools and techniques that are used in each phase of the hacking attack and how to avoid some of these attacks.

There are two most known operating system hackers or ethical hackers tend to use:

Kali Linux – is a Linux distribution for ethical hackers, hackers and computer forensics that comes with a pre-installed with an arsenal of hacking tools and has some fantastic features like full customization of kali ISOs which means it can be customizable to a person needs, usb live boot, kali undercover which changes the look of the environment to a Windows10 desktop environment, and many more [9].

Parrot OS – is another famous operating system when it comes to cybersecurity and computer forensics, it is secure, lightweight, free and open source and comes preinstalled with some IDE's and Compilers which helps IT teams of all sizes develop software and perform security-related tasks such as computer forensics, penetration testing, cryptography, hacking or reverse engineering [10].

Reconnaissance. According to the book "Ethical Hacking and Countermeasures" it's the phase where the hacker gathers as much information as possible about the target

or system and carefully plans the attack. Part of this reconnaissance may involve social engineering. A social engineer is a person who convinces people to reveal information such as unlisted phone numbers, passwords, and other sensitive information. Another technique is Dumpster Diving. Dumpster diving is, simply enough, looking through an organization's trash for any discarded sensitive information.

When an attacker is using passive reconnaissance techniques, he or she does not interact with the system directly. Instead, the attacker relies on publicly available information, social engineering, and even dumpster diving as a means of gathering information.

Active reconnaissance techniques, on the other hand, involve direct interactions with the target system by using tools to detect open ports, accessible hosts, router locations, network mapping, details of operating systems, and applications. Active reconnaissance is usually employed when the attacker discerns that there is a low probability that these reconnaissance activities will be detected [3].

Social engineering can be avoided by implementing good security policies describing how to act correctly with the organizations resources or data and regularly perform information systems audit.

Some tools used during this phase:

- Network Mapper (Nmap): free and open-source tool used for discovering available network hosts, what applications and the operating system they are running.
- Whois lookup: Contains personal information of the domain owners, the database is maintained by Regional Internet Registries. Can be used to get domain name details, contact details of the domain owner and domain name servers.

Scanning. Here the hacker/attacker uses gathered information in the reconnaissance phase to identify specific vulnerabilities, this phase can be considered a logical extension of an active reconnaissance. Often the reconnaissance and scanning phases overlap, and it is not always possible to separate the two [3].

The tools listed below can search for thousands of vulnerabilities and most of them verify web apps, databases, some of them verify networks and servers. They should be used during the development of the software and after the deployment so the vulnerabilities can be minimized if they exit.

Table 1. Scanning tools

Tool	**Short description**
Metasploit	One of the most famous and powerful vulnerabilities tools it is open source which means it can be customized. Metasploit contains a lot of tools that can help the ethical hacker execute attacks and evade detection
Netsparker	Paid web application capable of delivering auto verification of vulnerabilities in web applications or integrating security testing into the entire SDLC of the web app and creating a scan report summary

W3AF	Free and open source also known as Web Application Attack Framework. It´s a user-friendly app that can secure web apps by finding and exploiting vulnerabilities.
Nikto2	An open-source web application that focuses on web applications security and is capable of scanning web servers
Acunetix	Paid web application comes with many functionalities, capable of finding web applications and network vulnerabilities
OpenVas	Powerful tool, suitable for the organization. Can find vulnerabilities in databases, operating systems, networks, and virtual machines.

Gaining Access. In this phase the hacker will use the information he knows about the system to attempt to gain access. If the system doesn't have a robust implementation hackers can cause some damage to system just by trying to penetrate it. Knowing the system, you're penetrating makes it easier to for hackers to hack, that's why is important have a secure implementation in the software.

For instance, external denial-of-service attacks can either exhaust resources or stop services from running on the target system. Service can be stopped by ending processes, using a logic bomb or time bomb, or even reconfiguring and crashing the system. Resources can be exhausted locally by filling up outgoing communication links.

Attackers use a technique called spoofing to exploit the system by pretending to be a legitimate user or different systems. They can use this technique to send a data packet containing a bug to the target system to exploit a vulnerability. Packet flooding may be used to remotely stop the availability of essential services. Smurf attacks attempt to cause users on a network to flood each other with data, making it appear as if everyone is attacking each other, and leaving the hacker anonymous [3].

Hackers sometimes get into an organization system by the organization employee, they can send a phishing email or crack the password and get into the system, to crack the password they can use join brute force attack with social engineering, trojan, spyware keyloggers and maybe man in the middle.

Maintaining Access. After gaining access the ethical hacker should work to try to keep the access, he can keep a low profile and keep exploring the current system or attack other systems.

Attackers, who choose to remain undetected, remove evidence of their entry and install a backdoor or a Trojan to gain repeat access. They can also install rootkits at the kernel level to gain full administrator access to the target computer. Rootkits gain access at the operating system level, while a Trojan horse gains access at the application level [3].

Trojans can be avoided by automatically updating the operating system and the antivirus, the applications should also be updated to avoid security flaws, avoid suspicious sites and emails, and use complex passwords.

Rootkits can be avoided by scanning the system, updating, and avoiding suspicious links.

Covering or clearing tracks. For obvious reasons, such as avoiding legal trouble and maintaining access, attackers will usually attempt to erase all evidence of their actions. Trojans such as ps or netcat are often used to erase the attacker's activities from the system's log files. Once the Trojans are in place, the attacker has likely gained total control of the system. By executing a script in a Trojan or rootkit, a variety of critical files are replaced with new versions, hiding the attacker in seconds. Types of Hacker Attacks 1-9 Other techniques include steganography and tunneling. Steganography is the process of hiding data in other data, for instance image and sound files. Tunneling takes advantage of the transmission protocol by carrying one protocol over another [3].

3.2 The importance of ethical hacking in web applications

When it comes to application software web applications are the ones who suffer most hacking abuse since they can be accessed by everyone at any time and place so is important to conduct security testing during the testing phase of the SDLC and after the application deployment. To minimize the probability of successful attacks, software engineering teams must apply the effort necessary to introduce adequate security precautions. Achieving this goal is only possible by using various techniques and tools to ensure security in all phases of the software product's development life cycle [12]. The automated testing such as OWASP ZAP and Nikto tool is used to detect weaknesses in network infrastructure and web application [11].

The two most common risks in the Web environment, injection—namely SQL injection, which lets attackers alter SQL queries sent to a database—and cross-site scripting (XSS), are also two of the most dangerous (www.owasp.org/ index/Category:OWASP_Top_Ten_Project)[12].

SQL Injection is a database attack and a manifestation of the existence of flaws in WEB application programs. The mechanism of attack is to insert the user data into the actual database manipulation language by using the peripheral interface of some database. In this way, the goal of invading the database and even the operating system can be realized [5].

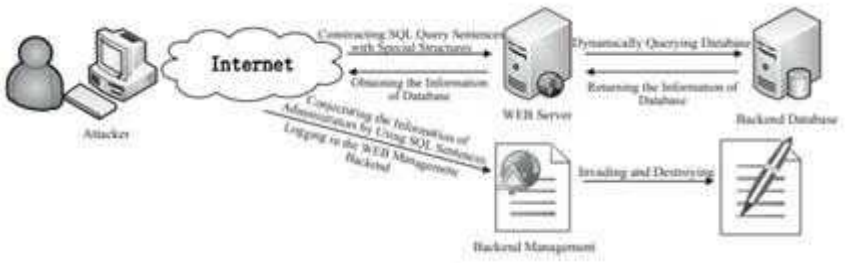


Fig. 5. Procedure of SQL Injection

Cross-Site Scripting also known by XSS attack is the topmost vulnerability found in the today's web applications which to be a plague for the modern web applications. XSS attacks permit an attacker to execute the malicious scripts on the victim's web browser resulting in various side-effects such as data compromise, stealing of cookies, passwords, credit card numbers etc. We have also discussed a high level of taxonomy of XSS attacks and detailed incidences of these attacks on web applications [7].

3.3 The importance of ethical hacking in mobile applications

Over the years mobile devices have become more indispensable and is presence has been increasing over these past years. Now a days we use and store a lot of sensible information in these devices so the necessity of having a secure application that stores these information or data has also increased.

The most important threats to enter phones start with malware or Trojans, these malicious programs hide inside good programs, stealing information and running automatically to other devices [14] [15].

Table 2. Security Threats in mobile applications [16]

Security threats	Explanation
Malware	Threats installed on the terminal for malicious behavior
Spam	Threats used to distribute advertisements and malware that can be sent to an unspecified number of people
Application vulnerability	Threats that perform malicious actions such as elevation of privileges by using the vulnerability of the developed application
Personal information extrusion	Threat of personal information leakage due to user carelessness when developing installed applications
Authentication bypass	Threats that randomly bypass or steal authentication for applications that require authentication
DoS	Threats that make the service provided by the application unusable

3.4 The use of ethical hacking in the development of embedded software

Is a developed software that grounds on devices like blood pressure monitors, gamming microcontrollers, aircrafts, cooking machines and many other devices that have custom hardware to perform specific functions.

Some incidents:

- Computer security researcher Chris Roberts was arrested on suspicion of having hacked into a United Boeing 737 during an April 2015 flight from Denver, Colorado, to Syracuse, New York [18] [19].
- In July 2015, two researchers demonstrated how to take over a Jeep Cherokee using the car's telematics system, shutting off the engine and disabling the brakes while a journalist drove the car [18] [20].
- In September 2015, Volkswagen admitted to installing software that defeated the emissions control system during testing on as many as 11 million diesel cars going back to 2009 [18] [21].
- In 2018, ethical hackers found Meltdown and Spectre hardware vulnerabilities that affect all Intel x86 and some AMD processors. Both vulnerabilities mess up isolation between user applications, giving applications access to sensitive data and expanding the attack surface. Both Linux and Windows developers have issued patches for their operating systems that partially protect devices from Meltdown and Spectre. However, lots of devices (especially old ones) running on vulnerable processors are still unprotected [22].

Vulnerability in embedded software can give hacker the opportunity of gaining sensible data, cause physical damage to the device hacked or even arm humans. Since they are expensive and valuable machines is important to ensure their security. Yet implementing security measures in embedded systems is connected with numerous challenges like power limitation, development expertise, network connectivity and poor access control, physical exposure [22].

Counter measures. Some counter measures could be considered to make sure all the vulnerabilities associated with the embedded system software is minimized.

The follow counter measures could help achieving a secure software:

- Conducting end to end threat analysis: The security of an embedded device can be improved by starting with identifying the potential threats. These threats must be evaluated in the context of the device manufacturer, operators (if the device is provisioned in such a way, and end users, including their usage). The attacks can be done in terms of wired Ethernet connection with the device used for communication, and common services such as web (HTTP). A complete product life cycle analysis needs to be performed [23].
- Select an Appropriate Run-Time Platform: - Restricting use of common platform govt should ensure that organizations should select an appropriate commercial runtime platform for an embedded system and make it mandatory for use. Implementing a system with components that have COTS security can increase the security and reduce the cost of development of the overall platform [23].

- Software design and implementations: It is important to write secure code so that the risks are of being attacked are minimized during the SDLC, is also a good idea to have a robust software architecture because he can make the software harder to hack and even minimize the hacking impact.
- Secure the Applications: - Same as the products should be tested first the application should also be tested first. Standards should be made and tested and then only permit the apps to get launch [23]
- Design and test for security: Security vulnerabilities are a class of software requirement deficiencies in design or implementation and earlier they are caught in the product development life cycle, the less costly it is to fix them and harden a system against attack. Security testing must involve defining the boundaries of a system and determining methods of exploiting weak defenses along these boundaries [23].

4 Conclusion

Is important to ensure the software is secure before deploying to the customers so it is crucial to conduct ethical hacking tests during the testing phase and before the deployment or production phase of SDLC. When it comes to developing a secure software is important to plan and schedule the software testing phase because if they manage to find vulnerabilities in this phase it will be less expensive correcting them now then correcting them during or after the production phase and consequently being vulnerable of a hacking attack like data breach and possibly generated even more expenses. It is a goal not only for developers but also for the customers to be confident that the software is less vulnerable to hacking and, in this paper, it is not only discussed the hacking phases the tools and techniques hackers used in these phases, but also particular security problems related to web application, mobile application and embedded system software security, the most common vulnerabilities associated and what are the risks of consequences if someone exploit them and what are measures avoid them.

5 References

1. “2021 Cyber Security Statistics: The Ultimate List Of Stats, Data & Trends.” *PurpleSec*, https://purplesec.us/resources/cyber-security-statistics/. Accessed 22 November 2021.
2. Altvater, Alexandra. “What Is SDLC? Understand the Software Development Life Cycle.” *Stackify*, 8 April 2020, https://stackify.com/what-is-sdlc/. Accessed 26 November 2021.
3. EC-Council. *Ethical Hacking and Countermeasures: Attack Phases*. vol. 1, EC-COUNCIL | PRESS. 5 vols.
4. Holst, Arne. *Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2025*. 07 June 2021. *Statista*, Statista, https://www.statista.com/statistics/871513/worldwide-data-created/. Accessed 03 October 2021.

12

5. Hu, Haibin. “Research on the technology of detecting the SQL injection attack and non-intrusive prevention in WEB system.” *AIP Publishing*, 8 May 2017, https://doi.org/10.1063/1.4982570. Accessed 23 November 2021.
6. IBM. “Software development.” *IBM Research*, https://researcher.watson.ibm.com/researcher/view_group.php?id=5227. Accessed 17 October 2021.
7. Gupta, Shashank & Gupta, B B. (2015). Cross-Site Scripting (XSS) attacks and defense mechanisms: classification and state-of-the-art. International Journal of Systems Assurance Engineering and Management. 8. 10.1007/s13198-015-0376-0.
8. simplilearn. “What Ethical Hacking Skills Do Professionals Need?” *Simplilearn*, 8 October 2021, https://www.simplilearn.com/roles-of-ethical-hacker-article. Accessed 29 November 2021.
9. “Kali Linux Features.” Kali Linux, https://www.kali.org/features/.
10. “Parrot OS - 2022: recensioni, prezzi e demo.” Software Advice, https://www.softwareadvice.pt/software/238015/parrot-os. Accessed 12 January 2022.
11. Devi, R. & Kumar, Mohankumar. (2020). Testing for Security Weakness of Web Applications using Ethical Hacking. 354-361. 10.1109/ICOEI48184.2020.9143018.
12. Antelo, Elisardo. “Defending against Web Application Vulnerabilities.” free statistics, https://eden.dei.uc.pt/~mvieira/2012_Computer_DefendWeb.pdf. Accessed 13 January 2022.
13. Zed Attack Proxy (ZAP), 20 January 2020, https://owasp.org/www-chapter-dorset/assets/presentations/2020-01/20200120-OWASPDorset-ZAP-DanielW.pdf. Accessed 13 January 2022.
14. Hernández, Miguel, Luis Baquero, and Celio Gil. "Ethical Hacking on Mobile Devices: Considerations and practical uses." International Journal of Applied Engineering Research 13.23 (2018): 16637-16647.
15. Craig Heath, Symbian OS Platform Security: Software Development Using the Symbian OS Security Architecture. 2006
16. “A Study on the Mobile Application Security Threats and Vulnerability Analysis Cases.” Korea Science, https://www.koreascience.or.kr/article/JAKO202034465346164.pdf. Accessed 13 January 2022.
17. Mutchler, Patrick & Doupé, Adam & Mitchell, John & Kruegel, Chris & Vigna, Giovanni. (2015). A Large-Scale Study of Mobile Web App Security.
18. M. Wolf, "Embedded Software in Crisis," in Computer, vol. 49, no. 1, pp. 88-90, Jan. 2016, doi: 10.1109/MC.2016.18.
19. http://securityaffairs.co/wordpress/36872/cyber-crime/researcher-hacked-flight.html
20. A. Greenberg, "Hackers Remotely Kill a Jeep on the Highway—with Me in It", Wired, July 2015, [online] Available: www.wired.com/2015/07/hackers-remotely-kill-jeep-highway.
21. M. Thompson and I. Kottasova, "Volkswagen Scandal Widens", CNNMoney, Sept. 2015, [online] Available: http://money.cnn.com/2015/09/22/news/vw-recall-diesel/index.html
22. https://www.apriorit.com/dev-blog/690-embedded-systems-attacks
23. EMBEDDED SYSTEMS SECURITY, https://tec.gov.in/pdf/Studypaper/Embedded%20sytem%20security.pdf. Accessed 14 January 2022.

The importance of Ethical Hacking tools and techniques in Software Development Life Cycle

Adolfo Cruz

Lusófona University of Porto, Portugal
adolfo00cruz@gmail.com

Abstract. Nowadays developed software can never guarantee to be fully secure against all the type of threats. To help with this task we have ethical hackers who are individuals that are responsible for using different tools and techniques to test the developed software, basically they incorporate the role of bad hackers forcing all the secure parameters of the software but besides of the bad hackers, when they pass through the security firewalls. They don't use the information that they got for something illegal, they just do a document with all the security breaches that the software has and deliver it to the CEO or a superior of the company that they work for. Therefore, the company just tries to find solutions for those breaches.

It's because of this that Ethical Hacking is extremely important for software development, but not just for the company, also for the user's safety (eg. personal data) so investing more in this sector of software development is a must for Internet and Software security around the world.

This research work aims to discuss about several techniques and tools involved in ethical hacking, known attacks and the respective solutions to avoid them on software development security.

Keywords: Hacking, Ethical Hacking, Penetration Testing, Software Security, Software Testing, Software Development, Vulnerability Analysis.

1 Introduction

Millions and millions of euros are lost through mistakes during the Software development process [1]. One of the most expensive mistakes are on the security area of the software (e.g., when the programmers leave security breaches without even knowing it). In case that some company it's hacked besides the economic expense the most crucial problem are the user and company data leaked through the hacking operation because these types of data it´s one of the most valuable for illegal purposes.

To avoid these million-dollar expenses, nowadays, companies contract ethical hackers. How are these individuals? Are people that have skill and knowledge to search and find security breaches on software with many tools and methods.

In this digital life dependency having our information secure and in “good hands” it’s crucial. With the result of that we depend on a lot of the ethical hackers and the security of the software that we use in our daily routine.

On this paper it will be explained:
In section 2 “Ethical Hacking” it will be explained what ethical hacking is and who are ethical hackers, the different types of ethical hacking, the phases of ethical hacking and what procedures ethical hackers follow, tools and techniques used by an Ethical Hacker
In section 3 we will analyze Software Development life Cycle and The Secure Software Development Life Cycle, the differences between each other and the advantages of the Secure Software Development Life Cycle.
In section 4 it will be a conclusion based on the research.

2 Ethical Hacking

When we hear the word “hacking” we associate with illegal things.

In other words, when we see a photo of someone with a hoodie and a mask the stereotypical image that comes to our minds it’s “Anonymous”.

In the end, nothing it’s like we think, “hacking” can be on a phrase with a good intention and a random guy with a hoodie and a mask don’t exactly as to be a hacker or anonymous.

What is ethical hacking? Ethical hacking it’s a penetration testing or pen testing.

The responsible of these penetration tests are called ethical hackers, people with skills and who enjoy a lot learning the details of computer systems and explore their max capabilities.[1][2]

What is the difference between an ethical hacker and a hacker? It’s simple, ethical hackers have an attacker’s mind but with the intention to help, doing it because they are paid for but in the end the share the security breaches that they found in the respective company that they work for. Bad hackers have the evilest intentions while they are doing an attack, most of the bad hackers do it for money but the difference between this and the ethical hackers it’s that the final propose it’s with a bad intent, some for being recognized as “heroes”.[1]

2.1 Types of ethical hacking

Organizations need to be up to date against every type of hacking attacks because the security that they have can already be outperformed by new hackers’ attacks attempts consequently we can use ethical hacking on different situations but let’s focus these assessments:

- Infrastructure/Employee
- Application
- Physical Entry
- Stolen Laptop

These assessments could entirely compromise one company, due to the financial costs of the breaches, the leaked information, compromise national security, that's why, once again, ethical hacking should be a must for every company in the software development area.

Infrastructure.

Nowadays this is probably the most dangerous breach that we can have on a company, different policy's have been introduced to prevent attacks by this breach but depends a lot of the company employees.

So, the way that the organization's prevent these attacks are by using a VPN, making a lot of safety policy's to be followed by employees, improving some critical Web Portals safety, … [3]

Ethical Hacking can be useful here by testing employees with Social Engineering and phishing emails to get company information for e.g., and if hackers gain some information by this way, companies can see how far hackers could go with that type of information preventing their following steps by increasing delicate points security. With this, they can be ahead of hackers ideas and prevent future damages to the company not needing to depend on their employees.

Application.

Performing networked-based testing to simulate hackers' behavior on our Web Applications and mobile apps it's another way of improving future damages and losses.
It will be helpful ethical hacking this area to test the resilience of the customer portal against unauthorized access or malicious behavior of a valid customer. [3]

2.2 Ethical Hacking Phases

Like one recipe, Ethical Hacking must follow some steps which are: Reconnaissance where the hacker tries to gain information about the target (footprint).
Scanning it's the phase that the hacker use the information of the last step to search vulnerabilities.
Gaining Access where with a list of vulnerabilities the hacker will attack the weak spots.
On Maintaining Access/Zombie System the hacker tries to keep the control of the victim.
The last step will be Evidence Removal that consists in cleaning the proves that the left when attacked.

Reconnaissance.

On this initial step hackers try to gain information of the target, this "information gathering" or "footprint" can be done without knowledge at all from the individual, but it will require much more effort from the hacker to fill all the information gaps, but it can be easily gained too.

There are to types of reconnaissance, active and passive, on the passive the hacker doesn't attack the system or the company network, depends a lot of Social Engineering methods on the target just by searching him on internet or physically getting information (e.g., picking up some target trash that could have vital information), active hacking it's only done when we have information of the target, it's unsafe for the hacker because he can be easily caught, the hacker enters on the company's network to discover individual hosts, network services, and Ip addresses, operating system, etc...

The information gained on this step will be useful on the following step.

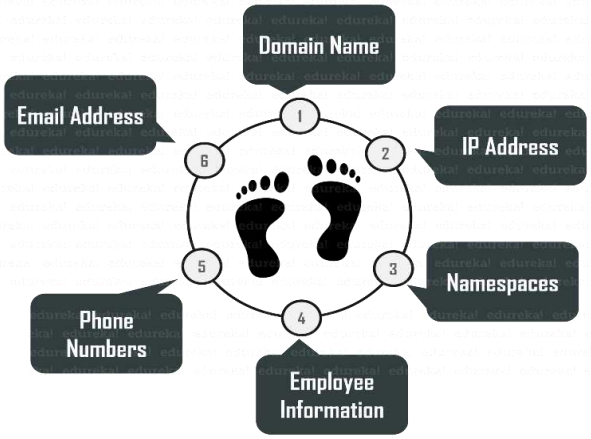


Fig. 1. Footprint main information's

Scanning.

Using the information that they get on reconnaissance the hackers now will look at that more deeply trying to find vulnerabilities so they can access the system.

Tools like dialers, port scanners, network mappers, sweepers, and vulnerability scanners are used in the scanning phase to scan data and records.

Ethical hacking uses three different methodologies:

- Vulnerability Scanning (find targets vulnerabilities and weak points using Netsparker, Nmap, etc…)
- Port Scanning (opening TCP and UDP ports with port scanners and dialers, finding open doors to access organization's system)
- Network Scanning (find and locates every device connected to the organization network, find ways to exploit the company network)

Gaining Access.

Ethical Hackers will try everything they can, to access the system on an unauthorized way. Every tool and methods will be used to gain access and enter the system, the system can be protected with a firewall and passwords that will slow down the time that a hacker can hack the system.

When succeed, they will be able to exploit the system with malware, steal and leak some sensitive information, infect the system with ransomware. Nowadays the tools that are the most used to do this it's Metasploit.

Maintaining Access / Zombie System.

After having the access ethical hackers will not give that up, so on this step, they will have to maintain the access. Maintaining it will need to launch DDos Attacks, exploit the system, use Trojan tools, steal the entire database, …

To avoid the system from being exploited, ethical hackers and penetration testers can scan throw the entire company infrastructure to see if it has any malicious activities.

Evidence Removal.

To not get caught the hacker must destroy every evidences and traces of hacking that he did by deleting logs or registry values, uninstalling folders and applications to ensure that everything it's on their original state.

Ethical hackers can erase their tracks:

- Using reverse HTTP Shells
- Erase the digital footprint deleting the cache and history
- Using Internet Control Message Protocol Tunnels

2.3 Tools and Techniques of an Ethical Hacker

Ethical Hackers to do their job use different techniques and tools, these can be used during the SDLC (Software Development Life Cycle).

Table 1. Ethical Hacking techniques

Attacks	Description
Phishing	*Consist on spam emails and bogus websites. To avoid this the company, need to have an anti-phishing detector.*

6

Malware	*We have different types of malware, to avoid them we need to have some program to detect it, dodging future damage.* .
SQL Injection	*It's one technique that the main focus it will be the application's database. To avoid this the input never should be used directly on the application code.*
Session Hijacking	*Technique that makes hackers steal our session on the Web Application. To prevent this, we can use secure HTTP or SSL between the application server and the user's browser.[10]*

Table 2. Ethical Hacking Tools

Tool	Description
Metasploit [11]	*Discover vulnerabilities and execute exploits. Enumerate and scan the networks and hosts remotely.*
Nmap [12]	*This tool finds vulnerabilities a network and do a network mapping.*
Nikto [13]	*Scan servers and perform scan tests.*
Wapiti [14]	*Finds security flaws in web application*
Burpsuite [15]	*It works by intercepting proxy traffic and scanning web applications.*

.

The operating system that Ethical Hackers use more it's Kali Linux [9], because there are 600 pre-installed penetration testing tools. Besides Kali Linux they use also: Parrot OS (tools such TOR and Onion share, lightweight dedicated CDN's), Fedora Security Lab (Security forensics, system rescue and education on security testing methods) , Dracos Linux (has three main directories attack, defense, forensics), Arch Strike (penetration testing, free open-source tools for investigation)

3 SDLC (Software Development Life Cycle)

The SDLC it's a process of developing, implementing, and retiring information systems through a multistep model: Requirement analysis, planning, architectural design, coding, testing and deployment.

It aims to aid developers and other project staff to create a system that meets all technical and user requirements as well as exceeds customer expectations.[16]

On Requirements analysis makes a document that have the expected behavior for the app or software to be developed.

The Planning step it's where the team of programmers, etc.., plan software development calendar.

On Architectural Design the team develops the design for the programmers start developing that on the coding step.

The coding phase it's when the application starts to gain form till the result.

On Testing phase, when the app development it's finished, it is tested for issues like performance, functionality, bugs, security.

Once the application it's tested and has a result, will be deployed in the market.

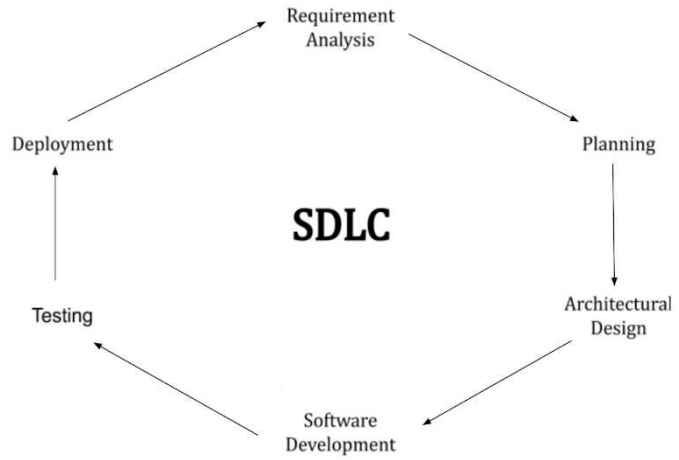


Fig. 2. SDLC steps

As we can see the topic "Security" has been briefly touched on the SDLC, leaving us thinking that the software made it's not secure.

The principal issues caused by this lack of security are: The future costs to resolve the problems ("On average enterprises pay US$551,000 to recover from a security breach. SMBs spend 38K. This is direct spend required to recover from an attack." [17]); The leaked information by cyberattacks, that it's bad to the company and an critical issue to the users because this information gathered by the hackers can have sensitive content ("90% of businesses admitted a security incident. Additionally, 46% of businesses lost sensitive data due to an internal or external security threat." [17]);

Fig. 3. Frequency of the three worst (chosen by respondents) consequences of a security breaches [17]

The threats experienced by these security and data breaches sometimes are not revealed by the companies, but the ones that revealed said that malware it's most common threat experienced.

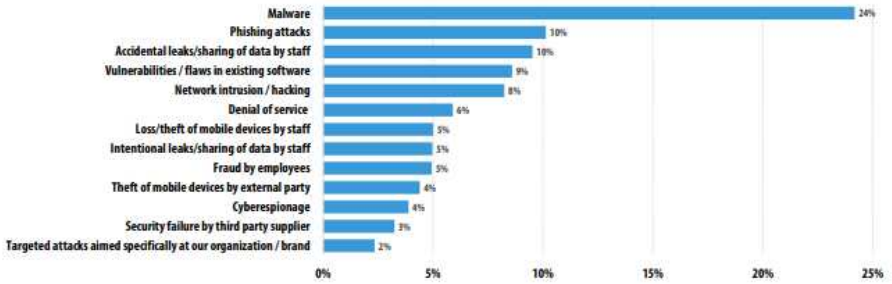


Fig. 4. Threats experienced on companies (chosen by respondents) that are consequences of a security breaches [17]

3.1 Ethical Hacking on SDLC (S-SDLC)

S-SDLC it's an incorporation of the Software Development Life Cycle and security, which means that a software development company can do a better process than the simple SDLC and do a S-SDLC which it's far better on safety. This method because of the security complexity that have made some companies to change their security policy's.

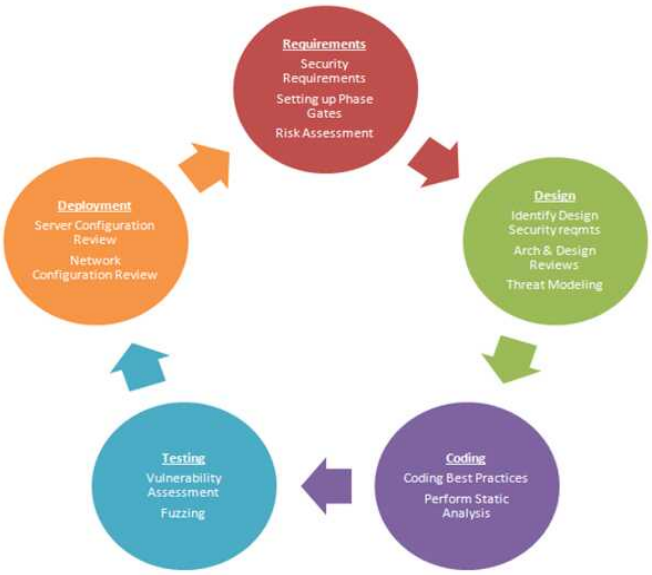


Fig. 5. Representation of a S-SDLC phases

On the requirements phase (after the documentation prepared and approved) it's created the Software Requirement Specification Document or Functional Requirements. These documents contain details of the project such as interfaces, system inputs… The difference between SSDLC and SDLC on this phase it's that here we will have security requirements and Risk Assessment (Strong Authentication, Asset Protection, Supply Chain Security, Data Usage Restriction) [18].

On the Design step we will ensure the security by using for e.g., Cryptosystems (Encryption and decryption of data) and Digital signatures. [19]

Entering the Coding phase, we will have security improvement by doing good coding practices (Error/warning messages, Program organization, clean code) [20].

On the Testing we can use the Fuzzing method that gives us a way of providing invalid inputs to programs to find bugs in software, which can help to find and fix critical bugs. [21]

Finally on the Deployment step we can use for e.g. Server or Network Configuration management that can be summarized as: [22]

- Device hardware and software inventory collection

- Device software management
- Device configuration collection, backup, viewing, archiving, comparison
- Detection of changes to configuration, hardware, or software Configuration change implementation to support change management~

On these phases ethical hackers are crucial and use their techniques to help on the S-SDLC.

4 Conclusion

Technology in the wrong hands can be dangerous and that's why hackers are wrongly misjudge by being only a bad thing to the society. All the news that we saw on TV about Ransomware on a Hospital, Companies getting hacked, etc.… are linked to the word hacker but not with "bad hackers" most people don't know that we have hackers that have good intentions, that help them use some application with more security. These individuals with good intentions are ethical hackers who are professionals that use their hacking skills to improve the security of the apps that we use. Furthermore because of this that Ethical Hacking is extremely important for software development, but not just for the company, also for the users safety (eg. personal data) so investing more on this sector of software development is a must for Internet and Software security around the world.

5 References

1. Luo, C., Bo, W., Kun, H., & Yuesheng, L. (2020). Study on Software Vulnerability Characteristics and It's Identification Method. Mathematical Problems in Engineering, 2020.
2. B. Pandey, L. Balani, A. Singh (2015). Ethical Hacking (Tools, Techniques and Approaches), 2020.
3. Deloitte Ltd (2017). Ethical Hacking Defend against Cyber Attacks, 2017.
4. Danish sharma1,Rituraj Chandra2, C.K Raina3 (2018). Review on Ethical Hacking, 2018.
5. S.Hassan, S.Ahmad (2021). The Importance of Ethical Hacking Tools and Techniques in Software Development Life Cycle (2021).
6. EC-Council. Ethical Hacking and Countermeasures: Attack Phases. vol. 1, EC-COUNCIL | PRESS. 5 vols
7. "Ethical Hacking | Footprinting"shttps://www.geeksforgeeks.org/ethical-hacking-footprinting/.(Accessed December 1, 2021)
8. "What is session hijacking? – Heimdal Security". https://heimdalsecurity.com/blog/session-hijacking/. Accessed 8 December 2021
9. . "Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution," Kali Linux. https://www.kali.org/ (accessed December 15, 2021).
10. I. O. Ogundele, A. O. Akinade, and H. O. Alakiri, "Detection and Prevention of Session Hijacking in Web Application Management," International Journal of Advanced Research in Computer and Communication Engineering, vol. 9, no. 7, pp. 1–10, Jul. 2020

11. “Metasploit | Penetration Testing Software, Pen Testing Security,” Metasploit. https://www.metasploit.com/ (accessed December 16, 2021).
12. “Nmap: the Network Mapper - Free Security Scanner.” https://nmap.org/ (accessed , 2021)
13. “Nikto.” https://tools.kali.org/information-gathering/nikto (accessed December 17, 2021)
14. “Wapiti : a Free and Open-Source web-application vulnerability scanner in Python for Windows, Linux, BSD, OSX.” https://wapiti.sourceforge.io/ (accessed December 17, 2021)
15. “Burp Suite - Application Security Testing Software - PortSwigger.” https://portswigger.net/burp (accessed December 17, 2021).
16. US Department of Justice - The Department of Justice Systems Development Life Cycle Guidance Document. (2003) (accessed January 13,2021)
17. Kaspersky Lab - Damage control: the cost of security breaches, IT security risks special report series. (accessed, January 14)
18. European Union Agency for Network and Information Security ENISA, The EU Cyber Security Agency - Indispensable baseline security requirements for the procurement of secure ICT products and services (December 2016). (accessed 14 January)
19. Le Moyne College INCUBATE (NSF Id 1500033) - Security Design Concepts Target Course: Software Engineering, Software Design. (accessed 14 January)
20. Karl W Broman - Department of Biostatistics Johns Hopkins University (accessed 14 January)
21. Danyang Zhao - Fuzzing Technique in Web Applications and Beyond (accessed 14 January)
22. Cisco Systems, Inc - Network Configuration Management (accessed 14 January)

Cybercrime Warfare Against People: Pessimistic Side of Online

João Sebe[1]
[1] Lusófona University of Porto, Portugal
joaosebe@gmail.com

Abstract. Cybercrime has become as common as the Internet itself and consequently, it is considered one of the biggest threats to unaware individuals who might become victims. Cyberattacks have already caused considerable damage to a huge number of companies and small businesses but not less important, to people. This paper aims to further advance discussions on cyberthreats, cognitive vulnerabilities and cyberpsychology through a critical reflection on the social and psychological aspects related to cybercrime. It also sights on the analyses of the psychological effects an attack might have on a victim, examine the motivation of criminals that perpetuate such attacks and the factors and vulnerabilities they exploit to become successful at it while educating about how these attacks can be prevented through prevention, detection, and investigation since they are not expected to fade from society anytime soon.

Keywords: Cybersecurity, cybercrime, cyberattacks, social impacts, psychological impacts, motivation, cybercriminals' profiling

1 Introduction

Over the last few decades, the Internet has transformed the world we live in. From changing businesses, education, government, healthcare to even changing the way we interact with our loved ones – it has become one of the key drivers to social evolution since everyone is somewhat dependent on computer networks and information technology solutions.

Although the Internet removed many communication barriers that previously existed and keeps us connected to the world almost instantaneously, along with its phenomenal growth, it became a place where numerous unfortunate events take place and where bad intended people practice criminal activity.

To better understand the relationship between technology and crime, it is important to establish the understanding of cybercrime and its effect on today's society. Cybercrime is a term that covers a broad scope of criminal activities by means of a computer and a network. Cybercrime is referred to the act of committing a criminal act using cyberspace as the communication medium [1]. Computer crimes include not only hacking and cracking, but now also include extortion, child pornography, money laundering, fraud, software pirating, and corporate espionage, to name a few [2].

Cyberattacks are described as events that attempt to compromise a system's integrity, confidentiality, or availability (technical or sociotechnical). These attacks can range from hacking and denial-of-service (DoS) attacks to ransomware and spyware

infections, and they can affect anybody from the public to a country's national infrastructure system [3].

Why cyberattacks flourish? Cyberattacks become more attractive and potentially more disastrous as our dependence on information technology increases. Cyberattacks are cheaper, convenient, and less risky than physical attacks [4]. Aside from a computer and Internet connection, cybercriminals only require a few expenses. They are not bound by distance, and they are tough to perceive and prosecute due to the anonymous nature of the Internet. Because cyberattacks against information technology are highly attractive, it is expected that the number, diversity, and sophistication of cyberattacks will continue to rise throughout the years [5].

2 Main threats

In the past years, we have seen a substantial increase in cyber criminality in the form of high-profile ransomware campaigns. Breaches leaked personal data on a massive scale leaving victims vulnerable to fraud. Cybercriminal's tactics are changing as businesses are being targeted rather than individuals, and while phishing attacks on individuals are on the rise, fewer are falling victim as people have become more aware [6].

2.1 Social engineering

Social engineering is a form of cybercrime that involves the use of deceit or trickery to persuade individuals into performing some unauthorized, unlawful, or illegal action. It seeks to exploit and take advantage of human psychology and is arguably the most effective way of committing a crime against an individual [15]. Phishing attacks are perhaps the most well-known, in which unsuspecting users are encouraged to click on a faulty link, enabling hackers to install malware and consequently gain access to the system. In all circumstances, social engineering assaults combine social interactions with technology exploitation, making it challenging for cybersecurity specialists in businesses and government organizations to build effective countermeasures [29].

2.2 Data breaches

Data breaches occur when sensitive, protected, or confidential information is copied transmitted, viewed, stolen, or utilized by an unauthorized individual to do so. According to the Identity Theft Resource Center, a recognized non-profit organization established to support victims of identity crime, released its United States of America data breach findings for the third quarter of 2021. For this period of time, the number of data compromise victims (160 million) is higher than the first and second quarter of 2021 combined (121 million) [7].

Not only data breaches, but unprotected cloud databases are to blame for the significant increase in victims. In addition, year-to-date (YTD), the overall number of

cyberattack-related data compromises is up 27% from 2020. Phishing and ransomware remain, by far, the most common threat vectors [7].

2.3 Internet of things

With the growing number of devices connected to the Internet, it is highly likely that we will see more attackers using the Internet of Things (IoT) to commit crimes. Many internet-connected devices sold to consumers lack basic cybersecurity provisions. With countless unsecured devices, vulnerabilities will continue to be exploited and used for activities (such as DDoS attacks) without the user's knowledge [6].

2.4 Cloud security

These days, small, medium, and large businesses are gradually adopting cloud services. In other words, the world is slowly moving towards the clouds. This latest trend poses a huge challenge for cybersecurity, as traffic bypasses traditional points of inspection [8]. Only 40% of all data stored in the cloud is access secured, although most companies report they are concerned about encryption and security of data in the cloud [6]. This increased use of cloud technology to store sensitive information will continue to tempt cyberattackers.

2.5 Crypto jacking

Cryptocurrency has been gaining increased popularity over the last years and with its interest still strong, it opened an opportunity for cybercriminals to exploit. Crypto jacking - where an individual's computer processing power is used to mine cryptocurrency without the user's consent - will likely become a regular source of revenue for criminals [7]. Popular websites are expected to continue to be compromised, offering crypto mining malware to users, and software that, when executed in a web page, mines digital currency using the visitor's spare computer processing power [6].

3 The impact of cyberattacks

According to research, people are more inclined to react to the consequences of a cyberattack than to the attack itself [9] [10]. One example is a cyberattack in which malware infects a national power plant, knocking out power to hundreds of thousands of people. Individuals will be more concerned about the effect of the attack, i.e., being without power, thus having no warmth or ability to prepare food [11].

There are two key areas of impact studies aim to consider and provide an overview about based on the current research and thinking. These are the social and psychological (emotional and behavioral) impacts. The social impact of a cyberattack includes aspects such as the social disruption it causes in people's daily lives, as well as more widespread issues like anxiety or a lack of confidence in technology. Psychological

impact can include more personal aspects such as an individual's anxiety, worry, anger, outrage, depression and so on [11].

3.1 Emotional reactions to cybercrime

The psychological impacts of cyberattacks may even resemble those of traditional terrorism, depending on who the attackers and victims are [12]. Victims of cybercrime and internet attacks may experience emotional stress, which can lead to depression. There is also some evidence of Acute Stress Disorder (ASD) symptoms in victims of online attacks, such as anecdotal tales of intrusive memories, emotional numbing, and upset from virtual sexual assault victims [13].

The emotional impact of identity theft, for example, might cause a victim to become agitated and leave them feeling violated, deceived, vulnerable, angry, and powerless [14]. Victimization frequently causes outrage, worry, a desire for protection over liberty, and a lack of interest in embracing new technology due to a loss of trust in cyberspace. The sufferer may go through stages of grief, anger, or rage. Victims may even blame themselves and develop a sense of guilt in some circumstances; sextortion is a great example of this because of how it begins [15].

3.2 Learned helplessness

According to the findings, only about one-tenth of people (9%) feel "very" safe online. In addition, only half of the respondents polled (51%) said they would change their internet behavior if they were a victim [16]. These findings show that, people might accept a certain situation, even if it feels unpleasant just because they cannot understand the reasoning and the process behind it. Following this point, one might argue that persons may accept cyberattacks because of a sense of 'learned helplessness' [11].

Users may simply accept the risk of being victims due to a sense of learned helplessness and a lack of understanding about online attacks and how to settle an incident. Indirectly, the key question becomes whether people accept the reality of repercussions while hoping for a low severity.

Nowadays, where the average user is required to make many security-related decisions, putting him under pressure and sometimes causing anxiety. These behaviors include:

- not opening emails from a sender they do not recognize;
- not accessing unknown attachments;
- only downloading and running programs from trustworthy sources;
- the use of anti-virus software and security software (e.g., firewall);
- creating regular backups.

Due to a lack of awareness about the potential consequences of making poor selections, some of these options can generate anxiety in the user. Even when individuals are aware of the online threats, they may not always understand them. Due to the public's lack of awareness of cyberthreats and security measures, there may be a lack of public engagement with security issues and a general loss of trust in technology.

This also has been seen in the domain of information privacy in the context of new forms of technology, where some users now consider privacy as ‘the boring bit’ [17].

3.3 Cyberattack related variables

A variety of cyber-specific elements, such as the attacker's identity, the target's identity, the magnitude of the assault, as well as government awareness of a cyberattack and the timing of disclosure of a harmful event, influence the public reaction to a cyberattack [11].

Terrorists, hacktivists, and criminals are the three main types of actors, all of whom are capable of initiating assaults that may be considered severe public concerns [18]. Criminals are less likely to expose their true identify (assuming any identity, pseudonym or otherwise) in public since anonymity allows them to operate more freely [11]. Furthermore, the identity of the target might influence public reaction.

4 Hacker’s profiling and motivations

With scientists, practitioners, the public, and even hackers themselves debating what constitutes “hacking”, who qualifies as a hacker, and their motivations for committing such crimes, hacking has become a contested topic. The definition of hacking as well as its meaning, have evolved over time, influencing how hackers are portrayed [19].

Hacking is the attempt, whether successful or unsuccessful, of exploiting computer and network vulnerabilities and consequently, to obtain unauthorized usage or access to a computer system [20].

4.1 Black Hat Hackers, White Hat Hackers and Grey Hat Hackers

Originally, the term "hacker" was used to describe exceptional and radical programmers in the field of computer science, gifted with “innovation, style and technical virtuosity” [20].

A clear difference is made within the computer security community between black hat hackers who exploit computer systems to cause harm or profit for themselves and white hat hackers who exploit computer systems to proactively uncover vulnerabilities that may be patched. Black hat trolls would typically be using forms of engagement that are not prescribed by the designer of the system and white hat trolls would be looking for ways to disable forms of non-prescribed engagement through research and education [21].

On the other hand, grey hat hackers operate in non-prescribed ways but are driven by a sense of public good rather than a desire to harm or earn personal advantage. They may see their acts as a method to show attack surfaces and put pressure on gatekeepers to improve their systems, or as a sort of "hacktivism" that exploits a system's weaknesses to advance a higher-order purpose of campaigning for human rights or "human security" [21].

Penetration testing, security research, and vulnerability disclosure may all be done by white hat and grey hat hackers. They might also take action by identifying negative actors, their motivations, and their tactics [21].

Furthermore, white hat and grey hat hackers may actively "troll back" or "troll the trolls", the black hat hackers, to counteract negative behavior.

4.2 Quantifying hacker motivations

Internal and external perpetrators have different motives and methods for accessing company data. External perpetrators or hackers are more skilled, organized, and innovative. Therefore, the data breach type depends on the perpetrator, their intentions, and the source of the threat [22]. The source is important because outsider activities will be more dangerous than those from the inside [23].

Due to the difficulty to reach out to hackers, to better understand their motivations, the following section relies on studies previously conducted. Although most literature that reports upon hackers' motivations merely explains which motivations can be deduced from the behaviors and interviews with hackers, these studies managed to shed some light on the differential importance attributed to motivations to hack and what vulnerabilities are being exploited to do so.

Thycotic Software Ltd (2018)

At Black Hat Conference, August 4-9, 2018, Thycotic Software Ltd conducted a survey of hackers to get their perspectives on vulnerabilities and attack vectors they find easiest to exploit.

With nearly 70% of 300+ poll respondents identifying as "White Hat Hackers," the study reveals a sizable proportion of participants committed to helping companies and organizations stay safe by exposing their most reliable exploits for IT systems. However, 30% of hacker participants anonymously acknowledged to possibly breaching the law in their hacking activities. Only 5% of those polled classified themselves as pure "Black Hat Hackers," who seek to breach networks for malevolent or personal gain [24].

The survey results were quite interesting, revealing some hacker's preferences when it comes to most attacked operating systems, the fastest means to get access to privileged accounts and the risky behaviors they exploited most often to access networks.

Despite Microsoft's efforts to increase cybersecurity, half of hackers said they were able to easily compromise both Windows 10 and Windows 8 in the year of 2017. Operating systems are only as safe as the people who use them and the configurations they have applied. Knowing that user account breach is almost certain, businesses should adopt a "zero-trust" policy that emphasizes least privilege to prevent over privileged accounts that offer hackers unrestricted access [24].

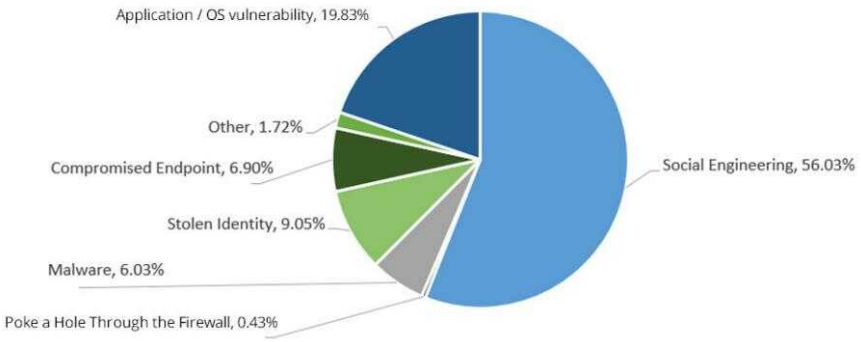


Fig. 1. Thycotic Black Hat 2018 Hacker Survey Report - "Which OS did you conquer the most in the past 12 months?" [24]

Once an attacker gains network access they can learn more about what software is being used, what patches are being deployed, when vulnerability scans are run, which systems and accounts have privileged access and how they can avoid detection. Vulnerabilities in applications and operating systems continue to be a major issue, with nearly 20% of hackers attacking unpatched systems. Identity theft is used by 10% of hackers to get network access, whereas malware and stolen endpoints are used by fewer than 7% [24].

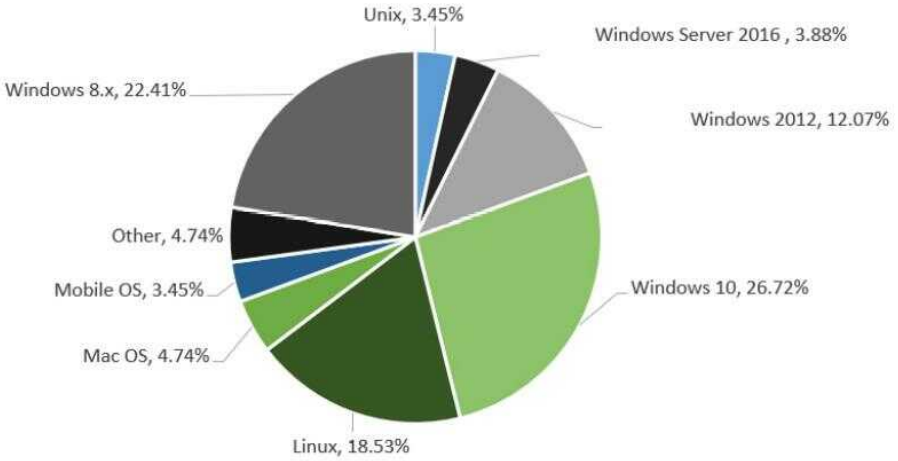


Fig. 2. Thycotic Black Hat 2018 Hacker Survey Report - "What's the fastest way for you to get onto a network to access privileged accounts?" [24]

Thycotic asked hackers to reveal an organization's most serious behavior-based security vulnerabilities — the ones they use the most to gain access to networks. Hackers revealed that half of their attacks discovered employees reusing passwords that had previously been compromised in past data breaches, allowing hackers easy access to the network. These findings demonstrate that employees suffer with poor password hygiene on a regular basis. Once hijacked, these end user accounts give hackers with an easy way to escalate privileges [24].

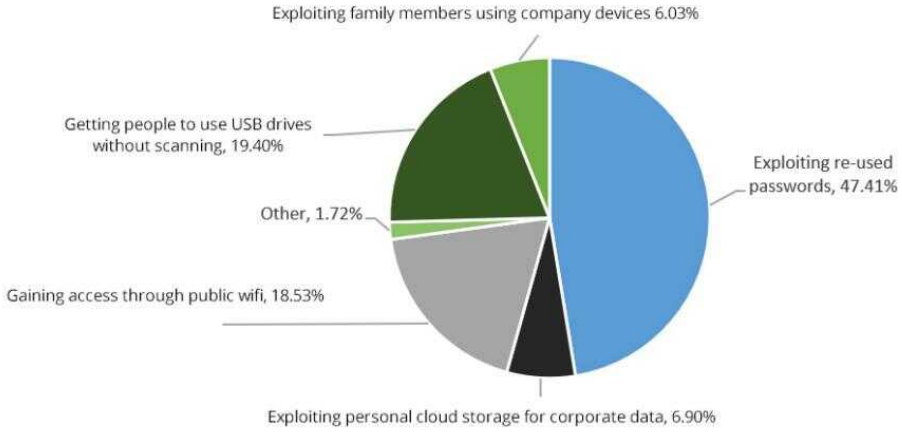


Fig. 3. Thycotic Black Hat 2018 Hacker Survey Report - "What risky behavior do you exploit the most?" [24]

Woo, Kim and Dominick (2009)

By analyzing the content of 462 defaced online pages in the English language, Woo, Kim, and Dominick investigated the motivations of hackers who defaced web pages. The motivations were categorized into two groups.

First, 'militant' impulses were confrontational and manifested as anti-outgroup reactions. More specifically, content was labelled militant when it alluded to nationalism, ethnicity, and religion, which were observed in 18% web pages examined and, the freedom of information and the prohibition of pornography were observed in 5% of the web pages examined [25].

"Pranking" motivations make up the second group. Prankster statements were found on 71% of the web sites examined. These statements brag about the hacker's abilities and skills (8%), impressing a romantic partner (2%), leaving a sign (24%) (e.g., "you were hacked by…"), or disparage the system administrator (4%) [25].

Goode and Cruise (2006)

Goode and Cruise examined the motivations of 28 software crackers by conducting an online survey. According to the results of this survey, the crackers were largely motivated by stimulation values. One of the most popular justifications was ‘personal challenge’. At the same time, crackers stated that they would even crack if they would have to do it anonymously and solitary. Peer recognition, as well as monetary incentives, were not considered major motivators [26].

In a similar vein, crackers indicated they were neither motivated by public demand nor by personal need. Open-ended questions, on the other hand, revealed that crackers were aware that they were admired by others, but they disagreed on whether consumers of cracked software owed them gratitude [26].

Turgeman-Goldschmidt (2005)

Turgeman-Goldschmidt arranged the accounts reported by the 54 hackers he interviewed from the most to the least mentioned. Besides motivations to hack, he also noted factors that might persuade people to refrain from hacking and excuses, or justifications, to hack [27].

Only the reported motivations are considered in this study. Fun, thrill, and excitement are the most cited motivations, followed by curiosity, computer virtuosity, economic considerations, nosy curiosity, voyeurism, and revenge [27].

Fötinger and Ziegler (2004)

Fötinger and Ziegler analysed the intents of 599 people who had committed identity theft using data acquired through a questionnaire administered by the German Federal Bureau of Criminal Investigation (Bundeskriminalamt, BKA). Perpetrators who broke into the victims' computers exposed personal data relating to their internet accounts on online forums. As a result of the stolen data, others were able to access the internet at the expense of the victims, resulting in identity theft. Only six of the 599 respondents admitted to trespassing on victims’ computers. None of the six people, however, admitted to posting the account information on the internet. As a result, the following results are based on responses from respondents who simply used 'publicly available' stolen details [28].

The two most frequently chosen drivers were: economic reasons (51.3%) and trial and error (33.1%). Among the less cited motivations (< 3%) were: fooling around, acceptance of the group, and competition [28].

5 Conclusion

In a world where cybercrime and malicious actions are as common as the sunrise, people substantially benefit in understanding more about the possible dangers of such useful tools as the Internet and technological devices. Human behavior is and will continue to be the source of many crimes. Taking advantage of one's ingenuity or lack of understanding on the topic will result in someone exploiting a service, blackmailing, extorting, or stealing someone's identity.

Considering the vast bulk of the aspects examined in this paper, we can conclude that the stream of crime is indeed increasing at a steady pace, either through the creation of new exploits, the use of misinformed people, poorly configured systems, outdated software, and the most common of all, human behavior, which leads to other types of threats such as extortion and blackmailing.

Nevertheless, not all is terrible, as organizations like INTERPOL and EUROPOL continue to move ahead and create methods to offer tools to start preventing most crimes, as well as national police forces throughout the globe being authorized to establish a unit to battle these dangers and respond faster and more efficiently.

It is essential to spread awareness as much as possible in order to continue preventing and minimizing damage. Reducing the amount of privacy violations and thefts must be a top priority; the data and statistics show that if nothing is done, more crimes will be committed.

References

1. Arora, B.: Exploring and analyzing internet crimes and their behaviours. Perspectives in Science. 8, 540–542 (2016).
2. Jain, N., Shrivastava, V.: Cyber crime changing everything – an empirical study. International Journal of Computer Application. 1, (2014). //reference incomplete
3. Nurse, J. R. C. Cybercrime and You: How Criminals Attack and the Human Factors that They Seek to Exploit. (2018)
4. M3AAWG, http://www.maawg.org/, last accessed December 10, 2021
5. Jang-Jaccard, J., Nepal, S.: A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences. 80, 973–993 (2014).
6. The cyber threat to UK business, https://www.ncsc.gov.uk/report/cyber-threat-uk-business last accessed December 1, 2021
7. Achten, A.: Identity Theft Resource Center to share latest Data Breach Analysis with U.S. Senate Commerce Committee; number of data breaches in 2021 surpasses all of 2020, https://www.idtheftcenter.org/identity-theft-resource-center-to-share-latest-data-breach-

analysis-with-u-s-senate-commerce-committee-number-of-data-breaches-in-2021-surpasses-all-of-2020/.
8. Reddy, G.N., Reddy, G.J.U.: A study of cybersecurity challenges and its emerging trends on latest technologies. International Journal of Engineering and Technology. 5, (2018).
9. Minei, E., Matusitz, J.: Cyberterrorist messages and their effects on targets: A qualitative analysis. Journal of Human Behavior in the Social Environment. 21, 995–1019 (2011).
10. Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., Laplante, P.: Dimensions of cyber-attacks: Cultural, social, economic, and political. IEEE Technology and Society Magazine. 30, 28–38 (2011).
11. Bada, M., Nurse, J.R.C.: The social and psychological impact of cyberattacks. Emerging Cyber Threats and Cognitive Vulnerabilities. 73–92 (2020).
12. Gross, M.L., Canetti, D., Vashdi, D.R.: The psychological effects of cyber terrorism. Bulletin of the Atomic Scientists. 72, 284–291 (2016).
13. Virtual rape is traumatic, but is it a crime?, https://www.wired.com/2007/05/sexdrive-0504/.
14. Kirwan, G., Power, A.: The Psychology of Cyber Crime. Advances in Digital Crime, Forensics, and Cyber Terrorism. (2012).
15. Nurse, J.R.: Cybercrime and you: How criminals attack and the human factors that they seek to exploit. The Oxford Handbook of Cyberpsychology. 662–690 (2018).
16. Norton's Cybercrime Report: The human impact reveals global cybercrime epidemic and our hidden hypocrisy, https://community.norton.com/en/blogs/symantec-cyber-education/norton%E2%80%99s-cybercrime-report-human-impact-reveals-global-cybercrime.
17. Williams, M., Nurse, J.R., Creese, S.: Privacy is the boring bit: User Perceptions and Behaviour in the Internet-of-Things. 2017 15th Annual Conference on Privacy, Security and Trust (PST). (2017).
18. Nurse, J.R., Bada, M.: The group element of cybercrime: Types, dynamics, and criminal operations. The Oxford Handbook of Cyberpsychology. 690–715 (2018).
19. Madarie, R.: Hackers' Motivations: Testing Schwartz's Theory of Motivational Types of Values in a Sample of Hackers. International Journal of Cyber Criminology. 11, (2017).
20. Sharma, R.: Peeping into a hacker's mind: Can criminological theories explain hacking? SSRN Electronic Journal. (2007).
21. Matthews, J., Goerzen, M.: Black hat trolling, white hat trolling, and hacking the attention landscape. Companion Proceedings of The 2019 World Wide Web Conference. (2019).
22. Juma'h, A.H., Alnsour, Y.: The effect of data breaches on company performance. International Journal of Accounting & Information Management. 28, 275–301 (2020).
23. Jouini, M., Rabai, L.B., Aissa, A.B.: Classification of Security Threats in Information Systems. Procedia Computer Science. 32, 489–496 (2014).
24. Thycotic Black Hat 2018 Hacker Survey Report, https://hosteddocs.emediausa.com/Thycotic-q4-18-2018-Black-Hat-Report.pdf.
25. Woo, H., Kim, Y., Dominick, J.: Hackers: Militants or Merry Pranksters? A content analysis of defaced web pages. Media Psychology. 6, 63–82 (2004).
26. Goode, S., Cruise, S.: What motivates software crackers? Journal of Business Ethics. 65, 173–201 (2006).
27. Turgeman-Goldschmidt, O.: Hackers' accounts hacking as a social entertainment. Social Science Computer Review. 23, 8–23 (2005).
28. Fötinger, C., Ziegler, W.: Understanding a hacker's mind - A psychological insight into the hijacking of identities. 1–48 (2004).

29. Klimburg-Witjes, N., Wentland, A.: Hacking humans? Social Engineering and the construction of the “deficient user” in cybersecurity discourses. Science, Technology, & Human Values. 46, 1316–1339 (2021).
30. Benson, V.: Emerging cyber threats and cognitive vulnerabilities. Academic Press (2020).

Cybercrime Warfare Against People: Pessimistic Side of Online

João Conceição

[1]Universidade Lusófona do Porto, 4000-098 Porto, Portugal
joaodiogocosta@hotmail.com

Abstract. The Internet and its inherent liberating properties, allow people to indulge in their imagination and do things that otherwise would not be possible, including deviating, perverse and dangerous activities.
Cybercrime is a term used to describe criminal activities involving a computer, networked device, or a network, and it can be done not only to companies and institutions but also to individuals.
Even though cybercrime constitutes nowadays one of the biggest threats for financial markets, it's undervalued by a numerous amount of the institutions, with studies showing that the efficacy and recurrence of these attacks do not seem to be decreasing, even with all the awareness being done by cybersecurity institutions.
There are various types of cybercrime, and an abundant share of them include social engineering, which is the art of manipulating and persuading an individual to reveal confidential information, so, by understanding not only the mechanisms behind these attacks, but equally important, the psychological factors as to why people still fall for these attacks, a list of preventive measures can be developed to hopefully guide people in this cybercrime warfare.

Keywords: Internet, Cybercrime, Psychological, Social Engineering, Confidential, Preventive Measures, Awareness, Crimes

1 Introduction

The usage of the Internet became in the last couple of years so ingrained in society, that almost every industry and field of work adapted their way of conducting and superintending businesses to accommodate and take advantage of the potential a vast network that connects people all over the world can offer [1].

Although the Internet is nowadays used by everyone, its concept is still vague for the vast majority of people. For some individuals the Internet is used for entertainment purposes, for others constitutes a source of information and learning, but for almost everyone, remains something mysterious, incomprehensible and for those who know what truly can be accomplished with a networked system like this, frightening.
With the growth of the Internet, emerged the possibility of committing crimes digitally. Crime and those who practice it, evolved in order to obtain the most out of their surroundings. Before the post-modern age, all the material assets were possessed in physical form and therefore the crimes committed, involved most of the time the threat of violence and physical force. These methods carried greater risks to those who committed them, as the perpetrators were frequently caught in the act and therefore arrested.

With the digitization of people's owned assets and information, criminals no longer need to reveal their identity as everything can be made anonymously [2], also the act of Social Engineering became much more accessible as a consequence of the multitude of methods there is to persuade and to reach people, such as emails, links, advertisements and blackmail threat [3].

2 Cyberattack Methods and Motivations

Prior to examining and understanding the different types of cyberattacks and possible mitigation/awareness techniques, we need to understand how these attacks are being done, why are they being done and lastly why are people falling for them, as people represent the not only the biggest direct threat to computing infrastructures since the attacks are being committed by people themselves, but also the biggest flaw when it comes to protecting these systems due to their vulnerability to psychological manipulation.

2.1 Social Engineering

Social Engineering is without a doubt the one of the main culprits behind this warfare as 99% of all cyberattacks use social engineering techniques [4]. This simple, yet extremely effective method explores the vulnerabilities of the human mind by strategically persuading one, using most of the times the promise of something as all human activity is prompted by desire [5]. There are various ways of schematizing the process of Social Engineering, but the most common model is Kevin Mitnick's social engineering attack cycle [6].

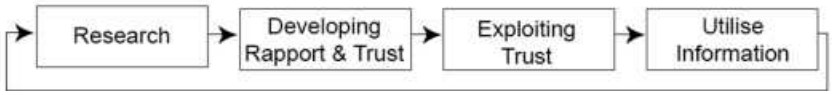


Figure 1. Kevin Mitnick's social engineering attack cycle model[6]

This model divides the process of Social Engineering in 4 parts:

Research. In this phase the attacker will try to gather as much information as he can about his target, this includes the victim's tendencies and vulnerabilities so that he can personalize his attack to his specific victim or victims.

Developing Rapport & Trust. In order to obtain information that in normal circumstances would be unobtainable, the attacker must develop a relationship with the victim, this is usually done with information gathered in the Research phase, for example, if the attacker knows that the victim likes animals and usually donates to animal shelter institutions, then he can impersonate someone from these institutions, giving a false sense of security to the victim.

Exploiting Trust. After developing a 'trustful' relationship with his victim, he can now lure her into giving away personal information or valuable assets.

Utilize information. Finally, with the information gathered, the attacker can now proceed with his attack without needing to interact with its victim any longer, and ultimately reaching his initial goal.

2.2 Types of hackers and their motivation

When we think of a cyberattack, we immediately think of something negative, with the name "cyberattack" in itself having a pejorative connotation, but this is not always the case. Frequently, the means and intentions of an attack are indeed wrong, but in some cases the intentions behind an attack are morally correct. With this being said, we can divide hackers and their ethical reasoning by using the "hat" terminology.

Figure 2. Scheme with the different type of hats[17]

White Hat Hackers. Hackers who "wear" the "white hat" constitute in their current field of activity, the group of hackers that are driven either by positive ethical motivations by their compromise with another company or institution to do the right type of attacks. One particular aspect to note is that, a considerable amount of these

hackers, especially those who work for a company or an institution, were once black hat or grey hat hackers, but were persuaded by these companies to use their expertise in exchange for money or some other type of extrinsic value asset, an example of this is Hector Xavier Monsegur, that worked with the FBI to help prevent and disrupt over 300 hacks in exchange for being released from prison[7].

Grey Hat Hackers. When it comes to Grey Hat Hackers, as with the mixture of both the black and white color, they behave with both white and black hat hacker tendencies, unlike black hat hackers their intentions are usually morally correct, but their means are usually unethical, an example of this, is a hacker who breaches a company network system without their permission, but then reports it to the company in order for them to fix their security flaws.

Black Hat Hackers. Black Hat Hackers are the ones we are going to target our focus to in this paper, they are the polar opposite of White Hat Hackers in the sense that, not only are their means of hacking into a system unethical, but so are their intentions, as they can release malware into a system, steal or hold someone's files and information by ransoming them. An example of a Black Hat Hacker is Kevin Mitnick, who was once the most wanted cybercriminal in the world having stolen millions of dollars from multiple companies. He was later convicted and eventually became a consultant and a writer (White Hat Hacker) [8].

Blue Hat Hackers. Blue Hat Hackers are security professionals whom companies and institutions often invite to check for vulnerabilities in their system.

Green Hat Hackers. Green Hat Hackers are seen as the "newbies" of the hacking community. They're still very much oblivious when it comes to the consequences of their actions, and therefore considered dangerous.

Red Hat Hackers. Just like white hat hackers, red hat hackers also have morally correct intentions in the attacks they commit, but contrary to white hat hackers, the routes they use are usually illegal, that's why they are often referred as the "Robin Hood" of hackers.

3 Cybercrime types, data and preventive measures

According to estimates from Cybersecurity Ventures, it is estimated that attacks like Ransomware happen every 11 seconds, and that across 10 countries, 330 million people have been victims of cybercrime in 2020 [9], with less than 0.05% hackers getting caught and convicted, that results in about 314 million cybercrime attacks made in 2020 in which the attacker was never caught, furthermore, a considerably high amount of cyberattacks aren't reported. It is also important to note that, when it

comes to cybercrime, there are serious jurisdiction issues, as in some cases law enforcement gather sufficient evidence about the perpetrator, but then lack the legal permission to arrest him.

To support the data evaluated in the next topics, a computer questionnaire was conducted by me, João Conceição and João Sebe. The survey was answered by 253 respondents of all ages and genders that use or have used a networked device at some point in their lives. The questionnaire included questions regarding the amount of effort the respondents put on security measures, the types of attacks they suffered and the preventive measures they adopted after such attacks.

3.1 Most common types of attacks

There's a multitude of types of cyberattacks, however some are much more prevalent and/or targeted to a specific demographic. According to the FBI's Internet Complaint Center (IC3) reports, there has been a significant increase in specific types of cyberattacks in the last couple of years [10], this is believed to be caused by the COVID-19 pandemic outbreak, where hackers have personalized their way of committing these crimes in order to obtain the most out of the current situation.

By Victim Count			
Crime Type	**Victims**	**Crime Type**	**Victims**
Phishing/Vishing/Smishing/Pharming	241,342	Other	10,372
Non-Payment/Non-Delivery	108,869	Investment	8,788
Extortion	76,741	Lottery/Sweepstakes/Inheritance	8,501
Personal Data Breach	45,330	IPR/Copyright and Counterfeit	4,213
Identity Theft	43,330	Crimes Against Children	3,202
Spoofing	28,218	Corporate Data Breach	2,794
Misrepresentation	24,276	Ransomware	2,474
Confidence Fraud/Romance	23,751	Denial of Service/TDoS	2,018
Harassment/Threats of Violence	20,604	Malware/Scareware/Virus	1,423
BEC/EAC	19,369	Health Care Related	1,383
Credit Card Fraud	17,614	Civil Matter	968
Employment	16,879	Re-shipping	883
Tech Support	15,421	Charity	659
Real Estate/Rental	13,638	Gambling	391
Advanced Fee	13,020	Terrorism	65
Government Impersonation	12,827	Hacktivist	52
Overpayment	10,988		

Figure 3. Most reported cyberattacks to the IC3[10]

As we can verify, Phishing/Vishing/Smishing/Pharming stands out from the ot cyberattacks when it comes to the victim count, with an increase of occurrences over 12 times in the last 5 years [11]. Non-Payment/Non-Delivery and Extortion also experienced significant increases of cases reported in the last 5 years.

Survey Analysis. From the 253 respondents, 52 (20.6%) suffered from a cyberattack at some point of their lives, with the most common one being, Phishing/Vishing/Smishing/Pharming as expected (48.1%) followed by Harassment/Threats of violence (36.5%) and then Non-Payment/Non-Delivery (38.5%).

Note that the respondents could submit multiple answers, therefore the percentages don't add up to 100%

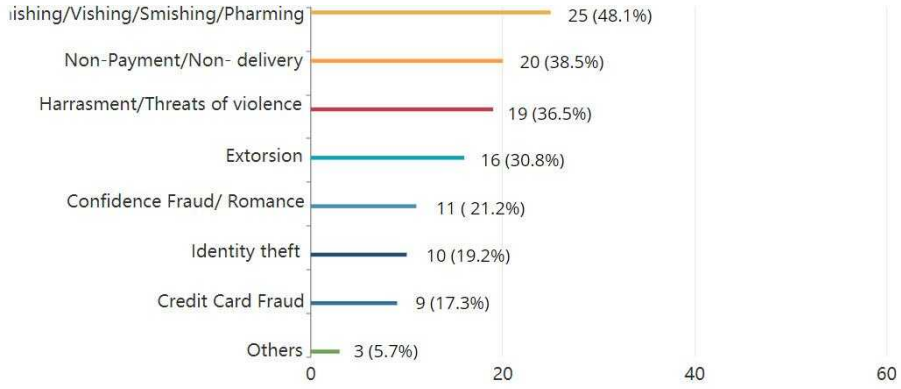


Figure 4. Most common cyberattacks according to the executed survey

As expected, Phishing/Vishing/Smishing/Pharming remained the most common cybercrime in the studied demographic, reinforcing the danger that this specific social-engineering act constitutes not only to individuals but also institutions and companies.

3.2 Cybercrime's financial damage and main targets

Cybercrime's industry seems to be growing each year without signs of stopping, the financial damages caused by cyberattacks are predicted to total $6 trillion USD globally in 2021, to put this in perspective, if cybercrime was a country, it would be the third-largest economy after the U.S. and China [12].

When it comes to attacks on individuals, security firm Norton estimates that in 2017 the total losses added up to $172 billion from 978 million people in 20 countries [13], moreover, last year according to the FBI's 2020 Internet Crime Report, the total losses in the US surpassed $4.2 billion, with approximately 43% of those losses ($1.8 billion) being from victims who were 50 years or more [11]. This statistic becomes even more worrying, when u consider that the percentage of people that are 50 years or older using technological devices is much lower than those who are under 50 years. The reason for this demographic preference is mostly due

to the fact that older people are generally less informed about the danger of using the Internet, and therefore more ingenuous when it comes to these attacks, but also due to the fact that they generally possess more financial resources[14].

The following scheme indicates the total losses in each of the 20 countries, represented in billions (USD).

	Australia	Brazil	Canada	China	France	Germany	Hong Kong	India	Indonesia	Italy	Japan	Mexico	Netherlands	New Zealand	Singapore	Spain	Sweden	UAE	UK	USA
2017	$1.9	$22.5	$1.5	$66.3	$7.1	$2.6	$0.1	$18.5	$3.2	$4.1	$2.1	$7.7	$1.6	$0.1	$0.4	$2.1	$3.9	$1.1	$6.0	$19.4

Figure 5. Estimated losses for each of the 20 countries (Billions)[11]

This following scheme indicates the total victim losses for each type of cyberattack according to the IC3[11].

By Victim Loss

Crime Type	Loss	Crime Type	Loss
BEC/EAC	$1,866,642,107	Overpayment	$51,039,922
Confidence Fraud/Romance	$600,249,821	Ransomware	**$29,157,405
Investment	$336,469,000	Health Care Related	$29,042,515
Non-Payment/Non-Delivery	$265,011,249	Civil Matter	$24,915,958
Identity Theft	$219,484,699	Misrepresentation	$19,707,242
Spoofing	$216,513,728	Malware/Scareware/Virus	$6,904,054
Real Estate/Rental	$213,196,082	Harassment/Threats Violence	$6,547,449
Personal Data Breach	$194,473,055	IPR/Copyright/Counterfeit	$5,910,617
Tech Support	$146,477,709	Charity	$4,428,766
Credit Card Fraud	$129,820,792	Gambling	$3,961,508
Corporate Data Breach	$128,916,648	Re-shipping	$3,095,265
Government Impersonation	$109,938,030	Crimes Against Children	$660,044
Other	$101,523,082	Denial of Service/TDos	$512,127
Advanced Fee	$83,215,405	Hacktivist	$50
Extortion	$70,935,939	Terrorism	$0
Employment	$62,314,015		
Lottery/Sweepstakes/Inheritance	$61,111,319		
Phishing/Vishing/Smishing/Pharming	$54,241,075		

Figure 6. Estimated victim losses for each type of cybercrime[11]

Survey Analysis. From the 253 respondents, 52 (20.6%) suffered from a cyberattack, surprisingly enough, from those 52 people only 3(5.8%) were from people aged 50 years or older, therefore, this means that according to the survey, respondents that were under 50 years suffered 16.3 times more cyberattacks then those who are 50 years or older. But if we already established that the older demographic is much more vulnerable to cyberattacks, why does the survey tell us otherwise?

Possible reasons:

- The amount of time spent on networked devices is much lower on the senior demographic.

- Due to their naivety in the field, they might not realize when they suffer from a cyberattack.

It is also important to note that from these 3 people, all of them (100%) reported financial losses when they suffered from a cyberattack.

Note that the respondents could submit multiple answers, therefore the percentages don't add up to 100%

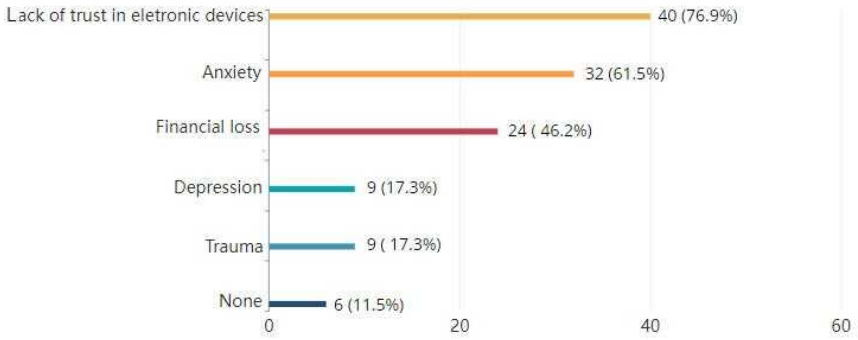


Figure 7. Consequences of the occurred cyberattack in the life of the respondents

3.3 Preventive measures

While it remains almost impossible to stop hacking attempts, we can preemptively adopt ways of conducting our internet usage so that those attempts never become successful, moreover we need to raise awareness to the dangers of conducting improper usage of personal/workstation devices by establishing the biggest telltale signs of a potential cyberattack attempt.

From the infinitude of ways to perform a cyberattack, the following list identifies the more commonly used methods to install malware into your devices and/or obtain access to personal information:

Email Phishing. 96% of all phishing attacks derive from fraudulent emails [15], with 1 in every 4200 emails corresponding to a phishing email [16]. These emails tend to mimic known banking or social media companies, and often claim there is a

problem with your account to incite you to click on a specific link or to share personal information.

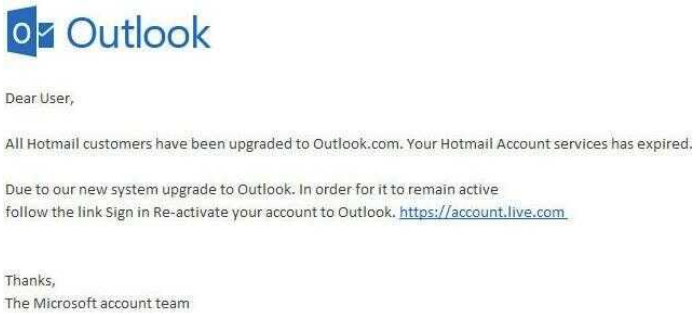


Figure 8. Email Phishing example

Email Phishing preventive measures:

- Never open links from emails you don't know or from companies you don't have an account on.
- If you have an account on the claimed company but you remain unsure whether it's safe or not, contact the company using a phone number or a website you know it's real.
- Check for grammatical errors in the email's content.

Website spoofing. Just like emails, websites can also try to impersonate known companies. This is especially common in online banking services, where the insertion of bank account information is common.

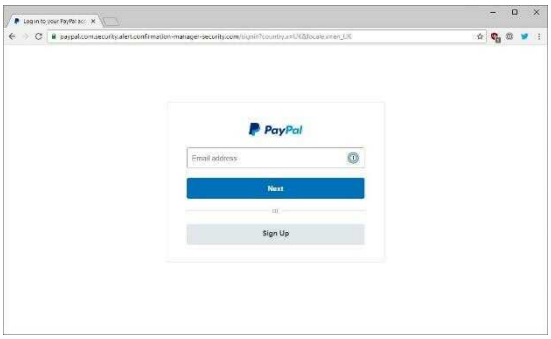


Figure 9. Website spoofing example

10

Website spoofing preventive measures:

- Check for suspicious patterns in the website's address. Usually when a website is trying to impersonate a legitimate company, it will have a very similar address but with slight changes.

- With the introduction of free SSL services, the green lock icon present in the search bar doesn't indicate the website is safe any longer, therefore, you should also check the certificate properties to verify the issuer legitimacy.

- Verify if softwares used to autofill login credentials work on the website you are trying to access, as these usually don't work on spoofed websites.

Malicious ads and pop-ups. Some websites are full of ads and pop-ups with sensationalist messages and images, that are strategically placed so you must press over them to access the website's functionalities. An example of this are invisible ads and pop-ups that are placed over a video player in free movie streaming websites. While most of these ads and pop-ups have the sole purpose of generating revenue, some can install malware into your computer or mobile device.

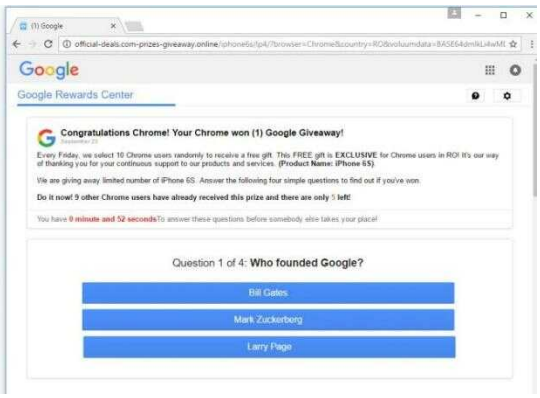


Figure 10. Malicious advertisement example

Malicious ads and pop-ups preventive measures:

- Avoid visiting suspicious websites altogether, as these are the one who usually contain malicious ads and pop-ups.

- On the Internet, general rule of thumb is, if it's too good to be true, then it probably is. Never click on something that claims u have won something.

- Use a trusted ad-blocking extension in your browser, which as the name suggests, blocks ads from showing up on your screen.

Survey Analysis. Having identified the most common ways a cyberattack can be made, and some preventive measures for each one of them, a few questions regarding the security measures people use and the willingness to add new ones were asked in the survey.

According to the retrieved data, from the 253 respondents, 64 (25.3%) believe their personal information is properly secured, 81 (32%) say they don't know and 108 (42.7%) say they don't think their personal information is safe from cyberattacks, conversely, 243 (96%) respondents said they feel like they could improve their security measures, however 169 (66.8%) consider the means to implement more advanced security measures inconvenient.

*Figure 11. Pie Chart 1**

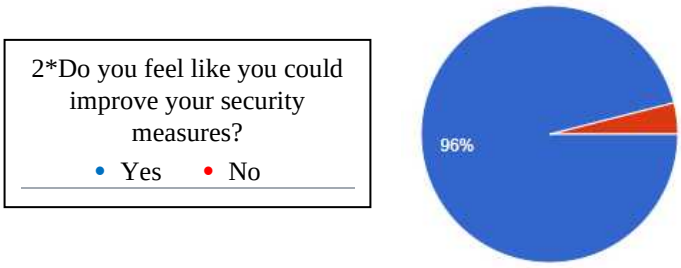


*Figure 12. Pie Chart 2**

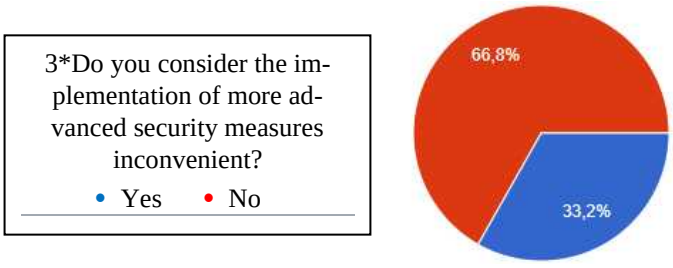


*Figure 13. Pie Chart 3**

4 Conclusion

The catastrophic effects of cybercrime were substantiated in this paper, eventuating not only massive financial losses to those who suffer from it, but also causing deaths. While the issue itself reached a point where full containment became impossible, we can work towards limiting the effects it has on people, moreover, Awareness must be made, especially to more vulnerable and less informed demographics. By decreasing the number of losses and consequently, proceeds to those who practice it, cybercrime may slowly but surely become a less sustainable activity, therefore, leading to a more cybercrime-free environment.

References

1. Apăvăloaie,E., The impact of the Internet on the business environment " (2015). ScienceDirect.
2. Bray, Jesse D., "Anonymity, Cybercrime, and the Connection to Cryptocurrency" (2016). Online Theses and Dissertations. 344. https://encompass.eku.edu/etd/344
3. CSOHomepage,https://www.csoonline.com/article/2124681/what-is-social-engineering.html. Last accessed 6 December 2021.
4. Proofpoint. (2019). Human Factor Report 2019 (Report No. 0819-032). Proofpoint, Inc.
5. Bertrand Russell (2013). “Human Society in Ethics and Politics”, p.160, Routledge
6. Kevin D. Mitnick & William L. Simon.: “Controlling the Human Element of Security”. The Art Of Deception, (2001)
7. CBS News, United States. Accessed 3 December 2021. <cbsnews.com/news/anonymous-hacker-hector-monsegur-turned-fbi-informant-breaks-silence>
8. Morgan, S. United States. Cybersecurity’s Greatest Showman On Earth: Kevin Mitnick. Last accessed 1 December 2021. <https://cybersecurityventures.com/cybersecuritys-greatest-show-on-earth-kevin-mitnick/>
9. Linn F. Freedman.: “Ransomware Attacks Predicted to Occur Every 11 Seconds in 2021 with a Cost of $20 Billion”. National Law Review, Volume X, Number 44 (2020)
10. FBI. (2020). 2019 Internet Crime Report. Federal Bureau of Investigation
11. FBI. (2021). 2020 Internet Crime Report. Federal Bureau of Investigation
12. Morgan, S. United States. Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Last accessed 1 December 2021. <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/>
13. Norton. (2017). 2017 Norton Cyber Security Insights Report Global Results. Norton by Symantec
14. FBI. (2021). 202 Elder Fraud Report. Federal Bureau of Investigation
15. Verizon. (2021). 2021 Data Breach Investigations Report. Verizon
16. Threat Intelligence. Threat Landscape Trends – Q1 2020. Last accessed 10 December 2021. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/threat-landscape-q1-2020
17. Sectigo, https://sectigostore.com/blog/different-types-of-hackers-hats-explained/. Last accessed 6 December 2021.

Cybercrime Warfare: Dark Web the Hidden Internet

João Pedro Conceição Barbosa

Lusófona University, Porto - Portugal

joaopcbarbosa98@hotmail.com

Abstract. We currently live in a world where technology is present in all aspects of our life, from the complex tasks performed in our work environment to the simple entertainment we have at our homes and most likely than not these have access to a simple web browser. Although most of these web browsers are considered "normal" it's through the computer that we can access these "anormal" browsers which in essence are a normal browser in all their aspects except the limitations that they provide, these are called dark web browsers. They allow their users to browse the web without the limitations of being "locked out/hidden away" from websites considered insecure/unsafe. On this paper we will be discussing the "power" of the dark web, comparing it with the "normal" web and all the threats present in the dark web. We will also discuss how to access it and make small comparison of the dark web with the deep web.

Keywords: Dark web, Deep web, Cybersecurity, Technology, Cybersecurity risk

1 Introduction

The internet from its origins was but a simple means of communications between people but as time has progressed it has evolved into a platform that easily allows one to expose their ideas, their art works or even just a simple image of them during a vacation.

This evolution ended up splitting the internet into 3 parts, the surface web, the dark web, and the deep web.

The surface web is your everyday web page that can be accessed directly from your web browser.

The deep web sometimes is inaccurately called the lawlessness or unregulated part of the internet. It is used by a lot of criminals but on the flip side it is an online refuge for people who are persecuted for their own beliefs, opinions and who they are. While the deep web is so anonymous by nature it is still possible to be tracked and monitored there by authorities or criminal groups.[1]

The dark web is the actual lawless place of the internet since that place requires a lot more effort to simply access it not to even mention tracking someone in it because of the simple fact that it doesn't operate in the same way as the surface and deep web.

This paper will focus on what is the various sub sections of the Clearnet and what they represent/what you are able to do there.

On section 2 we will be investigation in some detail what represents each part of the of the Clearnet and making some comparisons between the three of them.

On section 3 we will be explaining on how to access the dark web, the market that was considered to be the most famous for the trade of illegal products, one of the main reasons as to why the dark web had a massive boom in use due to the increase in difficulty to trace who performed trades in there and lastly, we will be evaluating its dangers.

2 Clearnet

The Clearnet is something that, to be accessed needs to have some sort of application like Microsoft edge, google chrome, opera, and many others out there available to the consumer and all it need it's some form of internet connection to be used.

Figure 1 – A size comparison of what is available in each of the available webs [2]

2.1 Surface web

So, what is the surface web, well its actually quite simple the Surface web is the portion of the World Wide Web that is readily available to the public and searchable with standard web search engines. It is the opposite of the deep web. The section of the internet that is being indexed by search engines is known as the "Surface Web" or "Visible Web".[3]

The surface web is in constant growth and ever changing but never removed and due to that a popular quote appeared “what happens on the internet stays on the internet”. According to one estimate, there were 334.6 million Internet top-level domain names registered globally during the second quarter of 2016. This is a 12.9% increase from the number of domain names registered during the same period in 2015. As of February 2017, there were estimated to be more than 1.154 billion websites. As researchers have noted, however, these numbers “only hint at the size of the Web,” as numbers of users and websites are constantly fluctuating.[4]

2.2 Deep web

Most people are familiar with the surface web or at least with the basic concept of what the internet is and what it allows one to do, but in most cases, they don’t know what the deep web is or have never even heard of its existence. So, what is the deep web well, the Deep web is part of the World Wide Web whose contents are not indexed by standard web search engines for any reason. The content of the deep web is hidden behind HTTP forms, and includes many common uses such as web mail, online banking, and services that users must pay for, and which is protected by a paywall, such as video on demand, some online magazines, and newspapers, and many more. Content of the deep web can be located and accessed by a direct URL or IP address and may require password or other security access past the public website page.[5]

The Deep Web, as noted, cannot be accessed by traditional search engines because the content in this layer of the web is not indexed. Information here is not “static and linked to other pages” as is information on the Surface Web. As researchers have noted, it’s almost impossible to measure the size of the Deep Web. While some early estimates put the size of the Deep Web at 4,000–5,000 times larger than the surface web, the changing dynamic of how information is accessed and presented means that the Deep Web is growing exponentially and at a rate that defies quantification.[6]

2.3 Dark web

Although those who know of the existence of the deep web or have at least basic knowledge of it also know of the existence of the dark web very few of those venture into it do to existence of some form of fear or lack of means/knowledge of how to access it.

So, what is the dark web, the Dark Web is defined as a layer of information and pages that you can only get access to through so-called "overlay networks", which run on top of the normal internet and obscure access. You need special software to access the Dark Web because a lot of it is encrypted, and most of the dark web pages are hosted anonymously.[7]

The Dark Web is also growing as new tools make it easier to navigate. Because individuals may access the Dark Web assuming little risk of detection, they may use this arena for a variety of legal and illegal activities. It is unclear, however, how much of the Deep Web is taken up by Dark Web content and how much of the Dark Web is used for legal or illegal activities.[8]

2.4 Surface web vs Deep web vs Dark web

So, what's the major difference between each of these webs, well in all honesty there isn't much besides its legality but there are still a few key points that one can take.

- Surface web
  - Only what's legal is visible there
  - Can be accessed by the normal search engines
  - Represents only 4% of all the web
- Deep web
  - Has everything from the most legal to the most illegal
  - Can be accessed by normal search engines but they will not be able to find it on their own
  - Represents 96% of all the web
- Dark web
  - Is mostly illegal
  - Can only be accessed by specific search engines like Tor
  - Represents around 48% of the web (in which this 48% encounter themselves inside the deep web)

	Surface Web	Deep Web	Dark Web
Description	Content that search engine can find	Content that search engine cannot find	Content that are hidden intentionally
Known as	Visible web, Indexed web	Invisible web, Hidden web, Deep web	-
Constitutes	Web	Web	Web
Contents	Legal	Legal + Illegal	Illegal
Information found	4%	96%	-
Browsers	Google chrome, Mozilla firefox, opera	-	TOR browser

Figure 2 – Picture comparing the various web and what they offer to the user [9]

3 Dark web

The Dark Web can be reached through decentralized, anonymized nodes on several networks including Tor (short for The Onion Router) or I2P (Invisible Internet Project). Tor, which was initially released as The Onion Routing project in 2002, was originally created by the U.S. Naval Research Laboratory as a tool for anonymously communicating online. Tor "refers both to the software that you install on your computer to run

Tor and the network of computers that manages Tor connections." Tor's users connect to websites "through a series of virtual tunnels rather than making a direct connection, thus allowing both organizations and individuals to share information over public networks without compromising their privacy." Users route their web traffic through other users' computers such that the traffic cannot be traced to the original user. Tor essentially establishes layers (like layers of an onion) and routes traffic through those layers to conceal users' identities. To get from layer to layer, Tor has established "relays" on computers around the world through which information passes. Information is encrypted between relays, and "all Tor traffic passes through at least three relays before it reaches its destination." The final relay is called the "exit relay," and the IP address of this relay is viewed as the source of the Tor traffic. When using Tor software, users' IP addresses remain hidden. As such, it appears that the connection to any given website "is coming from the IP address of a Tor exit relay, which can be anywhere in the world." While data on the magnitude of the Deep Web and Dark Web and how they relate to the Surface Web are not clear, data on Tor users do exist. According to metrics from the Tor Project, the mean number of daily Tor users in the United States across the first two months of 2017 was 353,753— or 19.2% of total mean daily Tor users. The United States has the largest number of mean daily Tor users, followed by Russia (11.9%), Germany (9.9%), and United Arab Emirates (9.2%).[10]

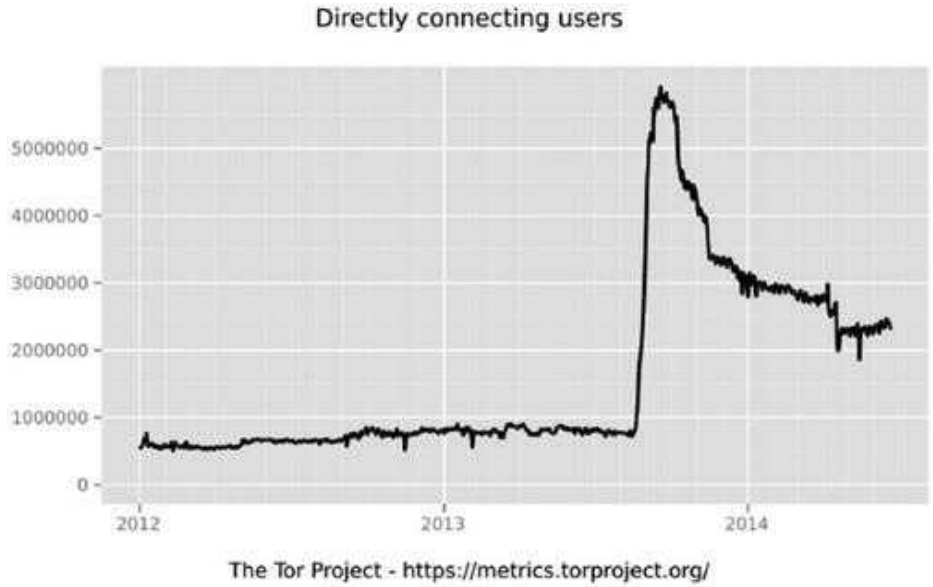


Figure 3 – User connection to Tor´s [11]

3.1 Silk Road

So, what is the Silk Road, well as the name entails it has to do with trade and in its most basic of forms a drug trading website located on the dark web.

How does one go about purchasing and selling drugs in such a website, well its quite simple in all honesty, the Payment for goods and services on Silk Road were made in Bitcoin, an encrypted digital currency. In contrast to the vulnerabilities exposed by Pay-Pal, Western Union and cash in post, this offered anonymity in financial transactions. The use of anonymous Tor mail for private and anonymized communications between site users was another important security feature.[12]

So how does one estimate how many trades were done in such a place well there is mostly two ways.

- Most purchases entail a review at the end, and reviews are displayed on the front page, so one can monitor the front page and extrapolate to estimate average number of transactions per day or week, and from there estimate turnover and what SR's commissions total.[13]
- Another way is to look in the blockchain for SR-related addresses or transactions; one possible address had a 2012-06-23 balance of Ƀ450,825 or $2,885,280.[14]

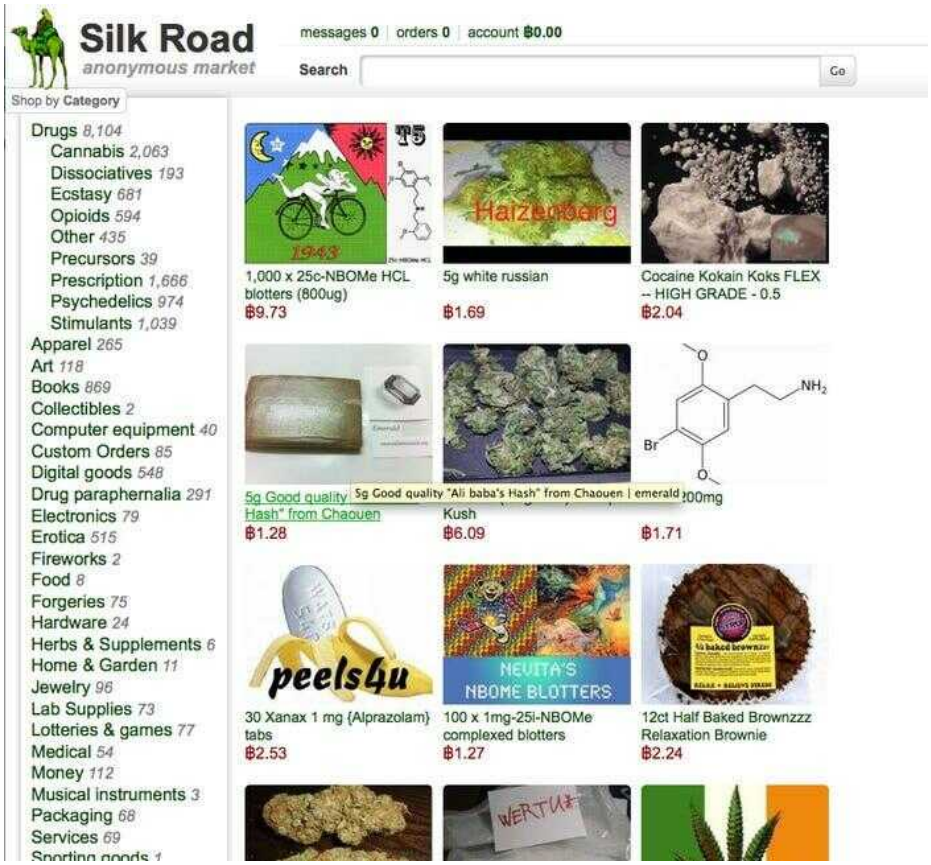


Figure 4 – Silk Road website [15]

3.2 BitCoin

By now and having in consideration the recent times most of us must know or at least have heard of bit coins and how they can influence the trade market, the simple truth is that the bit coin is currency like any other and it only has any real value because we deem it so.

So, what is a Bitcon, well a Bitcoin is a cryptocurrency that has received substantial attention given its innovative features, simplicity, transparency, and its increasing popularity. Since it was first outlined in a paper by Nakamoto (2008) and went online in 2009, the price of Bitcoin has increased by over 5000% up July 2016. Investors have employed Bitcoin as currency as well as for investment purposes with Selgin (2015) and Baeck and Elbeck (2015) arguing that Bitcoin should be seen as a speculative commodity rather than a currency. Yet, the efficiency of Bitcoin within the meaning of Fama (1970) has not been investigated.[16]

3.3 The dangers of the dark web

What became a real power behind the dark web was the bitcoin due to the simple fact that it is considered untraceable allowing for all kinds of transaction to be performed with out any of the dangers of being found and arrested.

For example, as shown before one can acquire drugs trough the use of the bitcoin and buy it in mass quantities without the fear of being traced, and the only problem that will remain is how one will manage to acquire it.

So, one can imagine that with enough monetary power in the dark web one will be able to acquire anything they desire, from the simple purchase of drugs to the potential of buying any kind of weapons be the simple side arms to ones considered to be of mass destruction.

Also, one can purchase the actions of someone or a group of people and direct them to perform attacks be they virtual or physical on a certain target.

For what I can take from the research I performed on this matter as long as one has the monetary power in the dark web one will be able to perform what ever they desire for the simple fact that in the dark web exists the lack of rules.

So, in basic principle as long as there will be any sort of demand there will be an offer to perform the given task.

4 Conclusion

So is the deep web and the dark web as dangerous as some of us fear it to be, well not really it depends on what you access and how you access it. One can find a hidden community that’s all about doing good to the world just as fast as one can find one that its sole purpose is to do harm to it.

But in majority what one will find the most in such place is a simple market that trades in all things with out regulations of the law and sometimes even without regulations of what is considered morally wrong, as said before as long as there is a demand there will be someone offering.

While one can take measures to prevent the maximum amount of danger as possible in most cases, they will serve almost no purpose other than self-assurance because while yes, it is a lawless place in most cases the only thing one seeks to do there is the act of buying/selling something that is considered illegal and will not try to track anyone that bought or sold a specific product.

References

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

Ransomware Vulnerabilities During a Pandemic

Marco Querido a22002877

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

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

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

1 Introduction

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

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

2 Main threats in IT during the pandemic

2.1 Major threats in Europe

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

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

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

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

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

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

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

2.2 Major threats in Portugal

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

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

- Unprivileged account commitment;
- Unauthorized access.

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

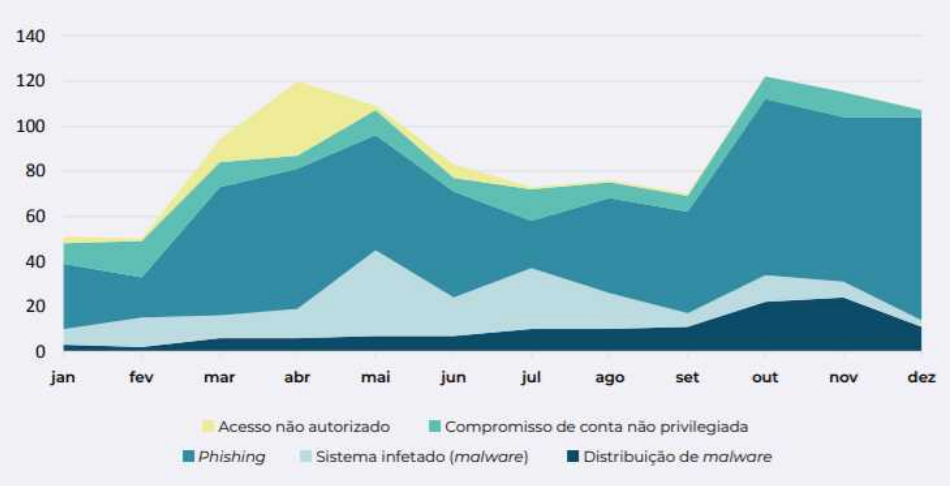


Fig. 1. Incidents by type recorded by CERT.pt,2020 (C/V)-Top 5, by month [3]

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

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

3 Ransomware

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

3.1 Definition and case studies

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

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

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

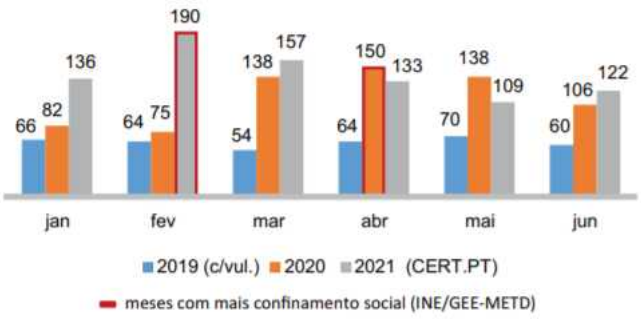


Fig. 2. Number of incidents registered by CERT.PT, on the first semester of 2019, 2020 and 2021, and peaks of social confinement [6]

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

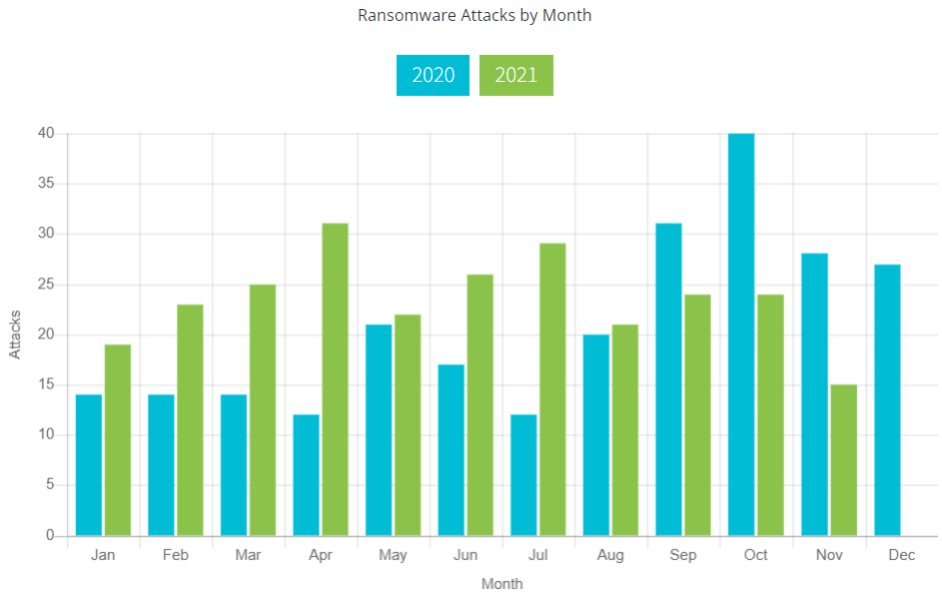


Fig. 3. Ransomware attacks by month [7]

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

3.2 Practical Example

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

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

```
#!/bin/bash
#
# Title:         Disable D3f3nd3r (Rubber Ducky)
# Description:   This Payload disables Windows Defender using Powershell, Works also for the Hak5
#                Rubber Ducky or any HID device that supports Quacking.
# Author:        REDD of Private-Locker
# Version:       1.0
# Category:      Disable Security
# Target:        Windows
#
# Source:        https://gist.githubusercontent.com/PrivateLocker/6711c4fe88eae75774284bd6efc377dc/raw/30c9a50a3dd9
#

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

Fig. 4. Windows Defender deactivation payload [10]

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

4 Portugal compared to the world

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

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

4.1 Ransomware cases in Portugal

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

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

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

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

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

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

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

4.2 Corrective and prevention measures

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

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

5 Conclusion

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

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

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

References

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

References

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

Ransomware Vulnerabilities during a Pandemic

Carlos Garcia

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

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

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

1 Introduction

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

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

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

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

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

2 Most common cyberthreats during the covid-19 pandemic

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

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

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

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

2.1 Prime Threats during covid-19 pandemic

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

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

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

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

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

A brief explanation of the most common cyber threats

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

2.2 Ransomware Vulnerabilities during covid-19 Pandemic

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

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

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

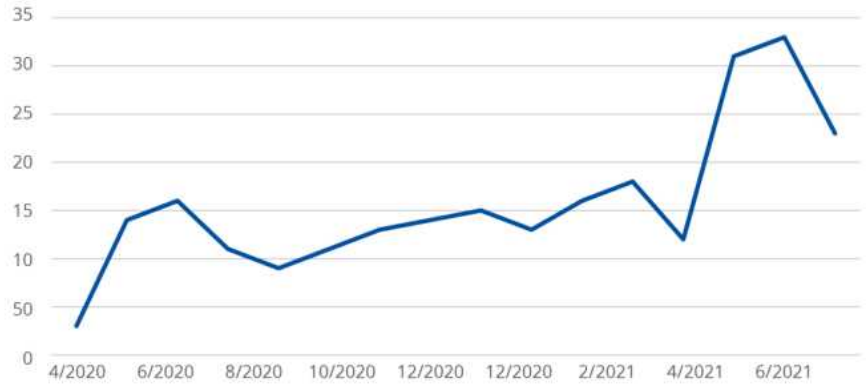


Fig. 1. Ransomware incidents observed by ENISA (April 2020-July 2021) [7]

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

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

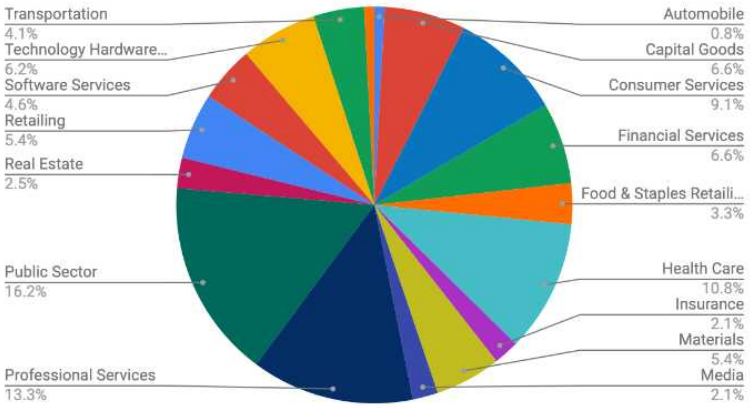


Fig. 2. Common Industries Targeted by Ransomware in Q2 2021 [23]

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

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

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

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

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

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

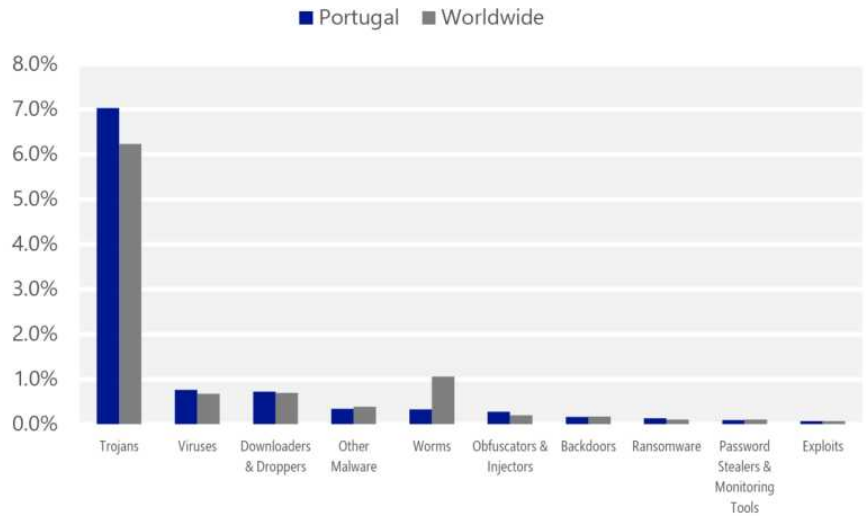


Fig. 3. Percentage of malware in the amount of analyzed Computers in Portugal as of March 2017 [17] [22]

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

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

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

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

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

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

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

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

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

4 Conclusion

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

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

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

Safety comes first!

References

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

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

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

Survey on Hacking Analysis and Mitigation Techniques

Diogo Santos

Lusofona University of Porto, Portugal

a22005114@mso365.ulp.pt

Abstract. Nowadays we see a greater number of malware attacks and we see that it becomes increasingly difficult to combat and track this type of attacks. Malware is just a term that mean "malicious software" and there are many types of it.

In this project we will be looking at mitigation techniques, we will talk about the ones that are the most used and which are the best and offer more protection.

Mitigation techniques also involve detection, not only protection but also involves the prevention against these types of attacks, often this serves as a protection to them, preventing this kind of attacks it is always better than trying to solve them. As hacking gets more and more complex technology needs to evolve with it, we are going to go deeper into what technology gives us the best ability to counter hacking.

As time goes by, hacker techniques will evolve, and this technique will improve so that its detection will be more difficult for our devices. Networks are expanding day by day and the need of security is getting more and more important, ethical hacking is more used today to help and create security. In this paper we will go along of the hacking technique and some examples about it.

Keywords: Hacking, Mitigation, Malware, Ethical Hacking, Technology, Software, Vulnerability Analysis, Exploits

1 Introduction

Over the last few years, we have seen hacking rise in popularity due to advances in the technology field. Today many of our devices are connected to each other and connected to an internet network, this means that the same information is available between the various devices and with this there is an increased risk of attack by a stranger or even accessing our network and consecutively our personal information, our device and everything that is connected to it depending on the complexity of the attack that may occur. The connections between devices have been very advantageous for all of us, it makes our daily life much easier, in terms of work and leisure but it can also bring many risks to the security of all our information, this is a topic that many people are not aware or not paying attention, syncing devices to a cloud makes it easier and faster to switch devices but it also increases the risk of information leakage, whether personal or work data.

Many people continue with the idea that hacking is always bad, whenever the word is referred to, the idea arises that it is an illegal activity and that its purpose is to cause the cause. Although it can be used for this, nowadays we know that hacking is widely used for reasons of increased security in companies to protect their data, furthermore it has become a practically essential activity to increase the protection of companies, to find problems, weaknesses and therefore being able to correct them, to avoid hacker attacks with malicious intent and also expenses in recovering lost information, through this type of hacking companies are attacked with their permission and then a report is made about the areas that need to be reinforced and why, we are going to speak about this later in this paper, based in a journal, this is called ethical hacking[1] that, following the law simulate these kinds of attacks. We are talking about a lot of types of attacks (e.g., DOS, DDOS etc.) These types of attacks have varying levels of severity and damage to companies for example, I chose to speak about these specific attacks because they are the most used nowadays as they are the most difficult to defend, in this paper we will talk about the attacks are made and also explain the process behind launching an attack of this kind, it is important to remember that more and more attacks are difficult to prevent and consequently it is important to know how to protect all information and devices within the network, attacks within the network if they affect multiple devices, cause them to become zombie machines[2], devices that are compromised during an attack and then pose a threat to the rest of the network they are connected to, we are going to talk about this in depth later in the paper as well. All these attacks require Mitigation techniques, these are important to keep all the data safe in case of attack.

Furthermore, the present introduction section 1, the paper will have 6 more sections divided as follows:

Section 2 – Discusses the concept of “Hacking”, why is it important, how hacking can help in companies protection.

Section 3 – We will go through the types of hackers that exist, explaining the purpose of each one and the situations that they act.

Section 4 – There are many types of attacks, in this section some of them will be presented.

Section 5 – As valuable as attacks, the techniques to avoid them will be presented in this section.

Section 6 – Presentation of a report that shows how an attack can cause more damage and panic than its taught.

Section 7 – Conclusion about the theme portrayed.

2 About Hacking

This activity started due to the curiosity of computer enthusiasts, these people are known for their skill in the field of technology (” He is a computer enthusiast and extremely proficient in programming languages, computer systems and networks.”) [4]. These very skilled people are referred to as better programmers, programmers who don't follow normal programming methods, they have their own methodology and

program as their will, overcoming various barriers including discovering new ways to program by going deep in this area.

Many times, a hacker is considered to have good intentions which is not supposed to be, hackers are considered the (" safeguards of networks") [4], when exploiting breaches in the network and in the company.

We also have hackers with bad intentions, they attack without authorization and enter networks ("Malicious hacking is the unauthorized use of computer and network resources") [4]. This often ends up with information theft and with it ransom requests in the form of cash.

2.1 Hacking importance

Hacking nowadays is used by companies all the time, they need to be working for the better future of the company, doesn't matter in each area, they need to be always working for better, in terms of technology used and now it's more common for companies to invest in cyber security, so their data is safe and they can just keep their services online for longer, if their services are not online because of an attack this means that the company is losing a lot of money, at that point every minute counts, with this hacking becomes an important tool to help companies being more safe in their networks and services. We are speaking about ethical hacking of course, this type of hacking is all about an organized attack between the company and the ethical hacker, summing up the objective is to find vulnerabilities in the network system of the company by invading it, after this process the hacker is supposed to find ways to prevent the same attack he performed and other attacks that might get the company's data in danger, this whole process has distinct phases, like shown in the next figure.

Fig. 1. Hacking Phases [3]

Evidence about the" test attack" [3], must be erased and without a trace, in order not to leave breaching hints that were discovered by ethical hacking at the beginning of this process. This test attack, as it is called, is aimed at a more complete analysis of the entire network to help build a better structure to ensure maximum protection for the company that hired the ethical hacker, this is a paid job [3] and

everything is done in a controlled environment with full knowledge of company members. After the testing process, the security is certainly improved to avoid damage in an uncontrolled real situation, in case of attack.

3 Types of Hackers

In the realm of hacking (whether we talk about authorized and controlled hacking or hacking in the realm of crime) we have three main types of hackers that are important to know ("these have categories according to the shades or color of the "Hat".") [4] according to the hat color we have: White Hat Hackers, Gray Hat Hackers, Black Hat Hackers.
The color of each one's hat represents a different type of person, with different intentions in the same field, the lighter the color, the lower the malicious intention on the part of the hacker

Fig. 2. Different types of Hacking/Hackers [5]

3.1 White Hat Hackers

In the case of the white hat hacker, we need to know that, being the lightest color of the three that will be presented, they are certainly the ones with the best intentions regarding the act of hacking, this type of hacker is the so-called ethical hacker, it is about a paid professional to test the security of a company's network, report on that same test and also resolve network weaknesses, leaving the company better prepared in case of attack, either on the network or on its information.[5] (They are also known as "IT Technicians") [6].

3.2 Black Hat Hackers

Opposed to the white hat hackers the black hat hacker is known for his bad intentions in the act against the network and against its users, often causing damage to both, often the purpose of this type of hacker is theft of important information for the company and

a request for monetary redemption of the data, or even the destruction of information with the intention of causing great damage to its services, making it an impossible operation.

This type of hacker acts according to all your personal interests, the objective is not to test your skills, but to cause problems for your target, blocking the access of network users and only removing this block after the high payment they want. They know how important information and services are to these companies, hence these high-value redemption requests. [5][6]

3.3 Grey hat hackers

Gray hat hackers have an intermediate profile between white hat hackers and black hat hackers. These hackers have the same intention of infiltrating the network system and taking access by force. After the attack and after knowing how to access all the information that compromises the company in question, the gray hat hacker offers his services to company by making known the vulnerabilities they have, demanding a payment that you think is correct for it. This type of attack is much more thoughtful, as it is carried out so that it can be reversed, if the company accepts the payment to improve its security, the attack can be reversed and thus improve the security of the company in question. Although the company does not agree with the attack, it can accept his services [6].

4 Attacks

There are many types of hacking attacks that may happen in our everyday life, and without us noticing it, with this we are going to see some of the most important attacks in different scenarios like wired scenarios or wireless network scenarios.

In a public network, in a caffe, library, everywhere when a device is connected to the internet an attack may occur, every unprotected device is a target if it is in the wrong place at the wrong time depending on the hacker’s intentions.

large companies or some type of service actively used by the population are usually targeted by Hackers these targets are the ones most likely to give hackers what they want as a ransom for data, money is usually what they ask for to give back the important data without any damage.

Table 1. Types of Hacking Attacks [10][8][11]

Type of Attack	Definition	Level of threat
DoS	"DoS" is a big attack base on throwing a lot of information(messages) at the same time for the same IP, overwhelming the all the traffic nodes throughout its passage, normally this type of attack is done to take down important servers for a few hours, all users connected to the server will suffer DoS as well	High
DDoS	In general, a DDoS attack aims to hindering the access of legitimate users to a target system or services by overwhelming the resources, this way the device cannot handle such amount of information and taking total or partial loss of services and files as well	High
Waterhole	Waterhole is done in websites with JavaScript or HTML code, this attack makes the user go in a website with a malware with will corrupt the device giving access of the whole user's network, this normally happens with the most used websites by the user	Medium
Fake WAP	Fake WAP is known to happen via wireless connections, this type of attack consists in getting a fake wireless access point to the network, as soon as a device is connected the user's data can be stolen by the hacker	Medium
Virus/Trojan	Trojan viruses are acquired by users by downloading programs with the virus, this gives the hacker access to the infected computer letting him know when the device is online and provides him with the ability of stealing users' information.	Medium
Phishing	There are 2 types of phishing, by link manipulation which is false URL's replacing sub domains different from the original sub domain so they can trick users to trust in links for example, or filter evasion which consists in using images instead of text, this makes anti- phishing filter useless when trying to detect it	High
Keylogger	This type of attack consists in a malware that is not visible at the normal view in the device, this records the keys that are pressed and write them in a log file which is usable by the hacker when login into a website the data is written, this way the hacker get access to all data about the user's accounts, personal information, passwords	Low

5 Mitigation Techniques

Mitigation techniques are all about keeping devices secured, servers and personal devices like computers, networks et. We know that today avoiding all these attacks is impossible, because there are always new ways to attack, despite of not being possible to defend your network from every single attack, it's possible to reduce the damage created by these attacks by avoiding some situations and using some tools to help you in the process. Some are simple than others but protection nowadays it's important, getting a secured network in your company decreases the risk of damage in case of attack [8][12] and with increasing security we don't waste money on recovering data, recovering data costs a lot of money. Many techniques are known but ignored by most of the population using devices all around the internet. Getting a strong password with numbers, capital letters and no names in it, most of the times this is ignored by normal users, and this might compromise their safety on the internet. Using VPN and avoiding downloads of cracked software's are some basic safety rules that are nor respected by many users.

For the attacks that we spoke about before, now we are going to tell you about the mitigation techniques to avoid those same attacks.

DoS/DDoS.

These attacks consist in sending a lot of information to the device at the same time making it to shut down. Nowadays this kind of attacks have been more frequently used as we can see from the graph under. This study was done by Google Pictures in the past year to show how popular these attacks since 2010 until the present time.[13]

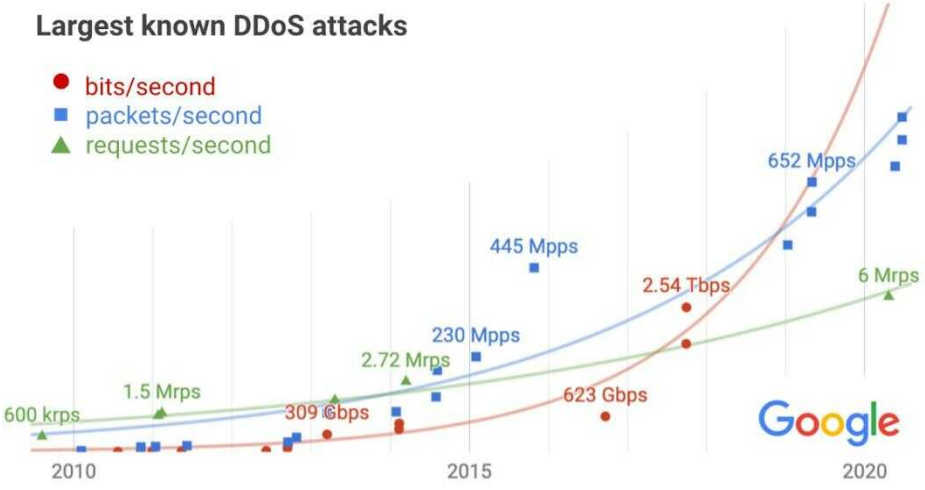


Fig. 3. Exponential growth in DDoS attack volumes [13]

("We need to factor in the exponential growth of the internet itself, which provides bandwidth and compute to defenders as well.") [13], comparing the growth of users with the growth of DDoS attacks we see that is a nice result, but it is important to use some counter measures to prevent these attacks. To prevent these attacks, we can use filters in our network, this only works if the hacker is not aware of this act, filtering lets your router analyze the information coming from outside the network and only letting into your device the clean information this prevents the overload of information. Using a secure overlay can be an option as well, this brings up a more trusted firewall that can only let go the clean information to the user's network. Honeypots is another way to protect your system from these attacks, it consists of miming your network, making the hacker attack a mimic network while your device and your network still intact.

Waterhole.

Protecting yourself from waterhole attacks u need to hide your online activity, you can use VPN for example this way your online activity gets encrypted, and it is more difficult for hacker to trace you.

Fake WAP.

To prevent this kind of attacks u should not connect your devices to unknown Wi-Fi's networks.

Trojan Virus.

Trojan virus are inside downloadable programs, first always avoid downloading software from unknown or not credited websites, most of these unknown downloads come with virus hidden in their installation launchers, making it unnoticeable to the user that is downloading apps, getting an anti-virus that can scan your pc from time to time also helps to clear any virus that got into your device by the user not noticing anything strange in downloads.

Phishing.

Avoiding Phishing is all about paying attention to emails that u might receive, some of them bring up messages that don't make sense with the user's reality, those are easy to spot. Getting a spam filter helps a lot in this manner and being informed and trained about some scenarios that appear when you get attacked by phishing.

Keylogger.

Defending versus a keylogger the user should get a 2-step verification, this always help to verify the usage of the website and may let you know if it's being used a keylogger or not, with this is important that the user is careful about his downloads, these malwares come on downloads from unknown sources as well.

6 Ciber attack on U.S. power grid could cost economy 1 trillion Dollars.

The report that we are going to see tell us about a study done by the university of Cambridge Center about the risk of a potential scenario that involves an electricity blackout in New York and Washington DC. The scenario created by Cambridge University is flagged as "technologically possible" to happen once in the next 200 years.

They speak of an episode for which it is necessary that the entities that ensure these electricity services are prepared for this possible threat.

The hypothetical attack created by this university, tells us about 93 million people with no electricity throughout New York and Washington DC. During this blackout the report shows an increase in the mortality of the population due to the lack of electricity in hospitals, which would cause the death of patients, including the non-operation of the hospital, security in all networks would also be a problem such as transport.

Since the US economy is directly linked to these types of services, it would be affected.

The estimated loss balance is also made, and we can draw our conclusions through this quote from the report ("The total impact to the US economy is estimated at $243 billion, rising to over $1 trillion in the most extreme version of the scenario") [14]

The extreme scenario speaks of the absence of support from 100 generators, which would lead to a loss of over 70 billion. These results are presented because of the evidence presented in 2014 in other major ("“Evidence of major attacks during 2014 suggests that attackers were often able to exploit vulnerabilities faster than advocates could remedy them,” said Tom Bolt, director of performance management at Lloyd's, in the report.[14]

7 Conclusion

Hacking is important because it helps companies in their own protection, to improve their services and make everything in a safer structure due to several known techniques.

We have several different types of hackers, and all have characteristics that can help in the evolution of security in this area.

Be they ethical hackers or malicious hackers, they all have the role of finding vulnerabilities and thus allowing for increased security.

We can observe that if security is not taken seriously, it can come to have great costs and an attack can come to affect great world powers at the economic level. These large-scale attacks can cause irreversible damage to companies.

Security must be taken seriously and more than protecting the network in real time, it must be taught how to avoid these same attacks, which part of the internet is secure and which part is suspicious through t these mitigation techniques. Attacks are more and more common which means that this area deserves much more attention from anyone thinking of connecting to the internet, now it is not just big companies that are the targets, but everyone can be targeted.

References

1. Regina D. Hartley Appalachian State University - Ethical Hacking Pedagogy: An Analysis and Overview of Teaching Students to Hack
2. Ms. Chandni M Patel*1, Asst. Prof. Viral H Borisagar #2 * C.S.E. Department, Government College of Engineering, Sector-28, Gandhinagar Gujarat Technology University, Gujarat, India. International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 9, November- 2012 ISSN: 2278-0181
3. Study Of Ethical Hacking Bhawana Sahare, Ankit Naik, Shashikala Khandey Research Scholar, Lecturer Department of Computer Science and Engineering, Kirodimal Institute of Technology, Raigarh Chhattisgarh – India - International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 4, Nov-Dec 2014
4. K.Bala Chowdappa et al, / (IJCSIT) International Journal of Computer Science and InformationTechnologies,Vol.5(3),2014,3389-3393- http://ijcsit.com/docs/Volume%205/vol5issue03/ijcsit20140503161.pdf last visited 2021/12/13
5. https://edgy.app/how-to-hack-for-the-greater-good-inside-ethical-hacking - photo by MatiasDelCarmine | shutterstock.com, last visited 2021/12/14
6. Palmer, C.C. (2001, April 13). Ethical Hacking. IBM Systems Journal Vol. 40 No.3 2001
7. Ethical Hacking Pedagogy: An Analysis and Overview of Teaching Students to Hack Regina D. Hartley Appalachian State University- https://scholarworks.lib.csusb.edu/jitim/, last visited 2021/12/14
8. A survey of distributed denial-of-service attack, prevention, and mitigation techniques Tasnuva Mahjabin1, Yang Xiao1, Guang Sun2 and Wangdong Jiang2 - https://journals.sagepub.com/doi/pdf/10.1177/1550147717741463, last visited 2021/12/14
9. Hacking Attacks, Methods, Techniques and Their Protection Measures Dr. Sunil Kumar1, Dilip Agarwal 2
10. Types of Hacking Attack and their Counter Measure Minakshi Bhardwaj and G.P. Singh
11. Survey of keylogger Technologies Yahye Abukar Ahmed, Mohd Aizaini Maarof, Fuad Mire Hassan and Mohamed Muse Abshir
12. Vulnerabilities and mitigation techniques toning in the cloud A cost and vulnerabilities coverage optimization approach using Cuckoo search algorithm with Levy flights Mhamed Zineddine MIS Department, ALHOSN University, Abu Dhabi, United Arab Emirates
13. https://cloud.google.com/blog/products/identity-security/identifying-and-protecting-against-the-largest-ddos-attacks, last visited 2021/12/14
14. https://www.reuters.com/article/us-cyberattack-power-survey-idUSKCN0PI0XS20150708-, Reporting by Carolyn Cohn, editing by Louise Heavens, last visited 2021/12/17

Survey on Hacking Analysis and Mitigation Techniques

Ricardo Neves

University Lusófona of Porto
Porto, Portugal
ricardomanuelvalenteneves@gmail.com

Abstract. Year by year, technology has evolved and integrated itself into our lives, allowing us to explore a new world where we can access or share relatively anything we want. Consequently, in today's society, we are present with constant use of those technologies and thus an accompanying and permanent flow of data throughout the world. This information, available on the internet, appears in various forms, such as images or texts, and holds its value. Therefore there will be entities that will try to obtain this data for numerous purposes with mixed approaches. Specifically, cyberattacks have been a common threat to both the data and the users of the internet. One of the most popular and common cyber threats is known as malware. This malicious software finds its way to our devices through various ways with different objectives, having only in common its intent, which is to damage computer systems. This survey will cover hacking analysis by deconstructing cyberattacks throughout its chapters and providing a practical application on a malware analysis, bringing forward a deeper understanding of hacking and mitigation techniques.

Keywords: Cybersecurity, Cyberattacks, Hacking Analysis, Mitigation Techniques, Network, Cybercrime, Hash, Strings, Cyberspace

1 Introduction

Currently, cybersecurity is a broad field that follows the ongoing growth of modern technology [1]. Acknowledged as one of the most notable drawbacks to governments, corporations, and individuals in the current century [2], cybersecurity plays a significant role in the lives of those who interact with cyberspace. Moreover, it extends through multiple sectors with various media articles and studies showcasing the harm caused by hacks to the respective, be it healthcare [3] [4], economics [5], or others.

The Federal Bureau of Investigation, commonly referred to as the FBI, is a well-known justice department whose actions have significantly benefit the victims of cybercrimes. Furthermore, it is also an exceptional source to understand the necessity of cybersecurity, mainly due to their publications in regards to the impact of cyberattacks throughout the world. According to the FBI's 2020 Internet Crime Report, there was a significant increase in complaints of suspected internet crimes in comparison to the previous year and losses that amount to billions of dollars. More so, deeper searches lead to ridiculous numbers supporting and justifying, the dread that many entities have towards the world of cybersecurity. As a matter of fact, this numbers might not even be close to the actual values by the simple fact that many companies and individuals tend to hide or wrongfully disclosure information regarding cyberattacks [6]. Notably, data breaches are often the cause for the concealment to the public, in order to mitigate any repercussions to an organization or individual.

Amidst the continuous approaches regarding cyberattacks, individuals are often classified based on their motivations [7]. On the other hand, and contrary to many, while they are divided by such designations, many share the same knowledge and set of tools.

This survey aims to deconstruct cyberattacks, by thoroughly covering hacking analysis, or attack analysis, and mitigation techniques. Moreover, the technical concepts will be followed with a practical application, that can be accompanied by anyone, independently of how knowledgeable they are on the matter.

2 Cybersecurity

A variety of concepts regarding the cybersecurity domain turn out to not only be hard to define but to explain due to their nature. As a concept that has changed through time, cyberspace is a perfect example [8]. In 2018 JP 3-12, DOD, the Pentagon released a term that would describe cyberspace as "the global

domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers" [9]. Such description was later accepted by some and refused by others, yet that isn't the point. The important part is to realize its correlation with cybersecurity, to further understand the consequent topics. In short, cyberspace is a critical infrastructure that holds information that is stored, shared, and communicated, a world of computer networks and its users [8]. When we engage with cyberspace, cybersecurity plays a huge role. The nature of the activities performed and involving cyberspace shape the necessity of cybersecurity, and whatever measures are applied when we engage with this world, they must support confidentiality, integrity, availability, and non-repudiation [10].
Nonetheless, securing something is about protecting it from the threats that could exploit its vulnerabilities [11]. Thus, the need to dispense any necessary resources to cybersecurity, and the required thought on how to steadily improve it. Striving for the utmost safety of our systems, organizations, and ourselves.

3 Hacking and Cybercrime

While cybersecurity has the constant need to keep up with the evolution of modern technology, attack analysis follows the trail of the increased complexity, severity, and events of cyberattacks [12].

First things first, taking each concept one by one, there is hacking. It's a scary term for many, yet an exhilarating sound for others. The word hacking, or hacker, didn't mean any harm a long time ago [13]. It was a way for individuals to either test their skills, or enjoy learning about the latest technology, but it doesn't represent that group of people anymore [13], not to the media at least. Hackers are now divided and described in various terms, all of them representing individuals in their differences, be it motivation, experience, or other [7]. The following denominations and respective descriptions, elaborate more about some of the existing types of hackers [14] [15].

- Black Hat: Contrary to White Hackers, this set of individuals are cybercriminals that intend to harm a computer system or network. They do so by stealing data, shutting down services, and more. Criminal communities where these cybercriminals interact and trade can be seen in the clear and dark web.
- Grey Hackers: Grey Hackers can be seen as both a Black Hat and a White Hack. They tend to decide on which hat will they wear for a certain job, depending on the best offer. This behavior is a major reason why many consider them one of the most dangerous types of hackers.
- White Hat: White hackers are also known as Ethical Hackers. They are security experts and a major strength to an organization's security team.

Shifting the focus to cyberattacks, these are the type of attacks carried out by cybercriminals. The European Union Agency for Cybersecurity, ENISA, released their Threat Landscape 2021 not too long ago [16]. Its documentation provides a well around update on many aspects surrounding this year's cyberthreats and cyberattacks. A resume of some of the content detailed in the Threat Landscape 2021 document is presented below [16]:

- Cyberattacks with nature in malware are still one of the major threats to today's entities.
- Hacktivism remains low yet impactful. It is mainly targeting specific organizations while maintaining their signature means of performing cyberattacks, like DDoS attacks and the release of sensitive data. A famous example of a hacktivist group is Anonymous.
- Conti was the ransomware with the highest monetary gain in 2021, going over 12 million dollars.

It also mentions the changes in cybercrime caused by COVID-19. Amidst the pandemic, many studies, and reports [17] have shown an increase in cybercrime since its early stages. Interpol COVID-19 Cybercrime Analysis Report [17], 2020, showcased data that would resonate in an alarming increase in cybercrime, involving phishing, ransomware on critical infrastructures, and overall, a group of cybercriminals exploiting people's weakness at unfortunate times. Even so, cybercrime events have been around for a long time and can carry out cyberstalking and cyberterrorism activities [18].

Nonetheless, there are still worldwide occurrences that showcase the positive side of hacking. Capture the Flag (CTF), in the scope of cybersecurity, are one of the many types of competitions that involve hackers. It is a great way to be part of the community while testing your skills and having a good time. Computer scientists, for example, have a lot to gain by being part of hacking conferences. Even more, many companies have been joining the world of bug bounties, congratulating hackers through monetary gains, most of the time, while improving the overall security of the business.

4 Hacking or Attack Analysis

Given the nature of cyberattacks, we can describe their analysis based on two points of view. We can view and approach a cyberattack in an offensive or defensive manner, each having its unique yet related set of methods. Although they can be divided by such terms, their motives shouldn't be assumed. An offensive approach can be taken to perform a security evaluation of a system, leading to an outcome that won't be considered a cybercrime. On the other hand, offensive methods can be used to deliberately make a cyberattack harder to fight against.

Depending on the perspective, we can think of attack analysis as the artistry that deconstructs a cyberattack, being that the overall goal is not only to identify it but to understand it [19]. Furthermore, it is crucial to mitigate its damage, if complete elimination of the problem isn't possible.

The methods of how attack analyses are carried out can vary depending on multiple factors, such as the nature of the cyberattack or the operating system of the targeted machine. [19] In the eventuality that an attack has occurred and we are aware of such, forensic analysis can help us better understand what happened by searching for possible actions made by the hacker, while also deducing the damage caused. If legal actions were to be taken, it is also possible to gather evidence for such, although a countermeasure could be used by the cybercriminal to prevent any traceable information, and make our work of analysis harder.

To achieve a certain level of complexity, we will focus on a specific type of cyberattack and base our hacking analysis and attack analysis on the respective. Being malware a great enemy to cybersecurity in today's century, it will become the focus of the next topics.

A dynamic or static approach are both ways to conduct malware analysis, where the difference lays down on whether we run the malware while we examine it or not [20]. Furthermore, we can describe them as basic or advanced.

Table 1. Approaches to Malware Attack Analysis

Basic Static Analysis	A basic and quick way to gather information. Not that effective towards advanced malware.
Basic Dynamic Analysis	Analyse based on monitoring the malware in action. It’s recommended to proceed with the necessary tasks in a safe environmnent.
Advanced Static Analysis	A more in-depth analyse, usually involving dissembling tools.
Advanced Dynamic Analysis	May provide information that might have escaped previous techniques

Both basic type analyses could be done by everyone, even the newcomers to the field. It can be an effective way to identify and apply measures to eliminate malware lacking in complexity. It is recommended that when running the dynamic analysis, the process should be executed in a safe environment, often called sandbox, to prevent damage to the main network and system. The advanced static analysis provides a clear understanding of what we are dealing with [20]. A great and helpful tool for this task, that involves assembly language is IDA Pro. If none of the techniques above seem to be giving the desired, or necessary information, then advanced dynamic analysis might be the answer. Usually, they are done through debugging to better deconstruct the running executable.

Below are introduced ways to gather information from executables, which are usually what we will be facing when analyzing malware [19]:

- Antivirus tools.
- Hashes for malware identification.
- File strings analyze

Out there, most antivírus software adopts one of these two methods: Signatures, Heuristic Analysis [21]. Those who follow the signature route, work by comparing the piece of viruses with a signature database,

to see if it finds a match [21]. A big problem with the described method is that there is always a possibility of no match being found, even though it is analyzing a vírus. However, the heuristic method doesn't stop at the code and tries to go further. It looks to predict and learn its behavior, often utilizing machine learning techniques [22].

To those who are unfamiliar with hashing, it is a great way to identify malware. One could describe hashing as an algorithm applied to data, such as a file, that later produces a unique hash [23]. You could think of this unique hash as a fingerprint that identifies the malware. This hash code can then be helpful to carry out further investigation. Below are listed two popular cryptographic hash methods [24]:

- MD5
- SHA

Although SHA is considered more secure, MD5 has the upper hand when it comes to speed [25]. Some similarities can be seen in regards to padding and resource utilization [25].

A string is a term that is very common in programming. It can be described as a sequence of characters, and while they reside inside files, extracting them can give crucial information about the binary in question [26]. It has proven to be a very efficient method for static analysis [27].

Regarding the offensive approach, although hackers vary concerning the reasons for their actions, they tend to share the way, and means of how they plan, and conduct their activities.

Table 2. Types of Hacking and respective tools

Port Scanners	Nmap
	Auto scan
Packet Sniffers	Wireshark
	TCPdump
Vulnerability Exploitation	Metasploit
	Social Engeneering ToolKit
Intrusion Detection Systems	Snort
	Netcap

As a matter of fact, Table 2 shows several techniques that are used for both offensive and defensive tasks, leaning more towards an ethical hacker approach [28].

5 Mitigation Techniques

New signatures, patches, and many more variables maintain as an imminent threat towards mitigation techniques effectiveness [29]. These techniques address multiple mechanisms to elevate its efficiency, such as [29]:

- Detection;
- Response;
- Tolerance.

Although there is a vast number of mitigation techniques out there, many studies, and reports from various entities have addressed crucial, and popular mechanisms that are approached independently of the threat that is being considered. Abstracting from the topic of the survey, we can describe mitigation as they diminish in harm or loss caused by some sort of unwanted event. On the other hand, prevention leans more towards guaranteeing that the unwanted event never happens, although some may further describe the term prevention and acknowledge that in some cases, it does look to reduce the negative impact of such situations.

Therefore, it is safe to view mitigation techniques in correlation to cybersecurity as any means or methods that lead to reducing the damage caused by a cyberattack. Such techniques will overview prevention, detection, remediation, and response mechanisms, to better mitigate any harmful tragedies.

The FBI Ransomware Prevention and Response for CISOs [30] is one of the many artifacts that will, in a way or another, end up touching on the following subjects when it comes to prevention:

- Training with a focus on threats and attacks awareness;
- Patching operating system and software;
- Advanced configuration of firewalls related to IP addresses;
- Managing access controls;
- Implementation of Security Policies.

Following the same structure as Hacking Analysis, mitigation techniques will be further analyzed with the usage of a cyberattack.

In the middle of 2014, a banking Trojan made its appearance. The so called Emotet is a malware that upon gaining access to the victims machine, it would gather information and communicate the same to a command and control infrastructure (C2 or C&C) [31]. Known to be a major threat to the financial sector in 2019 [32], the infection process would start by users opening a Microsoft Word document, earlier received through email, and upon clicking on the agreement displayed to them, the macros would activate the Emotet malware, using HTTP POST to send data from the victim's computer [31]. Regarding the financial sector, it was a major threat to the respective in 2019 [32]. Below there are listed a few mitigation measures that can be applied to protect against a malware with similar behavior:

- Blocking email attachments that can't be scanned by an antivírus software.
- Disabling file sharing services.
- Scanning suspicious email attachments.
- Implementing the suitable Access-control lists

6 Case Study

For study purposes, we will not formulate a plan to lure the victim into being attacked, but rather use a malware sample and let ourselves get attacked. This study will focus on attack analysis, from a defensive approach, covering both static and dynamic malware analysis that can be performed by everyone, independently of their knowledge on the matter.

For starters, an adequate way to boost the safety of our machine when analyzing malicious software is the use of a virtual machine. Virtualization has been steadily increasing in popularity, and it can both be used by the hacker and the defender, or victim. A virtual machine can be seen as a computer inside another computer, and it's a great way to minimize the potential damage to our main system. Furthermore, another key factor to be aware about is the network. As a defender and future malware analyst, we do not want to compromise our network. Since a malware can easily spread through a network, and proceed to infect other connected devices, this is of utmost concern. Nonetheless, we don't want to completely isolate the malware from the internet but is a key thought to keep in mind.

Following the construction of the lab, our safe environment to run the malware, we initially created a virtual machine, using the VMware software. Then, on that machine, it was installed the Windows 10 Operating System. After the installation process, it's time to download the necessary tools to do malware analysis. It's after this step that we can proceed with the configuration of the lab in ways that it won't affect the network, as previously intended.

The default network configuration has (NAT) as the Network Adapter. This was important to allow the download of the necessary tools to perform malware analysis. Now, we will change it and go a step further. One way of thinking about how one can protect a network when performing malware analysis, is to simply cut any connection to the internet. While this idea isn't necessarily the worst, a variety of malware require internet connection to act has they were designed to. If we want to understand and properly analyze the malware, we still have to allow some connection, yet find a way to control the malicious software. That's the usefulness of host-only networking. Host-only networking creates a connection between the guest and the host, containing the malware in the virtual machine while allowing some access to the internet. This way, we can better analyze it and understand what it does, like downloading other malware from the internet. Another step further would be the usage of multi virtual machines over the same concept, but it wasn't the method applied in this study.

The necessary precautions were made, and its now time to start shifting our focus to the malware. As a note, those were two main configurations that were needed in order to significantly boost our chances of guaranteeing security to our system and network, yet there are others who were taken in consideration. Version and updates of the used softwares, shared folder configurations, and USB connected devices are some of those.

Due to the nature of the chosen operating system, the antivírus that is currently working on the virtual machine is the Windows Defender. For study purposes, we want the malware to enter our system so we will be disabling Windows Defender.

The chosen samples required a password between the process of downloading them, and installing them. This is a helpful method to mitigate human error incidents when it comes to mistakes in this process.

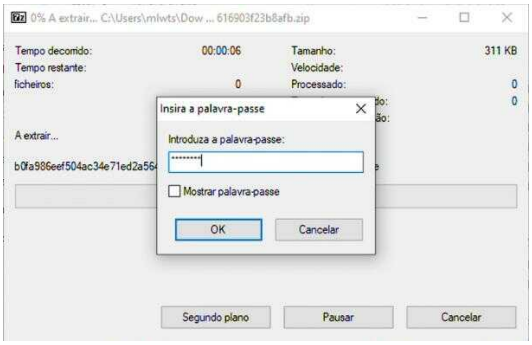


Fig. 1. Malware Sample

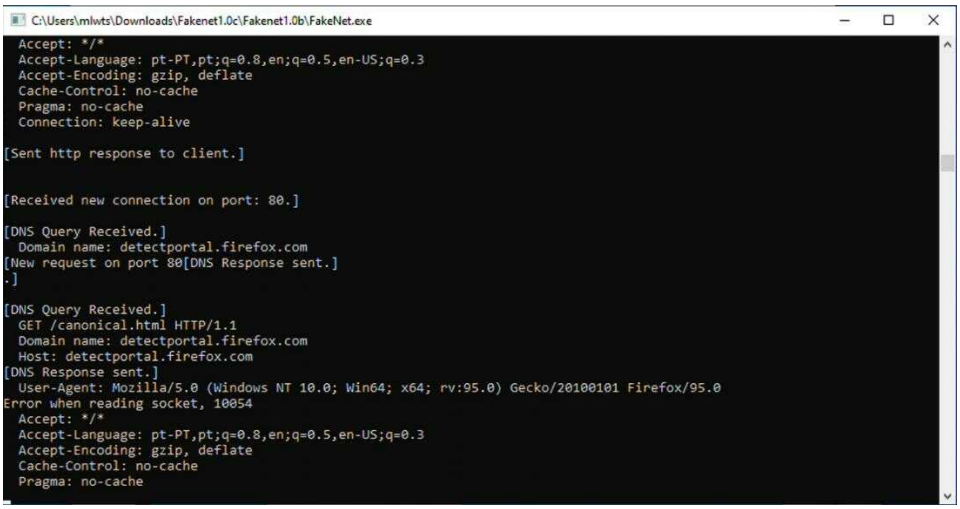


Fig. 2. Running fakenet

Furthermore, we use fakenet to trick the malware into thinking that the machine isn't isolated from the main network. It rises our chances of bypassing whatever methods the malware might have to detect if we are in environment systems or not.

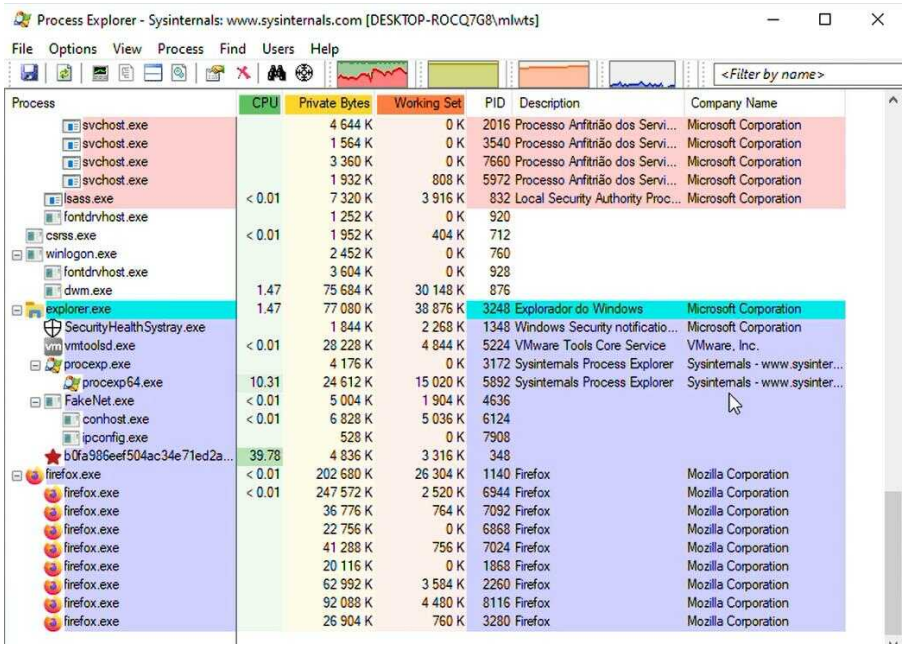


Fig. 3. Process Explorer after executing the malware

The Process Explorer is a notable tool for us to understand in real time what is happening in our system. Just from this view we can check a Process name, his description, if has any, company name, and more. If we look further into a Process, we are faced with a GUI about the respective that provides us with even more detail, such as strings and signatures.

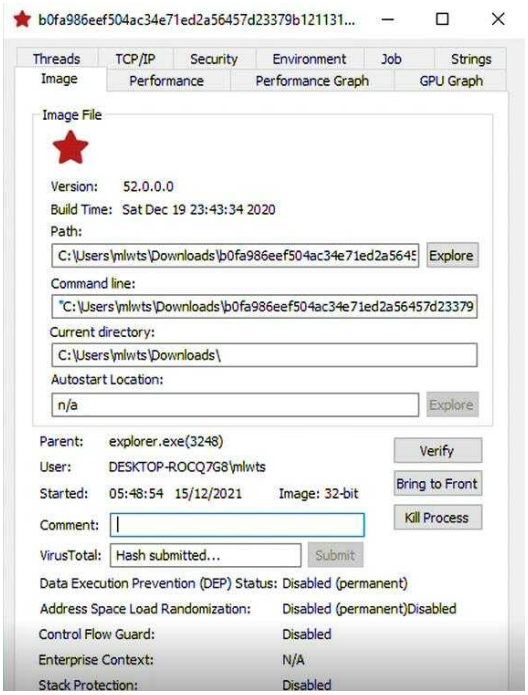


Fig. 4. Malware Process

Regshot allows us to create two shots that will monitor every change in the system between their activation. It is an amazing way to spot what changed after we run the malware. A report at the end can be made with the changes by the Comparing setting.

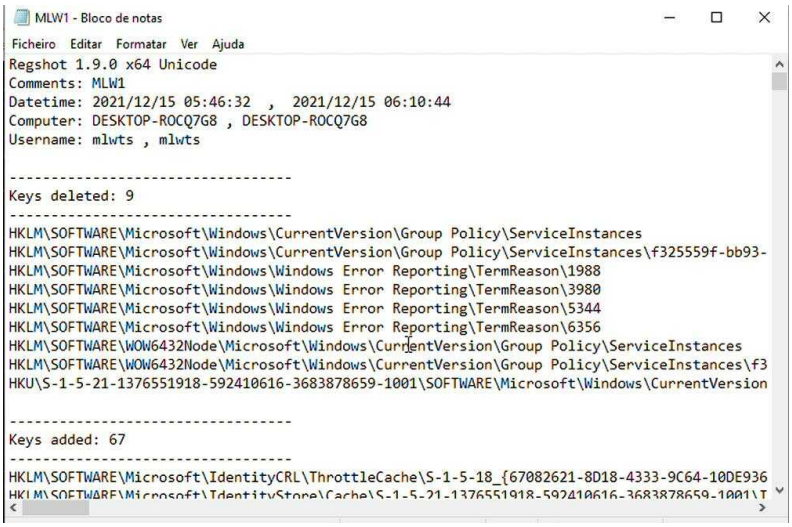


Fig. 5. Regshot Report

The information in the note is the result of the "Compare" feature in Regshot. There were a total of 309 changeswith values being changed, keys deleted and more.

Shifting back to static analysis, the MD5 hash code is the following.

Fig. 6. MD5 command and Hash

We do so in cmd, by first changing directories to the tool repository. Afterwards, we insert the following command with first, the hashing tool md5deep, and then the malware. The MD5 code was the following: 34568261ff17bda650f7c50d607fad4e.

To analyze the strings we can use the strings tool.

Fig. 7. String command

We will need to changed directories to the repository of the strings tool. We then want to run the command with the word strings, followed by the path to the malware.exe file. The following images represent portions of what was shown in the command line.

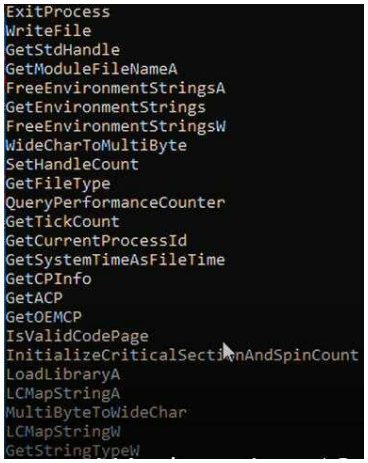


Fig. 8. Strings command outcome

The information gathered to this point was enough to have a slight understanding of this malware. It was a culmination of both static and dynamic analysis, although further investigation could be done to understand it to its fullest, while obviously requiring a deeper understanding of concepts such as dissembling. Nonetheless, we can still gather even more information by doing a search on google with the gathered data.

We can either use MD5 or SHA-1 that we retrieved from malware and check if other entities have performed analysis on this sample. As of today, this malware has been classified as suspicious by many individuals according to the website Virustotal.

7 Conclusion

Amidst the on growing surge of cyberattacks, attack analysis and mitigation techniques have shown to significantly affect the outcome of today's systems and networks security issues. Although they are generally seen as fields where only high knowledgeable individuals on the matters would succeed, there are many ways one without notable fundamentals on the subject could improve their security in regard to the mentioned network and system. The agglomerate of tools and means may be equally present in the process of a cyberattack, incident response and vulnerability check, be it to scan ports on a company's network or ARP spoofing to intercept communications.

Intending to properly understand the concepts involved in the practical demonstration, there was a first introduction to cybersecurity followed by a more focused view on attack analysis and mitigation techniques, acquiring knowledge on static and dynamic analysis for a more defensive approach. Moreover, it was introduced some tools which uses can be both for a defensive and offensive procedure.

Noteworthy, all entities that are in the slightest affected by the phenomenon's involving cybersecurity should look to continuously adapt their systems, networks, and knowledge as a means to fight back the never-ending changes and evolution of cyberattacks.

As for a future paper, going over a practical application of an offensive approach to a system or network would result in a more solid cybersecurity work. Further describing and analyzing cyberattacks would also significantly raise awareness for the possible damage derived by all the types of cyberattacks.

References

1. Sutherland, Ewan, Cybersecurity: Governance of a New Technology (March 26, 2018). Proceedings of the PSA18 Political Studies Association International Conference, Cardiff, 26-28 March 2018, Available at SSRN: https://ssrn.com/abstract=3148970 or http://dx.doi.org/10.2139/ssrn.3148970
2. SPIDALIERI, Francesca. State of the States on Cybersecurity. Pell Center for International Relations, 2015.
3. Capelão, F.; Barbosa, H.: "Cybersecurity in Healthcare: Risk Analysis in Health Institution in Portugal", International Journal for Research & Development in Technology (IJRDT), vol. 9:3, pp. 25 -31, (2018)
4. Clarke R, Youngstein T. Cyberattack on Britain's National Health Service - A Wake-up Call for Modern
5. CASHELL, Brian, et al. The economic impact of cyber-attacks. Congressional research service documents, CRS RL32331 (Washington DC), 2004, 2.
6. KIM, Bokyung; JOHNSON, Kristine; PARK, Sun-Young. Lessons from the five data breaches: Analyzing framed crisis response strategies and crisis severity. Cogent Business & Management, 2017, 4.1: 1354525.
7. YAACOUB, Jean-Paul A., et al. A Survey on Ethical Hacking: Issues and Challenges. arXiv preprint arXiv:2103.15072, 2021.
8. SINGER, Peter W.; FRIEDMAN, Allan. Cybersecurity: What everyone needs to know. oup usa, 2014.
9. Department Of Defense (2018), JP 3-12, Cyberspace Operation, Washington, DoD.
10. KOSTOPOULOS, George. Cyberspace and cybersecurity. CRC Press, 2017.
11. VON SOLMS, Rossouw; VAN NIEKERK, Johan. From information security to cyber security. computers & security, 2013, 38: 97-102.
12. UMA, M.; PADMAVATHI, Ganapathi. A Survey on Various Cyber Attacks and their Classification. Int. J. Netw. Secur., 2013, 15.5: 390-396.
13. PALMER, Charles C.. . Ethical hacking. IBM Systems Journal, 2001, 40.3: 769-780.
14. Richet, J. L. (2012). How to Become a Black Hat Hacker? An Exploratory Study of Barriers to Entry into Cybercrime (No.hal-02187741)
15. SAHARE, Bhawana; NAIK, Ankit; KHANDEY, Shashikala. Study of ethical hacking. Int. J. Comput. Sci. Trends Technol, 2014, 2.4: 6-10.
16. ISBN: 978-92-9204-536-4 – DOI: 10.2824/324797 – ISSN: 2363-3050
17. Interpol,https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

18. GORDON, Sarah; FORD, Richard. On the definition and classification of cybercrime. Journal in Computer Virology, 2006, 2.1: 13-20.
19. SIKORSKI, Michael; HONIG, Andrew. Practical malware analysis: the hands-on guide to dissecting malicious software. no starch press, 2012.
20. PRAYUDI, Yudi, et al. Implementation of malware analysis using static and dynamic analysis method. International Journal of Computer Applications, 2015, 117.6.
21. Shevchenko, Svitlana & Skladannyi, Pavlo & Martseniuk, Maksym. (2019). ANALYSIS AND RESEARCH OF THE CHARACTERISTICS OF STANDARDIZED IN UKRAINE ANTIVIRUS SOFTWARE. Cybersecurity: Education Science Technique. 62-71. 10.28925/2663-4023.2019.4.6271.
22. BAZRAFSHAN, Zahra, et al. A survey on heuristic malware detection techniques. In: The 5th Conference on Information and Knowledge Technology. IEEE, 2013. p. 113-120.
23. SIHWAIL, Rami; OMAR, Khairuddin; ARIFFIN, Khairul Akram Zainol. A survey on malware analysis techniques: Static, dynamic, hybrid and memory analysis. International Journal on Advanced Science, Engineering and Information Technology, 2018, 8.4-2: 1662.
24. CHI, Lianhua; ZHU, Xingquan. Hashing techniques: A survey and taxonomy. ACM Computing Surveys (CSUR), 2017, 50.1: 1-36.
25. Kumar, Sandeep & Gupta, Er Piyush. (2014). A Comparative Analysis of SHA and MD5 Algorithm. International Journal of Computer Science and Information Technologies. 5. 4492 - 4495.
26. Mohamed, G. A. N. & Ithnin, N. B. (2017). Survey on Representation Techniques for Malware Detection System. American Journal of Applied Sciences, 14(11), 1049-1069.
27. Lee, Jinkyung & Im, Chaetae & Jeong, Hyuncheol. (2011). A study of malware detection and classification by comparing extracted strings. 75. 10.1145/1968613.1968704.
28. KUMAR, K. Pavan; PRANATHI, K. A Survey on Ethical Hacking, Approaches, Attacks, Procedure & Reliability in case of Cyber Crime.
29. MAHJABIN, Tasnuva, et al. A survey of distributed denial-of-service attack, prevention, and mitigation techniques. International Journal of Distributed Sensor Networks, 2017, 13.12: 1550147717741463.
30. FBI, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view
31. KURAKU, Sivaraju; KALLA, Dinesh. Emotet Malware—A Banking Credentials Stealer. Iosr J. Comput. Eng, 2020, 22: 31-41.
32. KELLERMANN, Tom; YOUNG, B. Modern Bank Heists: The Bank Robbery Shifts to Cyberspace. Technical report, Carbon Black, OPTIV, 2019.
33. TUFAIL, Shahid, et al. A Survey on Cybersecurity Challenges, Detection, and Mitigation Techniques for the Smart Grid. Energies, 2021, 14.18: 5894.
34. HAWAMLEH, A. M. A., et al. Cyber Security and Ethical Hacking: The Importance of Protecting User Data. Solid State Technology, 2020, 63.5: 7894-7899.
35. SHABUT, Antesar M.; LWIN, Khin T.; HOSSAIN, M. Alamgir. Cyber attacks, countermeasures, and protection schemes—A state of the art survey. In: 2016 10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA). IEEE, 2016. p. 37-44.
36. HOQUE, Nazrul; BHATTACHARYYA, Dhruba K.; KALITA, Jugal K. Botnet in DDoS attacks: trends and challenges. IEEE Communications Surveys & Tutorials, 2015, 17.4: 2242-2270.
37. FEILY, Maryam; SHAHRESTANI, Alireza; RAMADASS, Sureswaran. A survey of botnet and botnet detection. In: 2009 Third International Conference on Emerging Security Information, Systems and Technologies. IEEE, 2009. p. 268-273.
38. PRAYUDI, Yudi. THE RECOGNIZE OF MALWARE CHARACTERISTICS THROUGH STATIC AND DYNAMIC ANALYSIS APPROACH AS AN EFFORT TO PREVENT CY.. Journal of Theoretical and Applied Information Technology, 2015, 77.3.
39. PATTEN, David. The evolution to fileless malware. Retrieved from, 2017.
40. HAMED, Zakaria A.; AHMED, Ibraim M.; AMEEN, Siddeeq Y. Protecting windows OS against local threats without using antivirus. relation, 2020, 29.12s: 64-70.
41. Alenezi, Mohammed & Alabdulrazzaq, Haneen & Alshaher, Abdullah & Alkharang, Mubarak. (2020). Evolution of Malware Threats and Techniques: A Review. International Journal of Communication Networks and Information Security. 12. 326.
42. BARIK, Mridul Sankar; SENGUPTA, Anirban; MAZUMDAR, Chandan. Attack Graph Generation and Analysis Techniques. Defence Science Journal, 2016, 66.6.
43. TEOH, Chooi Shi; MAHMOOD, Ahmad Kamil; DZAZALI, Suhazimah. Cyber Security Challenges in Organisations: A Case Study in Malaysia. In: 2018 4th International Conference on Computer and Information Sciences (ICCOINS). IEEE, 2018. p. 1-6.
44. AURANGZEB, Sana, et al. Ransomware: a survey and trends. Journal of Information Assurance & Security, 2017, 6.2: 48-58
45. N. Kshetri and J. Voas, "Hacking Power Grids: A Current Problem," in Computer, vol.50, no. 12, pp. 91-95, December 2017, doi: 10.1109/MC.2017.4451203.
46. AURANGZEB, Sana, et al. Ransomware: a survey and trends. Journal of Information Assurance & Security, 2017, 6.2: 48-58

47. Kruse CS, Frederick B, Jacobson T, et al. Cybersecurity in healthcare: A systematic review of modern threats and trends. Technol Heal Care 2017;25:1–10. doi:10.3233/THC-161263
48. Sutherland, Ewan, Cybersecurity: Governance of a New Technology (March 26, 2018). Proceedings of the PSA18 Political Studies Association International Conference, Cardiff, 26-28 March 2018
49. D. K. Alferidah and N. Jhanjhi, "Cybersecurity Impact over Bigdata and IoT Growth," 2020 International Conference on Computational Intelligence (ICCI), 2020, pp. 103-108, doi: 10.1109/ICCI51257.2020.9247722.
50. SPIDALIERI, Francesca. State of the States on Cybersecurity. Pell Center for International Relations, 2015.
51. Kuraku, Sivaraju & Kalla, Dinesh. (2020). Emotet Malware -A Banking Credentials Stealer. 10.9790/0661-2204023140.

SESSION 2

CYBER THREATS AND TECHNOLOGY SERVICES

Cyber Threats to Education Technological Services: a Case Study

João Moreira[1] and Hugo Barbosa[2] [0000-0003-1205-8990]

[1] Lusofona University, Porto - Portugal, joaobaldomero@gmail.com
[2] Lusofona University, Porto - Portugal | SIIS - Social innovation and Interactive Systems, School of Engineering of the Polytechnic of Porto, Porto, Portugal
hugo.barbosa@ulp.pt

Abstract. Information Technology systems in education have been part of the day-to-day of many schools and academic communities for many years. Thanks to the Internet and these systems, all operations in schools have become more efficient, making this sector more dependent on them. But with the transition of these systems to the education sector, the threats posed to other institutions and businesses, have propagated to the learning institutions. This paper covers some of the cyber threats that schools handle and explores the impact that the lack of knowledge about some of the basic concepts of Cyber Security can pose to educational technology systems. The threats are shortly presented and analyzed as to how they pose a threat to schools' sensitive data, providing an overview at some of the Cyber Security essentials that aim to prevent attacks or mitigate the damage that some of these threats can cause. Throughout the last few years, awareness has been raised to the importance of Cyber Security and therefore this paper seeks to find how much the academic communities in Portugal know about the Cyber Security vital concepts, resorting to a survey conducted in schools throughout the country, with the intent to investigate the knowledge that common users have seized throughout the years.

Keywords: Education; Information Technology Systems; Cyber Security; Cyber Threats; Survey Analysis; Case Study.

1 Introduction

Over the last few years, more and more organizations have become dependent on information technology systems, with the education sector not being an exception. Academia has also become dependent on the Internet, therefore cyber security has become a major concern to schools. [1]

Cyber Security experts research the threats to the cyberspace, studying how hackers can perform their attacks, detect design flaws and exploit weaknesses. Different types of threats have appeared throughout the years, but research highlights malware as a key weapon on the attackers' arsenal. [2] Malware stands for "malicious software" and it envelops a vast array of threats, all with the same objective: the infection of the target system(s); although the approach to achieve infection will vary. Common tactics include, for example, the infection of a single machine and then propagation to other

machines or deceiving a user to click on a pop-up, hyperlink or file, which proceeds to execute a drive-by download that downloads viruses or tainted files. [3] Malware can present itself in a multitude of ways, the most commonly seen being viruses, trojans, ransomware, adware, worms and spyware. [4] It can infect systems easily, but it can also easily spread, through a multitude of ways, such as an infected flash drive, through a phishing email or website or bundled with legitimate software, making it hard to contain, since it can affect systems at any point of their life cycle. Malware possesses many options of infection, spreading capabilities and an extensive span of possible victims, which include users, network devices and servers, making it one of the fastest growing and evolving threats that the cyberspace faces. [3]

Malware has the spotlight when cyber security is discussed and despite the fact that it's dangerous, it's not the only threat the cyberspace needs to face. Other threats like social engineering have come into the limelight recently and they pose just as big a threat as malware. [5]

Social Engineering is a broad term that encases a wide range of techniques that have the intent to deceive and exploit, applying different approaches in order to manipulate the common user into giving away any kind of private information. [6] These attacks attempt to bypass the cyber security systems that may be in place and exploit the human factor and, ultimately, deceiving the user. [1,7]

One of the most popular social engineering approaches is phishing. It involves a fraudulent process, masked to appear as a legitimate source while procuring to extract information from the user, usually camouflaged as a website or email. [5,8] Social Engineering exploits people through deception, making it an easy way to acquire information through the most vulnerable factor in the system, the people who use it. [9]

This paper aims to give an overview of the risks and threats to schools and their information systems. Schools are equipped with the tools to fend off attacks, however, good network design that is prepared to handle external threats is critical. It is crucial to educate the common users about basic cyber security concepts and practices.

The first section, divided into 3 parts, will analyze threats to the education technological services, exposing the major threats and risks that schools may be exposed to.

The second section presents the analysis of a survey performed in a few Portuguese schools, the results of which are the outcome of the data gathering of various members of the academic community surrounding the schools, addressing users about their basic knowledge about Cyber Security and day-to-day habits.

2 Cyber Threats to Education: An Overview

Cyber Threats are malicious acts that seek to gain unauthorized access to systems, aiming to damage the integrity of the data, sensitive or otherwise, present within the system by stealing or damaging it or just to disrupt a system or network, interrupting the system's normal life cycle. Cyber Threats are what Cyber Security aims to prevent and protect against.

2.1 Cyber Threats to the Education Technology Services

The expansion of technology services to schools provided advantages and disadvantages. It allowed professors and students to work more effectively, but with progress came some downsides; these being the threats that can potentially damage the school and its intellectual property. [10] Despite the raise in awareness over the years and investments made in Cyber Security, schools have become victims of cybercrime. [11] School systems are notoriously prone to attacks since they present themselves as an exploitation possibility with multiple avenues, as many schools possess a very lackluster Cyber Security infrastructure that, often, isn't capable of handling many of the prevalent threats. [12] Since schools are institutions that have had a significant growth in the amount of digital information acquired, it becomes difficult to implement Cyber Security measures, which leads to a problematic situation where the robustness of the Cyber Security infrastructure may have to be sacrificed, in favor of its simplicity, so the users can utilize the systems. [13]

In this regard, it's important to identify what the threats that impact schools are and that pose a risk to its technology services. The following list represents the types of threats that impact the Education sector: [14,15]

- Data Breaches,
- Malware-related Threats,
- Social Engineering Attacks,
- Denial of Service.

In the context of Education, the Privacy Technical Assistance Center describes data breaches as "any circumstance where a school's student data system is improperly accessed, compromised, or disclosed to a third party". [16] This threat can result in a wide array of complications, including identity theft, privacy violations and fraud. What makes data breaches hard to control and prevent is the many ways in which the data can be breached and leaked, which encompass theft through digital or physical means, human error, and hacking. [17]

Malware-related threats involve all sorts of malware. The most prevalent form of it is Ransomware, representing the second biggest threat type to education. These attacks can be in other forms like trojans, spyware, worms, and viruses. These malware-related threats have unique ways of operating and infecting devices, with the aim of gathering information, deleting, or altering data. [12]

Social Engineering Attacks involve different types of attacks, but the most common form is Phishing. Social Engineering is a method in which an attacker gathers information about a target through the exploitation of human weaknesses, using deception or manipulation to access sensitive information. [18] Phishing is a form of Social Engineering attack in which the attackers set out to obtain sensitive information through methods like malicious emails or websites that are designed to be as close to an admissible source as possible. [5]

Denial of Service (DoS) attacks are a major cyber threat, but it isn't as popular on the education sector, as only a slim percentage of attacks reported are DoS attacks. DoS attacks aim to exhaust the target's resources, attempting to minimize the target's service

performance or even stopping the service altogether. These attacks come in two major categories: Network Based Attacks, relying on the misuse of network protocols to flood the targets with requests, which will damage the victim's ability to provide service, and Host Based Attacks that exploit the victim's vulnerabilities found by attackers in systems or applications. [19]

2.2 The value and importance of schools' data

The education sector is a key target for attackers. According to the K-12 Cybersecurity Resource Center, in 2019, there were "348 publicly-disclosed school incidents" relating to cyber-attacks in various forms, representing a 200% increase in the number of incidents reported in 2018, displaying a worrying increase in the incident count. [14] Schools are reliant on their technology to manage and store the extensive amount of sensitive data gathered from the entire academic community (staff, students and parents).

Given these findings, it's important to analyze exactly what data most schools store and why it reaches the crosshair of hackers. Schools tend to deal with attacks by managing risks, which involves removing the source of the threat, addressing the vulnerabilities and lessening the impact by mitigating damage and restoring the regular functioning. The problem stems from the fact that these tasks are time and labor intensive, often only occurring after an attack as occurred. [20]

Schools are in possession of such a big array of data, storing an extensive amount of personal data, which comprises a big list of items, ranging from: student identification numbers, social security numbers, names, genders, race, addresses, dates of birth, city and country of residence, telephone numbers, email addresses, test scores and grades, information from members outside the student, faculty and staff group, like family members and alumni. [1]

Be it the sensitive information of students, faculty and staff or outside members, this amount of data turns schools into a bank of ample and valuable data, which puts a giant target on schools' backs [21]. Pairing the vast variety of valuable data with the fact that schools do not expend as many resources on Cyber Security as other sectors that are equally dependent on technology, we can identify a laid-back and complacent stance on a sensitive topic that can have brutal consequences. [22]

Considering the points above, it's important for schools to analyze threats and to implement techniques and best practices that allow them to better protect their information and to prevent attacks directed to their resources and IT systems.

2.3 Techniques and Best Practices Attack Prevention and Mitigation

Knowing the threats posed to Education, the value of the data and why it might be a target to intruders and attackers, it's important to know what measures to apply and how to mitigate the impact of a possible attack, taking on a proactive stance towards the Cyber Threats. In Cyber Security, it's important to take on a stance that aims to prevent and protect information and equipment, following the best practices and learning from worst-case scenarios to avoid being an easy target. [23]

The knowledge of the threats allowed us to develop techniques over the years, trying to evolve to protect against the constant surge of emerging threats. Below is a list with some of the mitigation techniques that can and should be applied, including a description of what each is and does. These are some of the most frequently used by organizations to protect the Cyber Space from the various Cyber Security Threats: [24]

- Implementation of Intrusion Detection Systems (IDS),
- Implementation of Anti-phishing Techniques,
- Implementation of Firewalls,
- Analysis of Anomalies in the Network Traffic,
- Implementation of Anti-malware software.

Intrusion Detection Systems are applications that provide constant monitoring of computer systems, alerting to when suspicious activity might be occurring. [25]

Anti-phishing techniques involve all sorts of techniques that we can implement to reduce the possibilities of a successful phishing attack. These techniques involve the use of email filters and content analysis, which is used to intercept spamming and phishing emails, the creation of Blacklists that contain a range of URLs that are known to be malicious and general best practices like only opening email attachments from trusted parties, never sending financial or personal information through email, using the latest versions of browsers, firewalls and IDS, and installing security patches when available. [26]

Firewalls are some of the most frequently implement mitigation techniques. “A firewall is a security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules”. These devices can be hardware or software based or both. They are the first line of defense in network security, establishing a barrier between the internal network and the external networks. [27

Analysis of Anomalies in the Network Traffic encompasses the analysis of all the traffic that flows through the network, making use of patterns collected from normal traffic and comparing them to the current traffic, aiming to find anomalies, enabling the possibility of enhancing and refining the network security. [28]

Anti-malware software is often associated with the term antivirus. Although both have similar objectives, succinctly, Antiviruses primarily aim to defend systems from viruses and other similar threats, Anti-malware software is way broader. It works in a spectrum that involves viruses, but bundles ransomware, trojans, worms and other threats. [29]

Along with techniques, we should consider the implementation of measures that can be encapsulated in the broader spectrum of Cyber Security. The measures below aren’t designed to just protect school’s information, it allows us to protect employees and all other users of the overarching school infrastructure and community, allowing us to implement prevention mechanisms where possible: [1,30,31, 38]

- Develop an Information Security Policy,
- Conduct Training and Awareness Raising Practices,
- Define roles and responsibilities,
- Device Management,

- Strong Authentication,
- Stay up-to-date and install security patches when available,
- Logout of websites and shut down the devices when done working.

Developing an Information Security Policy is a key step in Cyber Security. As such, one should be developed and revised as needed. It should involve what the school's objectives are and it should be presented to all parties, while advocating for compliance. A Security Policy will be helpful to lay down the guidelines that every interested party should follow, and in the process, also identifying who and what we're trying to protect, against whom or what and listing all the resources necessary to achieve said protection. [38]

Another major factor that plays into Cyber Security is the human factor. There should always be training and awareness raising practices implemented, because it doesn't matter how much security is implemented, physically or digitally. If users aren't aware of risks and good practices, they become a weak link in the defense and are open to exploitation, mainly through Social Engineering techniques. [1,5]

One integral step of writing a Security Policy is to attribute different levels of classification to information. The same way that we label information, we should attribute roles and responsibilities to the users. Every user should be conscious of their functions and roles towards information security, so that every party can be held accountable for their behavior and responsibility towards the school's security. [1]

Every device should be managed. That is to say that updates should be installed when available, devices should be password protected, install antivirus and anti-malware software. These are all good practices, but there's a different avenue to address proper device management. Personal devices like laptops and smartphones are less secure than the organization's devices; therefore, no sensitive information should ever be present in these devices. As such, this topic should also be addressed in the implemented Security Policy. [30]

Strong Authentication involves the use of more than just a Password, it applies the use of an additional identification factor. The three factors for authentication are Something you know ("SYK"), Something You Have ("SYH") or Something You Are ("SYA"). Nowadays, some systems apply the use of 2-factor authentication, which combines 2 of these factors, normally SYK and SYH. The most common combination being SYK and SYH. The Credentials are something the user knows. As for SYH, a security token is used, normally sent to the user's email address or phone number. Currently, the use of strong authentication is almost mandatory. The use of passwords is not enough anymore, so schools should implement strong authentication methods to access their resources or IT systems. [32]

Staying updated involves software and the users themselves. It's important to maintain software running its latest version. Often, security patches are launched to keep Operating Systems secure against threats and the same applies to antivirus and anti-malware software. Simultaneously, it's important for users to be informed about emerging threats and risks, particularly new phishing scams. [31]

This last practice is something that users don't realize is a dangerous behavior and this can be due to the world being progressively more connected to the internet,

especially with the Internet of Things. Users should always logout of the websites or applications that they were using when they're done using them. Along with logging out of websites, they should shut down their computers or end the session, so that access is locked behind authentication. [31]

3 Analysis of the Case Study

Regarding the theme of this paper, a case study was conducted, in the form a survey with the aim to examine the knowledge in basic concepts of Cyber Security from various members of different schools' academic communities, sent to different regions of the country, attempting to get as big a sample as possible, so as to produce discernible results that grant us the ability to analyze the knowledge of members from within said communities.

Google Forms was used as the platform upon which we built the survey itself and distributed it. This platform was chosen as a result of some factors that were taken into consideration: the ability to guarantee every participant's anonymity and the integrated tools that allow for data analysis. The survey consisted of 14 questions about the participants and their knowledge in basic concepts of Cyber Security.

The survey obtained a total of 153 submissions, of which we can display some demographic details. The following table presents the results of the population analysis.

Table 1. Demographic Information of the Participants

Age	Gender
Up to 15 years old – 30,7%	Male – 45,1%
16-18 years old – 30,1%	Female – 53,6%
19-25 years old – 7,8%	Prefer to not disclose – 1,3%
26-50 years old – 24.2%	
50+ years old – 7,2%	
Occupation	**Academic Studies Completed**
Elementary–Senior Year Student – 62,7%	Elementary School – 6,5%
College Student – 6,5%	Freshman Year – 50,3%
Elementary–Senior Year Teacher – 22,2%	Senior Year – 14,4%
College Teacher – 2%	Bachelor's Degree – 17%
Non-Teaching Staff – 6,5%	Master's Degree – 9,8%
	Doctorate – 2%

This section presents an analysis of the questions regarding the participant's knowledge of basic practices in Cyber Security that they should know and implement in their day-to-day lives. Below, there're two tables that reflect two different types of questions. The first table presents the data from five questions with yes or no answers relating to the participants' normal behavior and the second table presents the data from table two's questions 2-5 and the academic studies completed by the participants.

8

Table 2. Questions with yes or no answers

Question No.	Question	Answer (%)	
1	Do you possess any knowledge in Cyber Security?	Yes (85,6%)	No (14,4%)
2	Do your passwords include numbers and special characters? (e.g., +*!-<>)?	Yes (76,5%)	No (23,5%)
3	Do you use the same password for different services (e.g., email, social networks, etc.)?	Yes (38,6%)	No (61,4%)
4	Do you access your personal accounts on your institution's devices?	Yes (43,1%)	No (56,9%)
5	Do you access the Internet through public wireless networks (e.g., cafés, shops, etc.)?	Yes (60,8%)	No (39,2%)

Table 3. Correlation between the academic studies completed and the replies to the questions in table 2

Question No.	4th Grade	9th Grade	12th Grade	Bachelor's	Master's	Doctorate
2	Yes (5%) No (1%)	Yes (39%) No (1%)	Yes (10%) No (4%)	Yes (12%) No (5%)	Yes (8%) No (1%)	Yes (2%) No (0%)
3	Yes (1%) No (5%)	Yes (18%) No (32%)	Yes (8%) No (6%)	Yes (7%) No (10%)	Yes (3%) No (7%)	Yes (1%) No (1%)
4	Yes (3%) No (3%)	Yes (25%) No (25%)	Yes (7%) No (8%)	Yes (6%) No (11%)	Yes (2%) No (8%)	Yes (1%) No (1%)
5	Yes (3%) No (4%)	Yes (32%) No (18%)	Yes (10%) No (4%)	Yes (12%) No (5%)	Yes (3%) No (7%)	Yes (1%) No (1%)

Starting with the first table, question 1 aimed to analyze if users felt confident about their knowledge in Cyber Security, trying to establish a comparison between an initial portion of participants that felt like they possessed knowledge and the portion that did. The question itself doesn't allow us to assume anything from what the participants know, but it allows us to establish an initial number that can be useful to keep in mind for the questions that followed. An encouraging 85,6% (131) of participants reported that they felt like they had some knowledge in the topic. Even though this number is very positive, the following questions (2-5) that targeted the participants' day-to-day habits that pertain to their online security habits, showed that a generous amount of the participants doesn't know a lot of the important basics.

Starting with questions 2 and 3, as they are connected, 76,5% (117) of participants reported that they include special characters in their passwords and 61,4% (98) report that they don't reuse the same password. Regarding the use of special characters in passwords, this is a simple but easy thing to do to increase the security of passwords as they become harder to guess or to be found through brute force methods. [33] As for the reuse of passwords, it is a dangerous behavior because, assuming a hacker gets hold of a user's password, they'll have access to an array of accounts, not just the one,

possibly compromising an entire network. [34] Of the 153 participants, 55 reported to reusing passwords and 15 of them reuse passwords and don't including special characters, which is a big vulnerability.

For questions 4 and 5, the participants were asked about accessing their personal accounts in their institution's devices and if they connected to wireless public networks. In question 4, 43,1% (66) of participants reported to accessing personal accounts on their institution's devices. This shows the lack of proper device management, since these are not institutional accounts, these are personal ones that can become a vulnerability for both the users and the network, as the user may leave the account connected and not end their session and through that account, infect the network as computers in schools tend to be directly connected to the internal network, not a peripheral one. [35] Both questions pose underlying issues, but especially question 5 relates to a bigger issue, the connecting to free wireless public networks, ones present in cafés and malls. This type of behavior is dangerous for the users, especially since they may be dealing with sensitive information, and hackers may gain access to their private information stored in their mobile devices. [36]

Table 3 establishes a connection between the answers to questions 2-5 from table 2 and relates them to the different levels of studies completed. This table was created with the intention to examine how different levels of education influenced the results. With this connection established, it's worthy to note the following: 28 out of 77 participants with 9th grade completed reported that they actively reuse the same password for different services, 38 of those participants also report to accessing personal accounts on their institution's devices, 49 access public wireless networks. This denotes the need for better awareness raising between 5th and 9th grade, and possibly up to 12th grade, as a significant portion of participants that completed 12th grade show that they possess those same habits.

This covers the first two tables and the first part of the survey. The second part focuses on technical terms, and it has 2 questions. The first question is regarding phishing and the second one, ransomware. The first question possessed 3 possible answers, only one of them correct. The second question was a multiple-choice question having a definition of the term ransomware and the choices were 4, only one being Ransomware.

Table 4: Results of the questions related to technical terms

Question No.	Question	Correct	Wrong
6	Phishing is…	80,4% (123)	19,6% (30)
7	Malware is…	41,8% (64)	58,2% (89)

These two questions worked towards the same goal, but the first one being phishing had the purpose of it being a topic that has been brought to light by media outlets as of recently, also being that this type of attack sky-rocketed in recent years. [37] The overwhelming majority of participants, 80,4% (123) answered correctly to the question, but it's important to examine the fact that 19,6% (30) of participants, still don't know this term. As for the question about ransomware, this one was a bit more complicated for the participants, as only 41,8% (64) of participants answered correctly. Seeing that

ransomware is such a destructive and powerful tool in attackers' arsenals, this is an alarming response, as not even half of the participants could answer correctly.

With these results in mind, a few observations can be made. A lot of participants are aware of some of the basics and while some of the questions display a positive response, others arise a more alarming response. There can be improvement, especially in the range of 4th grade up to 12th grade, as it's in this range that most participants displayed a general lack of knowledge in Cyber Security.

4 Conclusions

There's a lot of threats that are thrown in schools' way, but with a comprehensive understanding of Cyber Security basics, everyone can benefit, and a more secure cyber space can be in sight, for all members of the academic communities. Investing in a proactive stance towards attacks and threats is the first step in protecting schools and their many members.

Overall, schools should invest in teaching Cyber Security to children and teens. As the current and future generations will continue growing up with technology, strides need to be made so the people are aware of the dangers and how to protect themselves. Keeping up with every advancement is hard, so schools should look to make strides in teaching, as to establish the principals of the subject earlier, which could go a long way in the formation and safety of children, teens, and young adults.

In this sense, schools should strive to achieve this as there is a variety of possibilities in which this objective can be reached, like lectures with experts, updating the curriculum to include a more focused emphasis on Cyber Security and demonstrations of threats and attacks in a safe environment to expose the risks and damage these threats can cause, especially to the younger and more impressionable populous.

References

1. Richardson, Michael D.; Lemoine, Pamela A.; Stephens, Walter E.; Waller, Robert E. Planning for Cyber Security in Schools: The Human Factor. Educational Planning 2020(27), 23-39 (2020).
2. Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime, https://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=coms%2Fcybercrime%2Freport.htm., last accessed on 2021/10/13.
3. Jang-Jaccard, J., Nepal, S.: A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences. 80, 973–993 (2014).
4. A Roadmap for Cyber Security Research, https://www.dhs.gov/sites/default/files/publications/CSD-DHS-Cybersecurity-Roadmap_0.pdf, last accessed 2021/10/13.
5. Breda, Filipe & Barbosa, Hugo & Morais, Telmo. SOCIAL ENGINEERING AND CYBER SECURITY. 4204-4211. 10.21125/inted.2017.1008 (2017).
6. "Hacking the human operating system: The role of social engineering within cybersecurity", Technical report, Intel Security (2015).
7. Prashant Kumar Dey, "Prashant's algorithm for password management system", International Journal of Engineering Science, pp.2424 (2016).

8. Nalin Asanka Gamagedara Arachchilage, Steve Love, Konstantin Beznosov, “Phishing threat avoidance behaviour: An empirical investigation”, Computers in Human Behavior, Vol.60, pp.185-197 (2016).
9. Mitnick, K. D., Simon, & L., W. The art of deception: controlling the human element of security. Indiana: John Wiley & Sons (2011).
10. Schuesster, J. H. Contemporary threats and countermeasures. Journal of Information Privacy & Security, 9(2), 3-20 (2013).
11. Alavi, R., Islam, S., & Mouratidis, H. An information security risk-driven investment model for analysing human factors. Information and Computer Security, 24(2), 205–227 (2016).
12. Katzan, Jr., H. Contemporary issues in cybersecurity. Journal of Cybersecurity Research, 1(1), 1-6 (2016).
13. Lestch, C. Cybersecurity in K-12 education: Schools face increased risk of cyber-attacks (2015).
14. K-12 Cybersecurity 2019 Year in Review. Part III: Cybersecurity Incidents: 2019, https://k12cybersecure.com/year-in-review/2019-incidents/, last accessed 2021/11/02.
15. Rock, A. Report: K-12 schools experienced 122 cyber-attacks in 2018. Campus Safety, (2019, February 10).
16. A parent's guide for understanding K-12 school data breaches, https://studentprivacy.ed.gov/resources/parent%E2%80%99s-guide-understanding-k-12-school-data-breaches, last accessed 2021/11/30.
17. College and University Data Breaches: Regulating Higher Education Cybersecurity Under State and Federal Law, http://docplayer.net/2539829-College-and-university-data-breaches-regulating-higher-education-cybersecurity-under-state-and-federal-law.html, last accessed 2021/11/30.
18. Nabie Y Conteh, Paul J Schmick, “Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks”, International Journal of Advanced Computer Research, Vol.6 pp.23-31 (2016).
19. Gu, Qijun, and Peng Liu. "Denial of service attacks." Handbook of Computer Networks: Distributed Networks, Network Planning, Control, Management, and New Trends and Applications 3: 454-468 (2007).
20. Sen, R., & Borle, S. Estimating the contextual risk of a data breach: An empirical approach. Journal of Management Information Systems, 32, 314-341(2015).
21. Davis, D. Best practices for balancing technology use and safety in a modern school. In Society for Information Technology & Teacher Education International Conference (pp. 1026-1030). Washington, DC: Association for the Advancement of Computing in Education (AACE) (2018).
22. Goldsborough, R. Protecting yourself from ransomware. Teacher Librarian, 43(4), 70-71 (2016).
23. Kleinberg, H., Reinicke, B., & Cummings, J. Cyber security best practices: What to do? Journal of Information Systems Applied Research, 8(2), 52 (2015).
24. Mamoona Humayun, Mahmood Niazi, NZ Jhanjhi, Mohammed Alshayeb, Sajjad MahMood. Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study (2020).
25. Jorge Gonçalves, Hugo Barbosa. A Survey of Cyber Security Systems: Approaches for Attack Detection, Prediction and Prevention (2020).
26. Jyoti Chhikara, Ritu Dahiya, Neha Garg, Monika Rani. Phishing & Anti-Phishing Techniques: Case Study (2013).
27. Cisco. What is a Firewall? https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html, last accessed 2021/11/22.

28. Félix Iglesias, Tanja Zseby. Analysis of Network Traffic for Anomaly Detection (2019).
29. Mohammed Talal, A.A. Zaidan, O.S. Albahri, Bilal Bahaa. Compreensive review and analysis of anti-malware apps for smartphones.
30. Arlitsch, K., Edelman, A.: Staying safe: Cyber security for people and organizations. Journal of Library Administration. 54, 46–56 (2014).
31. Coventry, L., Briggs, P., Bythe, J.: Using behavioural insights to improve the public' s use of cyber security best practices. Government Office for Science. (2015).
32. Do van Thanh, Jorstad, I., Jonvik, T., Do van Thuan: Strong authentication with mobile phone as security token. 2009 IEEE 6th International Conference on Mobile Adhoc and Sensor Systems. (2009).
33. Das, A., Bonneau, J., Caesar, M., Borisov, N., Wang, X.F.: The tangled web of password reuse. Proceedings 2014 Network and Distributed System Security Symposium. (2014).
34. Spafford, E.H.: Preventing weak password choices. Computers & Security. 11, 273–278 (1992).
35. Rhee, K., Jeon, W., Won, D.: Security Requirements of a Mobile Device Management System. International Journal of Security and Its Applications. 6, (2012).
36. Ayaburi, E.W., Wairimu, J., Andoh-Baidoo, F.K.: Antecedents and outcome of deficient self-regulation in unknown wireless networks use context: An exploratory study. Information Systems Frontiers. 21, 1213–1229 (2019).
37. Portugal is the 2nd country in the world most affected by spam and phishing, https://www.safecommunitiesportugal.com/cybercrimealerts/portugal-is-the-2nd-country-in-the-world-most-affected-by-spam-and-phishing/, last accessed 2021/12/2.
38. Bulgurcu, Cavusoglu, Benbasat: Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quarterly. 34, 523–548 (2010).
39. Gyunka, B. A., & Christiana, A. O. Analysis of human factors in cyber security: A case study of anonymous attack on Hbgary (2017).
40. Aziz, A. The evolution of cyber attacks and next generation threat protection. RSA Conference (2013).
41. Blythe, J. Cyber security in the workplace: Understanding and promoting behaviour change. Proceedings of CHItaly 2013 Doctoral Consortium 1065, (pp. 92- 101) (2013).
42. Atkinson, S., Furnell, S., Phippen, A.: Securing the next generation: Enhancing E-safety awareness among young people. Computer Fraud & Security. 2009, 13–19 (2009).
43. Javidi, G., & Sheybani, E. K-12 cybersecurity education, research, and outreach. In 2018 IEEE Frontiers in Education Conference (FIE) (pp. 1-5), Cincinnati, OH. IEEE (2018, October).

Cyber Threats to Healthcare Technology Services: a Case Study

Eduardo Neves[1]

[1] Lusofona University of Porto, Portugal
eduardoneves_12@hotmail.com

Abstract. Health is a vital industry in our society, and as we speak, we are evolving too, to another level, because we feel this need to simplify things, and that's where technology plays the major role in order to simplify and help us.
Since, as is normal in many organizations, hospitals started using electronic-based-systems so they can have easy access to so much information at the same time, things that were impossible to do in the previous time. However, there's no such thing as perfection and so aren't we. Nowadays, the healthcare industry is one of the prime targets for cybercrime, cause just like every industry in this "recent world" is surrounded by vital and confidential data. Hospitals, for instance, have a lot of important information about their patients, like sensitive, personal information or even financial. Therefore, it is mandatory to invest in new technologies, tools or even ways to prevent and control the risks of cyber attacks, for example, and protect this vulnerable industry.
The purpose of this article is to identify cyber security "trends", methods, results, consequences and measures that must be taken to face this problem.
The document also includes a study carried out with the support of information collected in a survey carried out with several health professionals in Portugal from various health institutions.

Keywords: Cybersecurity, Health, Threats, Attacks, Integrity, Confidentiality, Vulnerabilities, Cybercrimes.

1 Introduction

In recent years, as digital technologies feed into the backbone of the world economy, it is a critical resource, underpinning the complex systems that keep economies running, such as finance, healthcare, energy and transportation. Many of today's business models are based on the constant availability of the Internet and functioning information systems [1].

Technology is being used in our day-to-day lives, both in our work and in our relationship with people, it allows us to create greater possibilities of interactions between several people, which also, consequently, increases the associated dangers, because not all interactions with third parties are known interactions. On the internet, it is easy for malicious people to impersonate other people to gather information for malicious

purposes, often without the knowledge of the people who provide the information in an innocent way because they do not know they are being victims of cyber assistance [2].

To steal data from a hospital, hackers use, for example, Social Engineering. For this to happen they send an email containing links or attachments to employees and when an employee clicks on the attachment or link it will immediately infect the user's computer and start to spread throughout the health care system and thus obtain a fair amount of data from both patients and hospital staff [3].

A cybersecurity attack can result in a variety of threats, from simple identity theft to extortion attempts and loss of personal data. There are several organizations that must be protected in order for our society to function normally, such as hospitals and financial services companies, because they contain a large amount of valuable information, such as personal data, addresses, telephone numbers, contacts, etc [4].

As for the evolution of cybercrimes in the health sector, we can see that there was an increase compared to the year 2019, as that year the health sector was in the tenth place of the most attacked sectors of the year, with only 3% of the methods, but in 2020 it went from tenth place to seventh place with 6.6% of all attacks. The most used attack against the healthcare industry in the year 2020 was ransomware, accounting for 28% of attacks. A ransomware attack can be particularly devastating, as we can see in September 2020 in a German hospital, where the attack forced an ambulance to take a patient to another hospital 20 kilometers away, after this trip the patient died. German authorities determined that the attack did not play a decisive role in the death, but nevertheless, prompted that the patient could not receive the help he needed [5].

The purpose of this document is to raise awareness of the current status of technological health services, the vulnerabilities and risks of cybersecurity in health, and also to analyze the data from the case study. The purpose of the case study is to understand whether healthcare professionals act to prevent attacks and also to understand what they know about cybersecurity. Therefore, a survey was carried out and answered by several health professionals from different institutions.

2 Cyber Security in Healthcare

Cybersecurity is not just about the software, but also about who uses the network, as many people think that cybersecurity is just about protecting the email, the operating system and the network. It is a fact that this represents a slice of cyber security, but the largest share are the system’s users who play an important role in ensuring that organizations, in this case hospitals, are protected, for which it is necessary to provide prior training in the best practices that can help minimize the risk of a cyber-attack happening [6].

Cyber security in healthcare must be more efficient than in other areas due to the type of data circulating in the healthcare sector, because it can put a patient's data at risk and subsequently have consequences for the same. For example, when a credit card is stolen from us, the bank cancels the card and issues a new one and consequently refunds the customer. But in case the PHI (any identifying information linked to any kind of clinical data - for example a diagnosis) of a patient is stolen, the patient cannot

change the data that was there, for example the date of birth, his blood type generally cannot alter your genetic and health information, and this information is very valuable for a variety of crimes. Health information is considerably more valuable on the dark web where it sells for 10 to 20 times more than, say, your credit card number [7,8].

There are several factors that shape cyber health risks:

- A rapid introduction of digital systems by the healthcare industry.
- The emergence of health data as a high value to cybercriminals as it contains a lot of sensitive patient data and confidential data.
- The evolution of health associations as targets for hacktivists and nation-states.
- And the difficult implementation and maintenance of security controls derived from the technical and organizational aspects of the industry [9].

3 Risks and vulnerabilities of cybersecurity in the healthcare

A security vulnerability is a weakness that allows an attacker to compromise the confidentiality, availability, or integrity of a computer system. A weakness can be the result of design choice, poor management, implementation failures or even human error, which can compromise the security of the entire system and in addition, affecting the software can also affect the hardware [10].

3.1 Threats, Health Attacks and Consequences

Threats and vulnerabilities go hand by hand, but they are not interchangeable. Threats are internal or external activities or events with the potential to attack the quality, efficiency and profitability of an organization. For example, hurricanes are one at the external threats that can cause serious damages like power outages. A threat can also be an employee who decides to steal data or harm your practice [11].

Health attacks pass for cyberattacks. Cyberattacks can occur in many different ways hoverer the main attacks are always intended to harm control systems or valuate datas.

One is used to block or manipulate a physical structure, the other one is more diverted to steel fragile datas. You have to garantie that the confidential information's you consequently have may not "fall" on the wrong hands. They can norm others or systems for their own benefit [23].

As the healthcare industry becomes more dependent on technology, on a daily basis, its cybersecurity challenges are increasing. To help protect organizations, you need to understand these challenges. The following are the main cybersecurity challenges that healthcare organizations need to be aware of:

- Malware and ransomware attack
- Phishing attack
- Date breaches
- Insider threats

- Distributed denial-of-service (DDoS) attacks
- Cloud threats [12]

Threat: Malware and ransomware attack

Ransomware is a type of malicious software (malware) used without the knowledge of the owner or the common user. It is used to infect, block, and encrypt the victim's data, denying him access to that same data. In order for the victim's data to be rescued it is usually necessary to pay a ransom for the software to be removed, then it is up to the attacker to remove it or not [13].

This threat usually comes into contact with the user, through advertisements for websites that contain malware or through phishing campaigns. It works as follows, upon delivery, the ransomware identifies the data that is to be encrypted through a list of embedded file extensions and encrypts that data. After encryption, the ransomware leaves a notification for the user to pay the aforementioned ransom [14].

Threat: Phishing attack

Phishing is a method of using a fake email to try to collect private information, distribute malware or even commit fraud. It is usually carried out with the intention of committing identity theft, gaining access to the victim's credit cards and bank accounts or, in healthcare, having access to all patient data. Attackers use various tactics to trick the email recipient into believing that the email they received is genuine [15]. Phishing typically requires the recipient of the email to take an action, which relies on social engineering techniques, therefore impersonating trusted sites such as financial institutions, administrators, or healthcare personnel [16].

Threat: Data breaches

The healthcare industry experiences more data breaches than any other industry. Health has been impacted by an average of 2.8 million breaches per month, the need for proper device management and monitoring, as well as the protection of confidential information.

The problem is, although the requirements enforced by HIPAA (Health Insurance Portability and Accountability Act) law are in place, most organizations do not have the resources to stay informed about the security measures that must be up to date. This offers a great opportunity for cybercriminals to easily gain access to patient information [12].

Threat: Insider threats

An internal threat is one of the greatest threats to the health care environment. For example, we may have an attacker who could hide inside the healthcare organization to gain access to devices on physical media or even infect them through wifi, bluetooth or other tools. Internal attacks can leak confidential information from both patients and employees and can even paralyze the entire network [17].

These types of attacks can be caused by current or former employees, executives, administrators, in short, everyone working in the organization. A theft of credentials can be considered an internal threat because external attackers use these credentials to gain access to confidential and valuable data [12].

Threat: Distributed denial-of-service (DDoS) attacks

A DoS attack is parallel to a DDoS attack but takes very different forms. DoS requests exist in one of two broad ranges: Denial of Service (DoS) and Distributed Denial of Service (DDoS). Offers are offered by a single attacker with the aim of making an application, service, or machine inaccessible. DDoS attacks are an attempt to flood an organization's network with Internet traffic to the point where it cannot operate or function normally [18].

DDoS attacks use multiple devices to launch DoS attacks in one or multiple directions. A DDoS attack is made up of four elements:

- The real attacker.
- The compromised handlers or hosts, which manage to control multiple agents.
- Zombie hosts, responsible for producing the distribution of packages to the final recipient.
- Lastly, a victim or host [19].

Threat: Cloud threats

Cloud security is a big challenge and slows down the spread of cloud to cloud. In a CSA report related to cloud security, experts identified critical ratings such as data breaches and loss or unsafe APIs [20].

Healthcare associations are switching to cloud data storage solutions due to their data recovery simplicity, but unfortunately not all solutions are HIPAA compliant [12].

3.2 Prevention of Threats and Attacks

At this point, there are some measures and recommendations for improving cyber security in the health area. To improve cybersecurity in the vast healthcare IoT ecosystem, the following measures need to be taken:

- Cybersecurity training and awareness programs

- Ensure secure settings
- Remote administration of servers, work, and network devices, etc. on secure channels
- Computer technology standardization
- The cost-benefit sharing. It is important to understand the commitment between cyber security measures and their effect on services.

There are also recommendations that should be taken into account:

- Implement state-of-the-art security measures
- Conduct tests and audits regularly
- Risk assessment and vulnerability assessment
- Establish an information security sharing mechanism
- Maintain a firewall configuration, which firewall must be placed on each external network interface
- Promptly revoke access to users who should no longer have access
- Protect encryption keys from misuse or disclosure [21] [22].

4 Case Study

To carry out the case study, a survey was carried out, aimed at health professionals with and without computer park management responsibilities, in order to collect data relating to the evolution of technologies with the evolution of care for the common user and to verify whether the health professionals in Portugal are aware of cybercrime and cybersecurity.

This survey was carried out with 151 health professionals from various health organizations in Portugal and from various positions at the professional level.

The first piece of information obtained from the respective survey was whether people have any knowledge of cybersecurity, where the graph below was obtained.

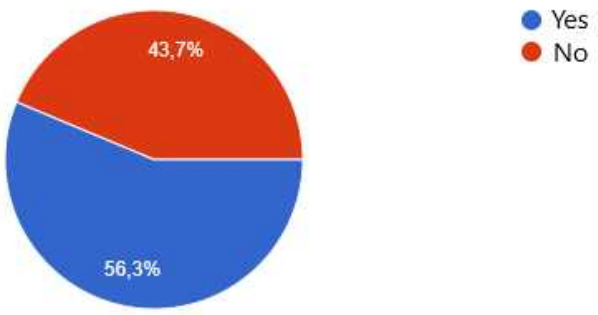


Fig. 1. Results obtained in the question: Do you have any knowledge about cybersecurity?

Observing the pie chart above, we can see that 56.3% (85) health professionals have some knowledge of cybersecurity or think they have some knowledge because many people say they have knowledge of cybersecurity when, in reality, they do not have it, and we also verify that the remaining 43.7% (66) confess that they are not sensitized to cyber security (figure 1).

With the information above only, we cannot conclude that our healthcare professionals are cybersafe, so we carried out more questions to verify their knowledge and actions in cybersecurity.

The first rule that a majority of people know is that we must have a strong password that is difficult guess, so to check if healthcare professionals were following it, a question was asked where we got the following data.

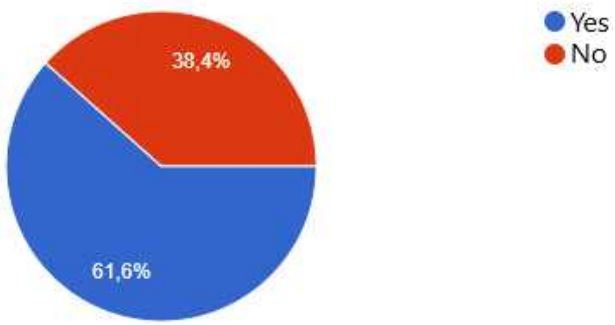


Fig. 2. Results obtained in the question: Do your passwords contain at least 9 characters and do they contain special characters (~ ! @ # $ % ^ &)?

Observing this chart, we can see that 61.6% (93) health professionals have a password with at least 9 characters and special characters, that is, here we can see that even some people who do not have cybersecurity knowledge use a secure or minimally secure password (figure 2).

But it's no use having a secure password if we use the same password for different services because even if the password is secure, it runs the risk of being discovered.

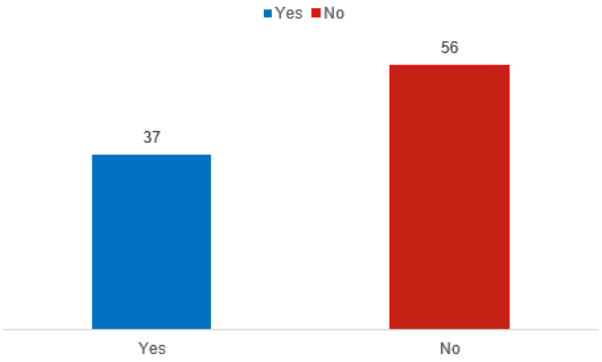


Fig. 3. This graph indicates the number of health professionals who have a secure password, but use it for the different services they use

As mentioned above, even with a secure password, we run the risk that it will be discovered. In this chart we have the number of health professionals who, despite having a secure password, use this password for the different services they use, which seriously increases the risk of data loss (figure 3).

For data to be lost, there must be an attack and two of the most frequent attacks on anyone's devices, not only in terms of health, are ransomware and phishing. To better understand if these healthcare professionals know what phishing or ransomware is, there are two questions in the survey that will give us that answer.

Fig. 4. This chart indicates healthcare providers' responses to the question: What do you understand by the term Phishing?

With the help of the graph, we can see that 56.3% (85) of health professionals correctly answered what phishing is when they say that it is the practice of sending

fraudulent emails that seem to come from a reliable source, but we still have a large number of people who simply do not know what phishing is, bearing in mind that this is one of the most well-known terms in society (figure 4).

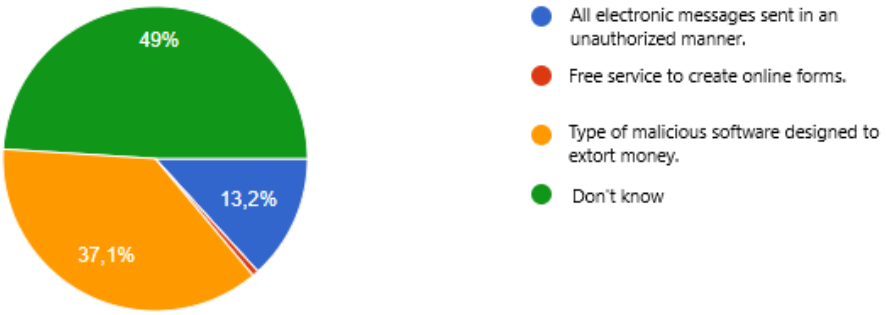


Fig. 5. This chart indicates healthcare professionals' responses to the question: What do you understand by the term Ransomware?

Ransomware is a term that is not as well known by society but it is one of the main threats to the healthcare sector as seen above, therefore it should be necessary that all healthcare professionals be alerted to this threat, but as we can see in the chart above only 37.1% (56) health professionals know what ransomware is, which highlights the fact that the vast majority do not know what ransomware is (figure 5).

A ransomware or phishing attack can attack the healthcare sector through healthcare professionals, so even in the survey there are 3 fundamental questions for us to verify that healthcare professionals act in a way to be safe personally, and for their organization.

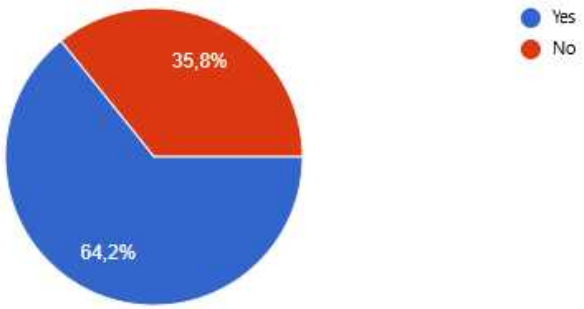


Fig. 6. This chart indicates the responses of healthcare professionals to the question: Do you access wireless networks in public spaces?

The first question concerns whether healthcare professionals access wireless networks in public spaces with their devices (figure 6). Based on the graph, 64.2% (97) of health professionals perform this bad practice that makes them susceptible to external attacks.

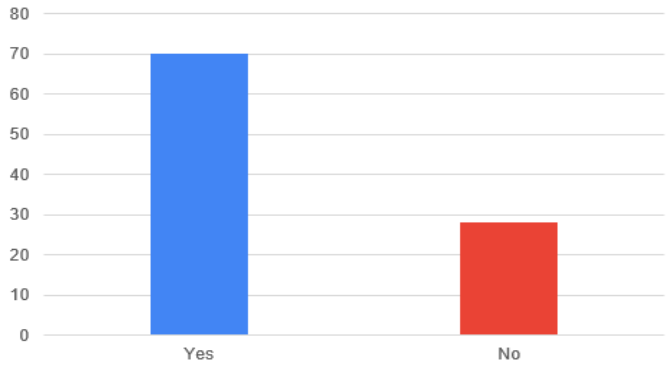


Fig. 7. This graph is the result of the answers of health professionals who answered yes to the previous question and the answer to the question: Do you access the wireless network in the workplace through your personal equipment? (ex: Mobile phone, laptop)

The second question concerns whether healthcare professionals access the wireless network of the organization where they work through their personal equipment. In figure 6 we can see that 97 professionals answered yes and 70 of these health professionals answered that they access the wireless network of their work organization with their personal equipment (figure 7). If these 70 had already performed a bad practice when accessing public wireless networks, they further aggravated the situation because their personal equipment could contain a virus that could pass to the network and contaminate the network and thus the organization is all contaminated.

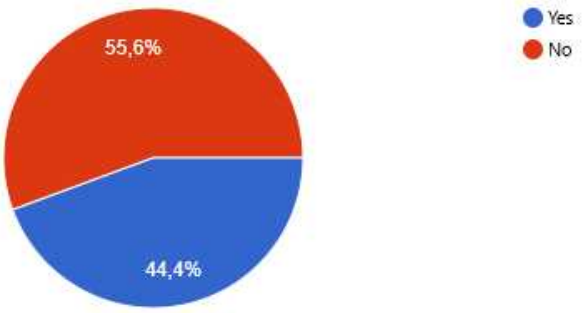


Fig.8. This chart indicates the responses of healthcare professionals to the question: Do you access your personal accounts on computers at the institution where you work? (ex: social media, email, etc.)

The third question concerns whether healthcare professionals access their personal accounts on the computers of the organization where they work. Based on the data acquired, we can verify that 44.4% (67) of participants pose a major threat to their work organization's network because they can mistakenly open an email that appears to be trustworthy and is actually a phishing email (figure 8). That's when the ransomware takes the opportunity to be masked in the links or files that the email contains. After this happens, we have a ransomware attack across the organization's network.

5 Conclusion

The healthcare industry is a sector that contains a large amount of sensitive data and continues to be very vulnerable.
Completing the case study, we can verify from the data collected from the survey that health professionals in our country are not properly informed about cybersecurity and cybercrime. To solve this problem, lectures to raise awareness of cybercrime / cyber security could be a step forward and policies created in their work organizations so that windows of opportunity are not created for an attack. While we can expect an increase in the number and types of threats throughout the years, we also have access to security measures that can reduce our exposure to being compromised.

References

1. "EU cybersecurity initiatives", https://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf pp.1 (2017)
2. Cavalcanti, C., “Cyberdefense: Challenges and comparative legislation between Brazil and Portugal”, (2017).
3. Shweta Vivekananda Kondewar, "Cyber Security in Healthcare", pp.146 (2021)
4. “What Is Cybersecurity?”, https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html#~how-cybersecurity-works
5. IBM,"X-Force Threat Intelligence Index ", pp.43 (2021)
6. Maria Christina,"What is Cyber Security", pp.1(2020)
7. Salem T. Argaw , Juan R. Troncoso-Pastoriza , Darren Lacey , Marie-Valentine Florin , Franck Calcavecchia , Denise Anderson , Wayne Burleson, Jan-Michael Vogel , Chana O’Leary , Bruce Eshaya-Chauvin and Antoine Flahault,"Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks", pp.2(2020)
8. Luna R, Rhine E, Myhra M, Sullivan R, Kruse CS. "Cyber threats to health information systems", (2016)
9. Symantec, "Cyber Security and Healthcare: An Evolving Understanding of Risk", pp.2 (2017)
10. "Vulnerabilities and Exploits", https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/vulnerabilities-and-exploits
11. U.S. Department of Health and Human Services, "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients", pp.5(2018)
12. “The Top 6 Cybersecurity Challenges in the Healthcare Industry”, https://securityscorecard.com/blog/top-cybersecurity-challenges-in-healthcare-industry

13. David P. Paul III, Nikki Spence, Niharika Bhardwa, Alberto Coustasse Dr.PH, MD, MBA, MPH,"Healthcare Facilities: Another Target for Ransomware Attacks", (2018)
14. Dr. James Angle, Michael Roza, Vince Campitelli, Alex Kaluza, AnnMarie Ulskey “Ransomware in the Healthcare cloud”, (2021)
15. Scott Rose, J. Stephen Nightingale, Simson Garfinkel, Ramaswamy Chandramouli,"Trustworthy Email", (2019)
16. Ward Priestman, Tony Anstis, Isabel G Sebire, Shankar Sridharan, Neil J Sebire "Phishing in healthcare organisations: threats, mitigation and approaches ", (2019)
17. Meng, Weizhi, Li, Wenjuan, Wang, Yu, Au, Man Ho “Detecting insider attacks in medical cyber–physical networks based on behavioral profiling” (2020)
18. Bhawna Tripathi, Dr. Devesh Katiyar, Gaurav Goel,” A Study of DDoS (Distributed-denial-of- service) Attacks and Its Preventions”, (2020)
19. Akhil K.M, Rahul C.T, Athira V.B, "Distributed Denial of Service (DDoS)Attacks and Defence Mechanism", (2021)
20. Jitendra Singh, “Cyber-Attacks in Cloud Computing: A Case Study”, (2014)
21. Enisa, “Smart Hospitals”, (2016)
22. Mohammed M. Alani, “Securing the Cloud: Threats, Attacks and Mitigation Techniques”, (2014)
23. Filipa Capelão, Hugo Barbosa “Cybersecurity in Healthcare: Risk Analysis in Health Institution in Portugal”

Cyber Threats to Mobile Technology Services

Rita Mendes de Azevedo

Lusófona do Porto University, Portugal
ritamendesazevedo@gmail.com

Abstract. With the evolution of technology, we started to see an increase in the usage of mobile technology daily, which for many has become an obligation or necessity due to their work or studies. Consequently, mobile device users over the years started using them more frequently for personal use or work. There are different types of mobile technology like cell phones, tablets, computers, or other devices we can find in companies. Despite the security methods provided by the creators of the operating systems, like android and iOS, they are not enough to protect the users from all the threats that come up daily, such as malicious websites or even emails intended to steal user data.

The emergence of the COVID-19 virus in the year 2020 led most countries to confinement. COVID-19 virus caused mobile technology users to use their mobile devices even more often, consequently, all the attacks and threats became more frequent, but we don't know if our knowledge is necessary to prevent ourselves.

In this paper, will be possible to find the necessary tips to help users protect themselves from these cyber threats and help the readers to learn more about specific threats.

The threats can have different environments and not only is it important to know how to protect our mobile devices from all kinds of threats and attacks but for companies becomes even more important because the damage can be more catastrophic.

Keywords: Mobile Technology, Mobile Technology Services, Cyber Threats, Threats, Mobile Threats, Phishing, Malware, DoS, DDoS, Mobile Security, Tips

1 Introduction

Cyber Threats are one of the biggest problems for mobile device users today. The present group of devices can be of various types like our mobile phones, tablets, laptops, and other devices we use daily.

Cyber threats to mobile devices can include various types of threats and theft, such as the security of our personal data, for example, banking data, privacy, and disrupting our mobile device, whether for personal use, like a mobile phone or tablet of the company we work for. By cyber threats, we mean different types of hacker attacks, as well attacks that can insert malicious code into our devices or even, have the objective of attacking the network we are connected to, and malicious messages with a suspicious link sent to our email or by message to our cell phone.

According to [1] Android devices are the most used and then iOS devices. According to their studies, access to Android devices has been increasing, leading users to need to be more careful.

Consequently, in 2020 the COVID-19 virus appeared, which caused several health problems to the world population, which forced the government of each country to take measures to protect the population while laboratories studied the virus. One of the solutions adopted was confinement, which gave online classes to students and workers working at home. Without the opportunity to leave the house except to buy essential goods, the population was forced to use their electronic devices often, whether for entertainment or to communicate with their family and friends or even for work, thereby, the use of mobile devices increased as also online shopping. With this increase in the use of electronic devices, hackers saw more opportunities to fraud the deceive users and, cyber threats became more frequent.

Sometime later the pandemic started, vaccines against COVID-19 from different laboratories began to be created, and with the vaccination, was created platforms and messages started to be sent for citizens to get vaccinated, according to [2] resulted in a Malware target, and the mobile device's users received fake messages.

Moreover, companies that use mobile devices can also be affected by cyber threats. Although the use of security measures is not inevitable, as any user within the company is connected to the network and takes some action that compromises the network and its data, that's why it's important to have a basic understanding of where certain threats can arise, and especially to avoid the use of company's devices or network for personal use.

In this paper about cyber threats to mobile technology services, different topics will be covered. The topic, Most popular cyber threats, talking about the threats that most affect mobile users' devices and give tips on how to prevent them, the topic, Types of Mobile Threats, talking about the different "environments" from which cyber threats can arise and the topic, How to protect Mobile Technology from Threats, where tips are provided on how to protect both personal and corporate mobile devices.

2 Most Popular Cyber Threats

The various threats to mobile devices mainly occur in the form of malicious code distribution that exploits the operating system and application vulnerabilities. These threats mostly appear by email or message on users' devices.

In this topic, we will see some of the ones that most affect mobile device users and give some tips on how to prevent them.

2.1 Phishing

A current case that catches many people even possibly our friends and family. A phishing attack is done in the form of a message or an email, containing a link for the

victim to open, in which the attackers pretend to be an entity they aren't to make the attack credible.

These attackers usually steal victims' sensitive data such as credit card details or login credentials. This happens when the victim clicks on any link sent by the attacker who takes the form of a genuine entity.[3]

Typically, the most common data stolen by attackers are bank account numbers, usernames, and passwords, credit card details, internet banking details.[4]

Below is an example of a phishing message, where we can see a message received from a personal number, to let me know they have my order waiting for delivery and, to access the link to know more details. In the warning found above with the alert icon, the system is asking if the message received is spam and, if I want to set the number as "Not Spam". The sender's telephone number is usually a personal number, in some cases the message received is already given as a spam alert as seen in the example. This alert occurs due to the user's complaint, in this case, the device presented is an android phone, this helps other users to be careful when receiving the message. Whenever a suspicious message is received it is possible to report the mobile number.

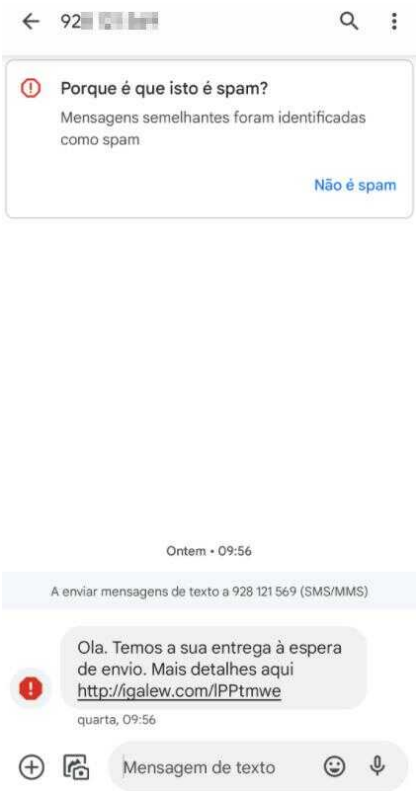


Fig. 1: Phishing message received on an Android phone

2.1.1 Phishing in Portugal

With the pandemic and the increase in online shopping, more phishing attacks emerged, where attackers claimed to be legitimate companies. One of the most frequent mobile device threats that possibly many of us suffered in Portugal, was receiving messages on our mobile phones indicating that our order was in customs and, for dispatch was necessarily accessing the link to pay if we wanted to receive the package, in some cases the user of the device had not even placed any order. For some people with less knowledge about Phishing, people looked for help on social media.

According to [5], phishing was one of the most recorded events. Consequently, one of the cases, the most frequent crime based on the registration of complaints to the PGR Cybercrime Office is fraud in the use of MBWAY, with phishing in 2nd place.

2.1.2 Phishing life cycle

A phishing attack is made up of a cycle with several steps.

The first step is planning, the attacker starts by planning the attack, identifying the victims, the target information, and the technique to use in the attack. Following, the attacker starts the "collection" step, as soon as the victim takes an action making him susceptible to information theft, he is then urged to submit his credentials through a trustworthy-looking webpage. Normally, the fake website is hosted on a compromised server, which has been exploited by the attacker for this purpose. The last step is given by "Fraud", finally, and once the attacker has achieved his goal, he then becomes involved in fraud by impersonating the victim.[6]

2.1.3 How to prevent phishing

In the case of receiving e-mails, it is necessary to pay attention if the e-mail address corresponds to the real company/entity, sometimes attackers create accounts with a similar e-mail address, changing insignificantly for users not to notice.

As for the phishing attempt by receiving a message on the mobile phone, it's necessary to pay attention to the address of the link sent, for most people it is easy to notice that it does not a legitimate link, in case of doubt, the attempted attack is almost always made by a personal mobile number of an operator. It's recommendable searching for the contact on google you can find information and comments about the contact on specific websites.

To test your knowledge of recognizing phishing attempts you can consult sites like phishingquiz.withgoogle.com, it will help you to increase knowledge about phishing.

2.1.4 Simulate phishing with Microsoft Defender

Although building a phishing website is a time-consuming and complicated process, it is possible to find phishing attack simulators to test your companies' policies and practices.

One of the most suitable is the Microsoft simulator, to have access you must have the Microsoft Defender for Office 365 plan 2.[7]

It is possible to select different techniques such as credential harvest (attempts to collect credentials), malware attachment, link in attachment, kink to malware, drive-by URL. The malicious URL in the message takes the user to a familiar-looking website that silently runs and/or installs code on the user's device.[7]

In each one, when selecting the desired one, first the name and description of the simulation are defined, then on the "payload" page, it is possible to define the language and view information such as the number of people who clicked on the link. For this same simulation, it is possible to determine specific users and groups for which it is intended and to carry out and simulate training in order to test the employees' knowledge.[7]

2.2 Malware

Malware is a contraction of malicious software, is designed to destroy computer systems and programs. It has many forms such as virus, worm, Trojan, and spyware. Malware can attack personal and organizational computer systems.[8]

2.2.1 Trojan

Given as a type of malware, Trojan is a program in which the code contained is harmful or data that takes control and its chosen form of damage, such as ruining or erasing data on the hard drive. A Trojan can cause massive harm to computer systems and may turn a system into a killing machine as well.[9]

2.2.2 Worm

Given as a type of malware, Worm is a program that self-propagates across a network exploiting security or policy flaws in widely used services.[10]

For a worm to infect a machine, it must first discover that the machine exists. There are several techniques for discovering multiple machines such as pre-generated target lists.[11]

2.2.3 Spyware

Given as a type of malware, Spyware is a type of software that can install itself or run on a user’s computer without providing notice, consent, or control to the user. Usually hidden among other programs or can be unwittingly downloaded to a user's system when specific websites are visited.[12]

2.2.4 How to prevent Malware

As [13] says, we can prevent Malware in the following ways:

- Keep your computer's current software up to date. The operating system and anti-virus application must be updated regularly.
- Always think before you install something. You don't know if the lengthy license agreement that you normally don't read, area waring you are about to install Spyware.
- Only download updates from reputable sources.
- Install and use a firewall.

2.3 Application Vulnerability

According to [14] application vulnerability is threats that perform malicious actions such as elevation of privileges by using the vulnerability of the developed application.

2.3.1 How to Prevent Application Vulnerability

This threat is aimed at programmers, according to [15], to protect applications some of the needs are, developing secure code, input validation, hotspot protection, output validation, and vulnerability detection.

2.4 DoS (Denial of service attack) and DDoS (Distributed Denial of service)

According to [16] denial of service (DoS) attack occurs when users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor. Affected services may include for example e-mail, web-sites, online accounts, or other services that are dependent on the affected computer or network. While DDoS attack occurs when multiple machines are operating together to attack one target.

2.4.1 Attack Symptoms

Both DoS attack and DDoS have the same symptoms, these are slow network, Unavailability of a particular website, or an inability to access any website. [16]

2.4.2 What to do if you are experiencing a DoS or DDoS attack

Most likely this type of attack happens in companies, but it is not inevitable that it also occurs in our home network when we are experiencing a DoS or DDoS attack it is possible to take some measures.

When we are targets of DoS and DDoS attacks, we can contact our network administrator to confirm whether the service outage is due to maintenance or an in-house network issue and contact our ISP to ask if there is an outage on their end or even if their network is the target of the attack and you are an indirect victim. [16]

3 Types of Mobile Threats

Threats to mobile devices can arise in several ways, as mentioned in the previous topic, in addition to cyber threats made by hackers, threats can be of other categories.

3.1 Physical Threats

Physical attacks can, as the name says, be practiced at the physical level by the attacker. Under these circumstances, it is easier to carry out a physical attack on a mobile device than on a computer, for example, our mobile phone despite being constantly with us, is more difficult to perceive its absence than a computer and it is faster for us to notice that disappeared due to its size.

The attacker can, through physical access to a mobile device, perform malicious actions, such displaying as flashing it with a malicious system image, that is connected to a computer to install malicious software or conduct data extraction. So, it is important not to leave devices unattended so that this type of threat does not occur. In addition, device authentication and encryption need to be applied to secure mobile devices against unauthorized access.[17]

3.2 Network-based Threats

You've probably read or heard cases of attacks on corporate networks on the news, so it's important to be careful when using a wi-fi network or even with whom you connect to your home/business network and, in addition to using Wi-Fi, be careful also when using Bluetooth connection.

Wi-Fi and Bluetooth interfaces have their own vulnerabilities and are susceptible to wireless eavesdropping attempts, using readily available tools like Wifite or Aircrack-ng Suite. [17]

3.2.1 Basic tips when using and with our Wi-Fi network

When using Wi-Fi networks and letting guests use our network, there are precautions that users can take to better protect our network and mobile device, these being basic tips for any user:

- Avoid connecting to public Wi-Fi networks, instead use mobile data or search for a more secure network.
- Keep the device's Wi-Fi turned off when you don't need to use it.
- At home, to protect the Wi-Fi network, you can create a guest account and keep the router in a barely visible place in case of visitors, change the predefined password and in case of doubt, install a specific program such as Nmap to check if there are open ports so there are no intruders.

3.3 System-based Threats

Manufacturers can sometimes introduce vulnerabilities into their devices unintentionally. Sometimes these incidences need to perform timely updates of mobile devices to mitigate system issues.[17]

3.4 Application-based Threats

Even if software updates are available, users may not update applications on their mobile devices promptly. Using outdated software increases the risk that an attacker may exploit vulnerabilities associated with this software. Malicious applications, also known as malware, mentioned earlier in this paper what this type of attack is.[17]

4 How to protect Mobile Technology from Threats

To protect mobile devices, besides basic knowledge about mobile threats, it is important to know how to protect mobile devices while using them.

The devices may include our personal data as well from the company we own or work for, so it is important to know what procedures the users should take, in order to make devices safe to use and protect them from the use of third parties.

An example applied could be, a friend of the mobile device user asks to consult his/her e-mail address, the user, when letting the friend use the device, does not know if he/she has sufficient knowledge about mobile threats, for example, phishing and may end up opening a malicious email that compromises personal data or the device.

Hence, it is important to take the necessary precautions to protect these same devices and that's why it's important to know if that person has the basic knowledge, before letting them access certain applications on their mobile device.

4.1 For individual users

The following measures indicated by Kaspersky [1] for individual users are intended for users of android mobile devices, namely:

- Protect your devices with secure passwords, it helps to prevent attackers from accessing personal data by stealing your device and brute-forcing the password.
- Never enable the option that enables apps from third-party sources to be installed on the device, the best is always to keep it turned disabled.
- It’s recommendable using the apps that antivirus software developers often create applications designed to test devices for unclosed vulnerabilities. Such applications are regularly updated to include data on newly discovered vulnerabilities.
- Use a security solution on your device and make sure it scans files as they are downloaded and protects the device from other types of Internet attacks.
- When making bank payments, always use 2-factor authentication.

- Use encryption if you have any valuable information (financial, personal, or work-related) on your device.
- If you believe that you may have fallen victim to or witnessed a cybercrime, do not hesitate to contact law enforcement as soon as possible.

4.2 For Corporations

The following measures indicated by Kaspersky [1] for corporation users are namely:

- The Bring Your Own Device approach, which allows employees to use their personal devices for work, can expose your company to virtually all 'consumer' IT security risks: sensitive corporate data stored on an employee's personal phone could be a valuable find for cybercriminals. A security solution with Mobile Device Management capabilities, including encryption and remotely wiping data from smartphones, will help you to keep your sensitive business-related information secure.
- If employees' companies are not aware of simple IT security rules, this is likely to cause security incidents. Training people to handle their mobile devices appropriately will be a worthwhile investment.

5 Conclusion

Cyber threats are one of the factors that most affect mobile device users, and it is necessary to take precautions to make the use of mobile devices safe, one of the possible consequences if the user is a victim of a threat is the theft of personal data.

To understand what these types of attacks are, it was defined each one was given and tips on how to prevent them. It was possible to observe phishing, malware, application vulnerability, DoS, and DDoS attacks.

About phishing attacks was also talked about the effects that the pandemic caused in Portugal regarding cyber threats, the life cycle of a phishing attack and the Microsoft phishing simulator was presented. About Malware, it was possible to discover that there are several types of attacks, each with a different objective.

Although most attacks have the involvement of a hacker, threats can be of different types, as seen above these can be physical threats, network-based, system-based, and application-based. As seen, all related to device software attack, but physical attacks are simply given by physical access to the device compromising its software as well.[17]

While it's important to learn how to protect our devices and data, it's also important to protect our company from employees' misuse of mobile devices by taking extra care and providing the necessary training.[1]

In a future paper, more cyber threats that affect mobile device users may be included and examples of how some of the threats are carried out along with statistics, helping further to appeal how dangerous it can be or the damage it can cause without due care in the use of mobile devices.

10

References

1. Kaspersky and INTERPOL Joint Report," Mobile Cyber Threats" 2014 https://media.kaspersky.com/pdf/Kaspersky-Lab-KSN-Report-mobile-cyberthreats-web.pdf
2. McAffe, "McAffe Mobile Threat Report" 2021 https://www.mcafee.com/content/dam/global/infographics/McAfeeMobileThreatReport2021.pdf
3. Antonette R. Muntode and Sandeep S. Parwe, "An Overview on Phishing- its types and Countermeasures" 2019 https://www.researchgate.net/publication/342118299_An_Overview_on_Phishing-_its_types_and_Countermeasures/link/5ee2d851299bf1faac4e66b2/download
4. Muhammet Baykara and Zahit Ziya Gurel, "Detection of Phishing Attacks," ISDFS, 2018
5. National Cybersecurity Center Portugal, Cybersecurity Observatory, "Cybersecurity in Portugal" 2021 https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/relatorio_riscos_conflitos2021.pdf
6. Rami M. Mohammad,Fadi Thabtah and Lee McCluskey, "Tutorial and Critical Analysis of Phishing Websites Methods" (last access December 2021) https://core.ac.uk/download/pdf/206070797.pdf
7. Microsoft contributors, "Simulate a phishing attack in Defender for Office 365" (last access December 2021) https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training?view=o365-worldwide
8. Mariwan Ahmad, "Malware in Computer Systems: Problems and Solutions" 2020 https://www.researchgate.net/publication/340770783_Malware_in_Computer_Systems_Problems_and_Solutions
9. Ghossoon M. Waleed and Hilal Mohammed Yousif Al-Bayatti, "A Comparison of Trojan Virus Behavior in Linux and Windows Operating Systems" 2011 https://www.researchgate.net/publication/51891535_A_Comparison_of_Trojan_Virus_Behavior_in_Linux_and_Windows_OperatingSystems
10. Mark Eichin and Jon Rochlis. With Microscope and Tweezers: An Analysis of the Internet Virus of November 1988. In IEEE Computer Society Symposium on Security and Privacy, 1989
11. Robert K. Cunningham, Nicholas Weaver, Vern Paxson and Stuart Staniford, "A taxonomy of computer worms" 2003 https://www.researchgate.net/publication/220796741_A_taxonomy_of_computer_worms
12. D Anil Kumar, Sisira Kumar Kapat, Susanta Kumar Das and Satya Narayan Tripathy, "Classification of Spyware Affected files using Data Mining Techniques" 2019 https://www.ijrte.org/wp-content/uploads/papers/v8i2S6/B10880782S619.pdf
13. Robert Moir, "Defining Malware: FAQ" 2009 https://docs.microsoft.com/en-us/previous-versions/tn-archive/dd632948(v=technet.10)?redirectedfrom=MSDN
14. Kim Hee Wan, "A Study on the Mobile Application Security Threats and Vulnerability Analysis Cases" 2020 http://koreascience.or.kr/article/JAKO202034465346164.pdf
15. Nuno Antunes and Marco Vieira, " Defending against Web Application Vulnerabilities" 2012 https://eden.dei.uc.pt/~mvieira/2012_Computer_DefendWeb.pdf
16. Cybersecurity&Infrastructure Security Agency, "Security Tip (ST04-015) Understanding Denial-of-Service Attacks" 2009 https://us-cert.cisa.gov/ncas/tips/ST04-015
17. Pang Jian Hao Jeffrey, Chua Chee Leong, Chan Guan Huat and Lim Seh Leng, "Challenges in Mobile Security" 2016 https://www.dsta.gov.sg/docs/default-source/dsta-about/challenges-in-mobile-security.pdf?sfvrsn=2

Cyber Threats to Automotive Technology

Luis Emilio Núñez Morales

Lúsofona University of Porto, Portugal
University of Vigo, Spain

emilio-0111@hotmail.com

Abstract. In the last decades, automobiles have been transformed from mechanical machines, with barely any electrical device, to advanced machines that contain hundreds of electrical components. All of this new features have to be managed and controlled by software, turning today's vehicles into technological devices with up to millions of lines of code. This amount of software opens up the opportunity for hackers to find vulnerabilities and exploit them, being able to cause a lot of damage. This paper will discuss the importance of cyber security in the automotive industry and how it is becoming a new dimension of quality in vehicles. We will talk about cyber attacks on cars, focusing on remote attacks, and overview some of the methods and standards used to prevent those cyber attacks. Finally, this paper will show two case studies of attacks on cars, one well known from 2015 (Jeep Cherokee attack) and another one from a more recent year, with the purpose of arriving to a conclusion on whether or not there has been any improvement.

Keywords: Cyber Security, Automotive Industry, Cyber Threats, Case Study, Standards, Remote attacks.

1. Introduction

In recent years, software development has had a more or less relevant weight for the industrial sector, but increasingly, the integration of software in the production chains of organizations makes it an essential element in the process of digital transformation of the production chains. Manufacturers are integrating new technologies, such as Internet of Things (IoT), cloud computing and analytics, and AI and machine learning into their production facilities and throughout their operations. This implies the appearance of a Fourth Industrial Revolution.

The Fourth Industrial Revolution, also known as Industry 4.0, is changing the way business operate and therefore the environments in which they are forced to compete. Industry 4.0 can improve business operations and revenue growth, transforming products, supply chain, and customer expectations [1].

Nevertheless, with the advantages of applying software in the industry, the threats of its use appear. The vulnerabilities of the different industries are increased by the cyber threats that come with the application of the software in the production operations and in its use in the final products.

The automotive industry, evolving alongside Industry 4.0, is directly affected by its pros and cons. The exponential growth in the amount of software found in automobiles today is a great challenge for manufacturers, who have to respond to a constantly evolving market for software innovations while addressing the threats of adding large amounts of software in their final products.

This paper will focus on the threats posed by adding software functionalities to the final product of automotive industries, their consequences for manufacturers and customers, and ways to mitigate them. This paper will also address the current regulations in Europe regarding cyber security in automobiles, which will determine a large part of the production of automobiles. Finally, we will attend to two case studies, separated in time, and analyze the evolution of both the functionalities and the threats of software in vehicles.

2. Cyber security as a quality feature for automobiles.

“Once, software was a part of the car. Now, software determines the value of a car,” notes Manfred Broy, emeritus professor of informatics at Technical University, Munich and a leading expert on software in automobiles. “The success of a car depends on its software much more than the mechanical side.” Nearly all vehicle innovations by auto manufacturers, or original equipment manufacturers (OEMs) as they are called by industry insiders, are now tied to software, he says [2].

In the last decades, automobiles have been increasing their functions, gadgets that increase safety, improve efficiency and contribute to the well-being and entertainment of the user. In order to do this, they make use of several ECUs, which contain the necessary software to monitor and control these functions.

With the increase in the number of functions in automobiles and their complexity, the number of ECUs required to control these functions has also increased. A decade ago, a luxury car could have up to 100 ECUs controlling the mechanical elements and hardware of the car, executing more than 100 million lines of code. With functions such as Cruise Control, Rear View Camera, Emergency Braking Systems or Parking Sensors becoming a standard in modern cars, today, we can find this amount of ECUs in more basic and lower-end cars. On the other hand, modern high-end cars like the Mercedes S-Class can have up to 150 ECUs as they have a large number of complex functions. This amount of code creates ample opportunity for cyber attacks, not only on the car itself but also on all components of its ecosystem (e.g., back end, infrastructure).

Cyber security in cars is becoming a new dimension to measure their quality [3] as well as the prestige of the manufacturer. OEMs will have to invest the necessary resources to face this new challenge in the automotive industry, protecting against cyber threats will be a difficult but necessary task in the coming years. The ability of

OEMs to provide online software updates on their cars will be one of the key pillars to ensure proper vehicle safety management.

3. Security threats: common attacks and countermeasures.

Currently, cars have gone from being mechanical machines with a minimum amount of electronic components to regulate their operation, to being machines with advanced technology that makes them smarter, more efficient and safer. Most manufacturers offer software services in their products, such as the possibility of interacting with a vehicle remotely via the Internet or knowing its GPS location from a smart phone. These services present vulnerabilities that can be exploited by malicious hackers, which can lead to serious accidents, data theft and damage the image of the manufacturer.

3.1. Remote attacks.

One of the most dangerous and powerful threats to modern automobiles is performing a remote attack. The nature of this type of attack allows the malicious hacker to get access to the target car, without the need of having any kind of physical contact with it. Hacking a car remotely can help the intruder access into the car´s internal network without being noticed by the owner of the car. Remote safety attacks against automobiles are generally divided in three stages [4].

The first stage is to gain access to the vehicle internal network. An attacker can gain access to an automobiles network by using ECUs that connect to the car with its surroundings. One way of doing so could be sending a wireless signal to a listening ECU on the car, subsequently injecting code. This will allow the attacker to send malicious messages into the car's networks, controlling the desired ECU. There are a bunch of point entries in modern cars. These include Bluetooth, Remote Keyless Entry, RFIDs, Tire Pressure Monitoring Systems, WiFi, and Dedicated Short-Range Communications among others.

Gaining access to these ECUs, whose job is only receive and process radio signals, will not give attackers the opportunity to perform a cyber physical attack -attack that result in physical control of various aspects of the automobile- . In order to perform a cyber physical attack, it will be necessary to inject messages onto the internal automotive network in an attempt to communicate with safety critical ECUs, such as those responsible for steering, braking, and acceleration. This is the second stage of a remote attack. The attacker will somehow have to get messages from the bridged network to the internal network where the target ECU lives. One way of doing so is to escalate privileges inside the CAN network (the network inside a modern car where control commands for various components inside the vehicle travel), creating a bridge between the firstly infected ECU, the one that interacts with the external world, and the target ECU, that controls critical features of the vehicle.

Once the ECU is been wirelessly compromised, and after being able to use it to communicate to the ECUs that control safety features, the attacker will want to send them instructions for malicious purpose. This is the final stage, trying to make the

target ECU behave in some way that compromises vehicle safety. In order to perform such action, the attacker will have to reverse engineer the messages on the inner network and figure out the format of the instructions, that way the attacker can replicate those instructions and execute them at will, resulting on physical actions such as braking or steering the wheel. Since each manufacturer (and perhaps each model and even each year) use different data in the messages on the bus, the message reverse engineering process requires a large amount of work and will be manufacturer specific.

3.1. Countermeasures.

In order to prevent these malicious attacks, automobiles must be built with cyber security in mind. In this paper we are going to overview security practices and standards that will help avoid not only remote attacks on vehicles, but every kind of cyber security threats.

Automotive threat modeling. Threat modeling involves understanding the complexity of the system and identifying all possible threats to the system. During the formation of security requirements, these threats are analyzed based on their criticality and likelihood, and a decision is made whether to mitigate the threat or accept the risk associated with it [5].

When it comes to automotive threat modeling, there is one particular framework popular in the computer industry, that seems to be the most suitable for the automotive industry, STRIDE. This framework covers the main six board categories of threats: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege. This threats are always present in remote attacks on automobiles, they are the ones that make this type of attacks happen, so seems to be appropriate to adopt a framework that focuses on covering these threats.

AUTOSAR. AUTomotive Open System ARchitecture is a global partnership of leading companies in the automotive and the software industry to develop and establish the standardized software framework and open E/E system architecture for intelligent mobility [6].

The standard comprises a set of specifications describing software architecture components and defining their interfaces. The principal aim of the standard is to master the growing complexity of automotive electronic architectures.

The AUTOSAR standard defines security mechanisms that can be used by the software modules implemented into the vehicle system. It further specifies interfaces and procedures to provide secure on-board communication, and the exact implementation is left for the OEMs to decide on. OEMs choose the cryptographic algorithms and encryption techniques which they want to implement and use in the vehicle system.

4. Cyber security standards and regulations in Europe.

In 1885, Karl Benz invented a car that is credited as the first car in the world to be powered by fuel.The design of the car was based on a horse carriage—the difference was that instead of a horse, he put an engine [7]. At that time, horses were considered to help avoid collisions and humans were not going to be able to carry out this task. Those who thought this way were not going wrong, the advances that vehicles brought with them generated new dangers. It was common to drive at high speed or under the influence of alcohol, so it was necessary to create a series of rules and make them known to society to have control over the behavior of drivers. Thus, Road Safety was born.

The industry has a relevant role in this whole process, since ensuring that the cars were safe enough for their occupants was essential for Road Safety to continue advancing. In 1930 the first cars with hydraulic brakes and steel frames came onto the market, and in 1959 Volvo began to install one of the most important passive safety features: the three-point seat belt.

Nowadays, as we have cover already on this paper, vehicles have been incorporating software functionalities and becoming data centers on wheels. With the appearance of new functionalities in automobiles, new rules appear so that they continue to be safe. The new regulations address the risks which arise from the increasing digitalization of vehicle functions and the connection of vehicles with their environment (connectivity). The regulations' objective is to generate a harmonized regulatory framework for vehicle development to enable international vehicle trade.

On March 4, 2021, UNECE publishes regulations R155 and R156, for cyber security in automobiles and software updates respectively [8]. UNECE regulation 155 (Cyber Security) introduces a cyber security Management System (CSMS) in automotive on organization level. This regulation encourages the use of standards in the production of automobiles that address the cyber security of the product.

UNECE regulation 156 (SW Updates) introduces a legal framework for remote updates (over-the-air) with a Software Update Management System (SUMS). The main objective of this regulation is to make sure OEMs provide secure software updates with the guarantee that vehicle safety is not reduced.

4.1. ISO 26262.

Automotive manufacturers and suppliers must be certified, as they must offer formal third-party assurance according to the safety standard, such as ISO 26262. The ISO 26262 [9] standard defines a framework, an application model, the activities to be carried out, the methods to be used and the results, offering manufacturers a common mechanism to measure and document the safety of an automotive system. It is necessary to manage functional safety and regulate the development of automobiles at the hardware, software and system level throughout their life cycle.

5. Jeep case study.

This section of the paper will overview the case study of the Jeep Cherokee cyber security attack that was performed on 2015 by two white hat hackers, Charlie Miller and Chris Valasek. The mentioned hackers elaborated a document [10] with the details of the attack that allowed them to take control of the Jeep Cherokee. In this document we will try to analyze the entire process of said attack without going into too specific details, and we will point out those security threats that should have been covered at the time of production of this vehicle.

5.1. The entire exploit chain.

Identify target: There are a variety of entry points on this vehicle, such as Bluetooth, WiFi or radio. The most interesting one is the cellular connection functionality, since it seems to be the most powerful one as it has the larger range. If you knew the Vehicle Identification Number (VIN) or GPS, you could scan the IP ranges where vehicles are known to reside until you found one with corresponding VIN or GPS. We could target one car only or use a worm to hack a number of them.

Get an SSH connection to be able to run code in the car´s system: Once we have the IP address of the vehicle we can port scan the default gateway and examine if there are any ports open. At the time the hackers were performing the attack, the 2014 Jeep Cherokee had several ports open. Here we find the first vulnerability of this vehicle. This vulnerability presents a big threat, as it provides a way for attackers to get into the car´s internal network. The port that is most interesting for us is the 6667, that was connected to a D-Bus. D-Bus (Desktop Bus) is an inter-process communication system (IPC) and a remote procedure call (RPC), for software applications in order to communicate with each other. This D-Bus message daemon is part of an infotainment, Wi-Fi connectivity, navigation, apps and cellular communications system called Uconnect 8.4AN/RA4 radio manufactured by Harman Kardon. D-Bus can require authentication. On the Jeep head unit, the authentication is open to anonymous action. Here is another security breach. The D-Bus should not offer the possibility of logging into the system with an anonymous authentication.
At this point we can interact with the D-Bus services on the Jeep. Some of them will allow us to acquire direct interaction with the head unit, giving us the ability to adjust the volume of the radio, access PPS data, among other things.
There are other D-Bus services that actually provide an “execute” method which is designed to execute arbitrary shell commands. This is a big security flaw. There should be no way to be able to execute shell commands from outside of the vehicle's

interior system. This vulnerability should have been covered before the vehicle was put on the market. Taking advantage of this vulnerability we can establish a reverse shell to obtain an interactive shell session on the vehicle´s OMAP (Open Multimedia Applications Platform) chip which manages the majority of the functionality of the Uconnect system.

Flash the v850 with modified firmware: In order to perform a cyber physical attack we will need to be able to send instructions through the CAN bus of the vehicle. Controller Area Network (CAN) is a protocol based on messages designed to allow vehicle´s Electronic Control Units to interact with each other. The OMAP chip, on which we have code execution on after the D-Bus exploit, cannot send CAN messages. It can, however, communicate with the v850 chip which can send CAN messages. In order to use the v850 to send CAN messages we need to upload a modified firmware that will allow us to send those messages. Reverse engineering the update file for the v850 should allow us to flash the v850 with the modified firmware.

Perform cyber physical actions: Once you can send CAN messages via remote exploitation, it is simply a matter of figuring out which ones to send to affect physical systems. There are two types of CAN messages, normal and diagnostic. Normal messages are seen all the time on the bus during normal operation. Diagnostic messages typically are only seen when a mechanic is testing or working on an ECU, or some other unusual circumstance is occurring. Using normal CAN messages we can manipulate physical features such as the turn signals, the locks and the tachometer. Diagnostic messages are more powerful than normal messages, however most ECUs will ignore diagnostic messages if the car is traveling at speed, usually faster than 5-10 mph. Therefore, these attacks can typically only be performed when the car is traveling rather slowly, unless the attacker can figure out how to forge a speed used to determine if diagnostic messages should be accepted. Using diagnostic messages we could kill the engine, disable the brakes and even get control of the steering wheel.

6. Tesla case study.

In this section we will study two Tesla cyber security researches made by Keen Security Lab of Tencent, a team focused in cutting-edge security research of mainstream PC/Mobile operating systems, applications, cloud computing technologies, IOT smart devices, etc. One of the researches describes how they remotely compromised the ECUs of Tesla cars [11], and the other one focuses on the vulnerabilities of the Tesla autopilot system [12]. We will start with the 2018 document that shows how they managed to gain remote access and then we will

continue with the 2019 document where they show how they compromised the autopilot system.

6.1. Remotely obtain root privilege of APE (AutoPilot ECU).

In 2017, Tesla had built-in a Webkit based web browser in their vehicles to allow the users of the car to navigate through the internet. The Tesla Model S had this browser inside a 17-inch touchscreen Center Information Display (CID) in the middle of the dash. Keenlab Team found an Use After Free (UAF) vulnerability in Webkit. Basically, an UAF vulnerability occurs when a pointer to an object that has been freed is referenced, an attacker could modify an unintended memory location that potentially can lead to code execution. Keenlab Team managed to insert the right instructions in the right memory address and gained arbitrary code execution inside the CID as a result.

The AutoPilot ECU (APE) module in the Tesla has control of the systems that provide driving assistance to the driver, such as lane centering, adaptive cruise control or self-parking among others. Unlike CID, there are few interfaces on APE interacting with the outside world, making it difficult to hack into APE. Keenlab Team took advantage of a vulnerability in the update file of the APE that allowed them to modify the existing firmware with a customized code that granted them a way to execute commands with ROOT privilege.

6.2. Remotely control the steering system.

APE is responsible for managing the steering system and the electronic speed control of the car whenever the is on Automatic Parking Control (APC) or adaptive Cruise Control (ACC) modes. The necessary communication between ECUs to manage the steering is made throw a CAN-bus system.

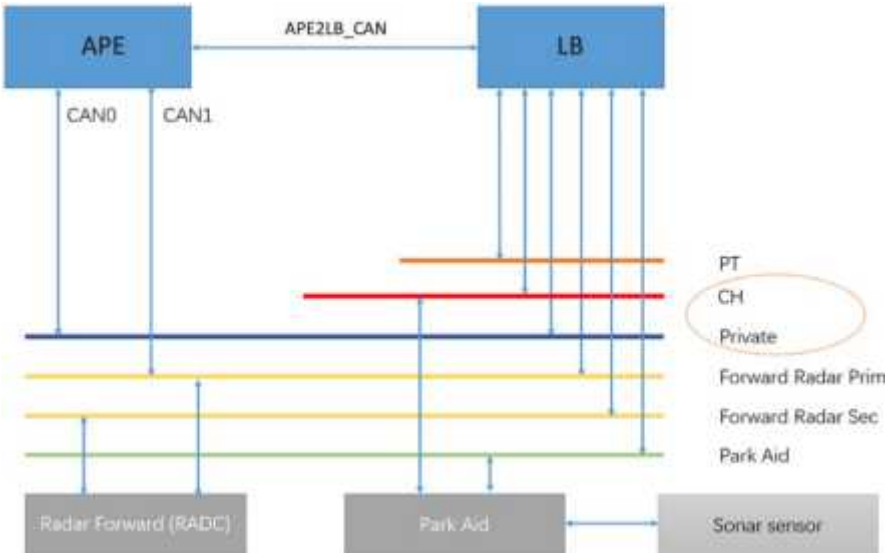


Fig. 1. CAN Bus System of APE.

After reverse engineering some CAN services, Keenlab Team managed to understand how the networking in the CAN bus system of APE works. They discovered that they needed to get access to the Power Train and Chassis CAN buses through the APE2LB_CAN and LB unit (see fig.1) in order to control the Electric Power Assisted Steering (EPAS) unit.

DasSteeringControlMessage (DSCM) is a CAN message produced by the Cantx service (a service associated with CAN-bus in APE) designed to control the steering system when the car is in ACC or APC modes. Keenlab Team managed to inject malicious code into the Cantx service and send DSCM messages that allowed them to control the steering of the car.

6.3. Attacks from physical adversary scenarios.

So far we have only covered remote attacks that took advantage of vulnerabilities in the software´s design of the vehicle (in both the Jeep and Tesla case study) to access the key components that manage important aspects of the car, allowing us to change the way they behave by sending malicious instructions. But now we are going to overview a different kind of security threat, one that does not require an intrusive attack to be exploited.

Auto wipers: Tesla´s auto wiper system uses a pure computer vision solution, based on a 120-degree fisheye camera and an artificial intelligence network to determine whether the wipers should be turned on. Keenlab Team found a way to deceive the

auto wiper system by displaying an image that used a noise function. The image displayed in front of the car´s camera made the system think it was raining and therefore it turned on the wipers.

Lane Detection: The lane detection system also uses a computer vision solution, but includes more communication between various components of the car, as it has to know where the car is on the road and perform the necessary actions (such as steering the wheel) to keep the car in between the lines. There are two different types of lane recognition attack: eliminate lane attack and fake lane attack. The eliminate lane attack consists in blurring the road lane in the physical world, forcing the system to ignore that there is a lane on the road. This attack is quite difficult to perform because the Tesla´s lane recognition system is designed to recognize even the most abnormal lanes (broken, occluded). But this feature has also it´s cons, since it might recognize a lane where there isn't one. This is a fake lane attack. Keenlab Team managed to deceive the lane recognition system by just putting some small stickers on the road, making the vehicle think that there is a lane there. A fake lane attack could be extremely dangerous if the fake lane is pointing to the reverse lane of the road.

7. Conclusion.

In this paper we have talked about how software has been progressively introduced in the automotive industry. We pointed out the importance of building a strong and secure software architecture in automobiles, as it is becoming a new dimension to measure the quality of modern vehicles. We have focused on the structure of remote attacks and overviewed some countermeasures and good practices to avoid them. Furthermore, this document summarizes the objective of the new and necessary cyber security regulations in the automotive industry, which will help to target a better cyber security scene in the automobiles of the future.

In both the Jeep and the Tesla cases, we have seen security vulnerabilities that allowed intruders to get remote access to a ECU inside the vehicle that connects to the outside world. We have seen that it is possible to extend the attack using the vehicle´s CAN bus to reach key ECUs that control very important aspects of the vehicle. In the Tesla case, it seemed to be a harder job to perform these attacks, which might let us think there has been improvement in cyber security in comparison with the Jeep case. But one thing that stands out for me in the Tesla case is how new vulnerabilities are coming together with new technology and features. It is undeniable that there has been a slight improvement in cyber security regarding known and past threats. Nevertheless, it seems that the desire to create new technologies and add new software in vehicles that can make them more advanced is overtaking the initiative to seek safer structures in these new technologies.

References

1. IBM: What is Industry 4.0? URL: https://www.ibm.com/topics/industry-4-0
2. Robert N. Charette: How Software is Eating the Car. IEEE Spectrum. (2021).
3. Ondrej B., Johannes D., Benjamin K, Klaus P, Gundbert, S.: Cybersecurity in automotive (2020)
4. Charlie Miller, Chris Valasek: A Survey of Remote Automotive Attack Surfaces. (2014)
5. Zhendong Ma, Christoph Schmittner: Threat Modeling for Automotive Security Analysis. (2016).
6. AUTOSAR: General Information About AUTOSAR. URL: https://www.autosar.org/about/
7. CarAdvise: What Was The First Car In The World (2019)
8. Henning Schweder: UNECE Vehicle Regulation for Cyber Security & Software Updates.
9. ISO.org: ISO 26262-1:2018 Road Vehicles - Functional Safety. (2018)
10. Keen Security Lab of Tencent: Over-The-Air: How We Remotely Compromised The Gateway, BCM, and Autopilot ECUs of Tesla Cars. (2018).
11. Keen Security Lab of Tencent: Experimental Security Research of Tesla Autopilot. (2019).
12. Charlie Miller, Chris Valasek: Remote Exploitation of an Unaltered Passenger Vehicle. (2015).

Security with Smartphones

Alicia Sambade Mata

Lusofona University of Porto, Portugal
University of Vigo, Spain

aliciasambade31@gmail.com

Abstract. It is undeniable that nowadays the rise of technologies has caused a big change in our society and economy, and it produces new facilities but, at the same time, problems. Furthermore, the use of the smartphone has become a day-to-day basis and we have more and more functions on them. Despite their success, smartphones have many problems in use and we have to become aware of what dangers we have to face and how to avoid, as far as possible, that they affect us. In this paper, the risks of having a smartphone are going to be analysed and will delve deeper into the security of the Android operating system and some differences with IOS. It will also show some types of cyberattacks and it is going to be analysed from both a theoretical and a practical framework, showing different case studies and showing different solutions and failures in society and technology.

Keywords: smartphones, security, Android, technology, risk, attack, malware

1 Introduction

Nowadays, smartphones have a very important role in our lives, but it is very interesting and surprising how they have evolved to the point where they are now. In 1876, the first telephone communication was achieved and, since then, it has been improved to better adapt to people's lives, until the mobile phone was created almost 100 years later. This point is very important, because since that date many companies have been competing to achieve the best speed in their devices and to be the first to create something innovative. After that, and with the turn of the century, as humans we are looking for more and more comfort and we start to add more and more functionalities to the mobile phone, to the point that nowadays we can do almost everything with it; from basic everyday things like raising the shutter, to work.

Like any change in society, this also has pros and cons. In addition to having faster and real communication, it has become faster to do anything, both to satisfy our needs and for entertainment. New ways of spending our time, new fields of study and new professions that did not exist before have emerged and will continue to do so. On the

other hand, these developments also mean the disappearance of many other jobs, obsolete knowledge and people seeking to take advantage of others because they have more knowledge in this area, leading to the emergence of another type of crime: cybercrime. As more and more people make use of ICTs, the number of people who can be targeted by these attacks is growing, and strong countermeasures must be put in place.

Section 2, *use of smartphones*, describes the current situation of smartphones and the existing operating systems and then focuses on one of them, Android, and analyses it. In addition to a brief comparison with its other strong competitor IOS, its architecture will be explained in section 3. Then, sections 4 and 5 present two case studies that have in common that they are both related to each other by the use of SMS: Joker and Flubot malwares. Finally, methods for securing a device and guidelines on how to deal with malware will be presented.

2 Use of smartphones

Smartphone sales grow exponentially over the years. In the graph below, although we see a decline in 2019, this is due to the COVID-19 pandemic, but even then, it recovers in 2020 and continues in 2021 (see **Fig. 1**).

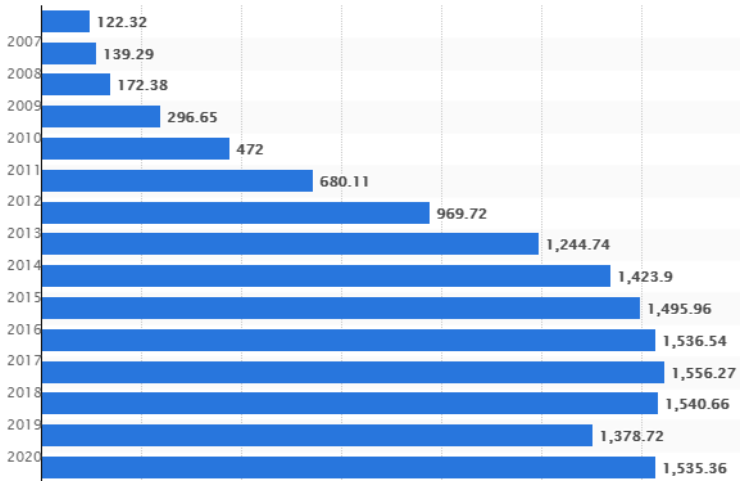


Fig. 1. Number of smartphones sold to end users worldwide from 2007-2021 (million units) [1]

In terms of cybercrime, it is increasing, as is the use of mobile devices. According to a study, the volume of targeted malware threats increases by 15% in 2020 compared to 2019. It was also observed that the threat database grows from 556 million threats in 2019 to around 652 million by the end of 2020, so approximately 17% of these emerged in the last 12 months. It is a reality that there are increasingly better trained specialists to look for vulnerabilities in systems, which we will explain later, and more and more skills are required to combat them [2].

2.1 Security in operating systems

The most representative operating system today is Android, which is the leader in sales (see Fig. 2). The reasons for its success are, among others, the price range of the devices that have it implemented, its wide variety of free applications, the customisation options and the fact that it is open-source software, which allows it to be manipulated for one's own purposes. Despite this, iOS continues to have many Apple brand loyalists and new users and occupies a significant space in the market. Some of the other operating systems available in 2010 have failed to maintain sales in the smartphone area after being beaten by the two giants; in 2017, 98% of smartphones sold had some of the two operating systems (see **Fig. 2**).

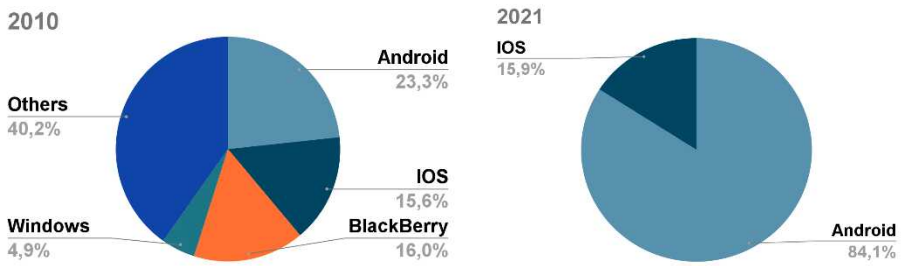


Fig. 2. Global smartphone market share by operating system in 2010 and 2020 [3]

If we make a comparison from a security point of view, the Android model has many different features, but it has certain limitations. Being an open-source software, anyone can access to the source code and test its vulnerabilities countless times. Because of this, it is also very easy to find free apps in Google's shop, Google Play, where there are approximately 3 million apps, while Apple's store, App Store, has approximately 2 million. In addition to the official shop, the Android operating system also allows apps to be installed from external sources in the form of APKs, which carries a risk that does not exist on iOS.

Another characteristic of Android is that it is implemented in smartphones from different companies: Samsung, Sony or Xiaomi, for example. This makes each company's device use software that is not specifically created for it, so some functionalities are programmed with more flexibility and security is more difficult to guarantee. Apple, on the other hand, has strict control over the ecosystem of its devices and how software is deployed, so it has more control over when and how updates are made.

3 Android architecture

Android is an operating system consisting of an open-source software stack based on the Linux kernel and created specifically for mobile devices. This section is important to know how they can be introduced into the system and how they can affect it.

Its architecture is based on 4 layers, depending on the level of abstraction, which form a hierarchy. The first layer is the Linux kernel (the core of the operating system) and is used for abstraction for the hardware, so developers do not have access to it. It provides services to higher layers, such as managing resources (like battery or memory), the file system and allows applications to access it via drivers (be it keyboard, image, audio...). If a manufacturer wants to include some new hardware element, he must create the necessary drivers within the kernel first. [4]

Above this is the abstraction layer (*HAL*). It is made up of several modules, each of which implements interfaces for each hardware component (such as the camera, Bluetooth or the device's sensors).

The next layer is the Android native libraries. Together with the kernel, they form the most important part of the operating system and are programmed in C or C++. Some of the most notable libraries are *libc*, which includes all the headers and functions in C, Media Libraries, which provides the codecs for multimedia content, SQLite, which manages the database or OpenGL/SL and SGL, for the graphics part of Android. [5]

Another section at the same level is Android runtime and includes the Core libraries, which incorporate most of the functionality of the Java programming language, and the Dalvik virtual machine. The latter is a virtual machine adapted to Android's processor and memory limitations, optimising them to the maximum and reducing its execution time.

Between the last two layers is the Application Framework, which includes the classes and services that the applications need in their functionalities, that is to say, the tools for development. Some examples of the APIs it contains are Activity Manager, Window Manager or Resource Manager.

The last layer is the one closest to the user, that of the applications, where you can find native applications (C or C++), managed applications (Java), those that Android has by default and those that the user wants. [6]

4 *Joker* case study

In 2020, Google reported on its blog about the existence of malware that has existed since 2017 called *Joker* hidden in multiple apps on Google Play. It is classified as spyware and belongs to the family called *Bread*. It is one of the most prevalent malware families that continuously infects Android devices and it is not yet certain how many thousands of devices are infected, because more and more apps are being found with this malware, but it has managed to reach approximately 40 countries. What it does is sign the user up for subscription services and trick them into paying these fees. In Denmark, it has managed to sign up thousands of people and earn €7 a week from each of them. [7]

One way to gain access to a device is by using applications that users often use and that are not included on some smartphones. Some of those affected are *Easy PDF Scanner* (to scan a document from a photo), *Now QR Code Scan* (to scan QR codes, bearing in mind that now in COVID time their use has increased), *Super-Click VPN* (to browse with VPN) or *Tangram App Lock* (to lock your items). Attackers need an easy way to access our data, and this is how they get it.

This malware manages to bypass Google Play's app checking mechanism because it continually changes its code and execution methods. On multiple occasions, it gets past Google's filters because when apps are submitted and displayed in the shop they are 'clean' versions and where they installed the malware was in the updates. In this way, the attackers manage to gain the user's trust and permissions for the app and then infect the device.

As a malicious program classified as spyware, it steals information, but specifically the *Bread* family consists of large-scale billing frauds. Early versions were via SMS, but Google has managed to combat them with successive updates; recently, phone fraud is being used. These leverage techniques that involve the user's operator, as they can partner with mobile service providers to allow users to pay for services by SMS. The process involves the user sending a text message with a keyword associated with a prescribed number and then a charge is made to the applicant's bill with their provider. Payment can also be made via the company's website; for this, the user uses his or her phone number and is sent an SMS also with a password Attackers use custom HTML parsers and SMS receivers to automate the process; this is possible because these processes do not require explicit user interaction.

Focusing on a more technical level, *Bread* applications use several methods for string encryption. These include standard encryption, using, within the *`java.util.crypt*o' library, encoders such as AES, DES or Blowfish; custom encryption algorithms, using basic XOR or nested XOR; and avoiding basic string matching. In addition, these substrings are sometimes scattered throughout the code and are invoked through static variables or method calls.

5 *Flubot* case study

Another SMS-related case is Flubot, so called because "its spread rate and infection vector resemble the common flu". It is a banking malware and, above all, it is having a big impact in Spain; it is known to have infected more than 60,000 victims and stolen more than 11 million phone numbers. It has been found to have textual content to target German, Polish and English-speaking users, so attacks by this malware are beginning to spread across more territories. [8]

They access the smartphone via SMS messages, supplanting well-known parcel delivery companies such as "Fedex", "DHL" or "Correos", saying that a parcel is about to arrive and that the order can be tracked via the link they provide. Once the user clicks on this link, the malware is installed and searches for an application to overlay

it and obtain the user's credentials, thus also their banking details. Once it has access, it can also make calls, get our contact list and send phishing content or listen to notifications; if the user has linked their phone number to websites of any kind, when user verification is performed, the malware can even get hold of that data.

The problem with this particular malware is getting rid of it. To prevent the user from removing anything from the attacker, the attacker implements mechanisms that stop system protection and the installation of third-party security applications. An Android team has designed an application to safely remove this malware called Malninstall, but many devices are unknowingly infected and will fall victim in the same way.

6 Malware defence and detection

In the present, we can distinguish two profiles of users: the new generations, who grew up in the 'information age', and those who did not. The former, despite having more and better means to deal with possible threats, still do not have a strong understanding of the risks that can come with the use of technology. The latter need to adapt and learn, so they are more at risk of being attacked due to their ignorance on the subject.

On the Internet browsing, attackers can gain access to our data in several ways. One way is to direct the user to a previously infected web page that the user considers trustworthy and obtain all the data entered, or to trick the user into accessing a spoofed page. They also use seemingly inoffensive advertisements, images or any type of file, but with malicious code.

On defence, to begin with, it is essential for a good defence against malware to install all available updates, both to the device and to applications, as they often fix security bugs. As with most devices, one of the most important methods against malware is to install an antivirus. It runs static, dynamic or mixed scans. Static scans focus on observing and investigating the APK, which is defined by AndroidManifest, where the permissions that an application may require, the code with the functionalities (in Java) and the resources it needs, such as database or audio, are declared. Dynamic analysis analyses the behaviour of the system, looking at user interaction or system calls and require excessive resource usage. Mixed analysis is the combination of the two previous ones and is very complete, but it is difficult to maintain due to the cost of development and maintenance [9].

The antivirus requests a lot of permissions from the device in order to scan all data for compromise and it is very important to get it from a trusted site, because many attackers can hide malware in such applications. In some cases, fake advertisements are used, warning that the device may be compromised and prompting people to download an antivirus, which most of the time is free and contains malware. Although

this is important, it is not essential, because by surfing safely and being cautious, an attack can be avoided.

As mentioned above, it is very easy to install third-party applications on Android due to its freedom at the operating system level. For apps in the Google Play shop, there is a review by Google Bouncer that looks for malicious software and compares it with other apps to identify malware and remove the app, if applicable. Apps that are not on Google Play lack this review, so be careful when downloading them. A good way is to do it from APK repositories that use filters and are secure; it is very important to know the origin of an APK when you intend to use it. Remember to have the *Install apps from unknown sources* option deactivated and, in any case, activate it only when necessary.

Regardless of how you obtain the application, you should always carefully examine the permissions that are requested before accepting them, as some may be unnecessary and indicative of suspicious activity. Currently, many of them have the option to activate them only when the application is in use and it is a good method to control access to data or functionalities and make use of them when they are not required; it is a method to protect yourself but also to control resources. It is recommended to review and update from time-to-time what permissions are granted to each application in case there are any suspicious or unneeded ones. This can be done from the device's settings. In the image, we can see the permissions given and denied to a video playback application; none are accepted because they are not necessary (see **Fig 3**).

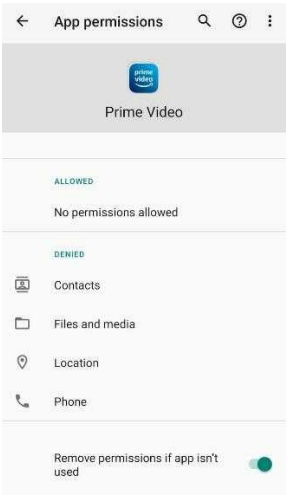


Fig. 3. Application permissions in *Device settings*

The appearance of excessive advertisements or in non-advertising applications and unknown installed software are signs that malicious activity may be occurring. Battery or data usage can also help to detect this, as excessive or unidentified data usage

can mean unknowingly running functions in the background. Android warns if it registers anomalous activity, identifies it and allows an action to be taken (see **Fig. 4**).

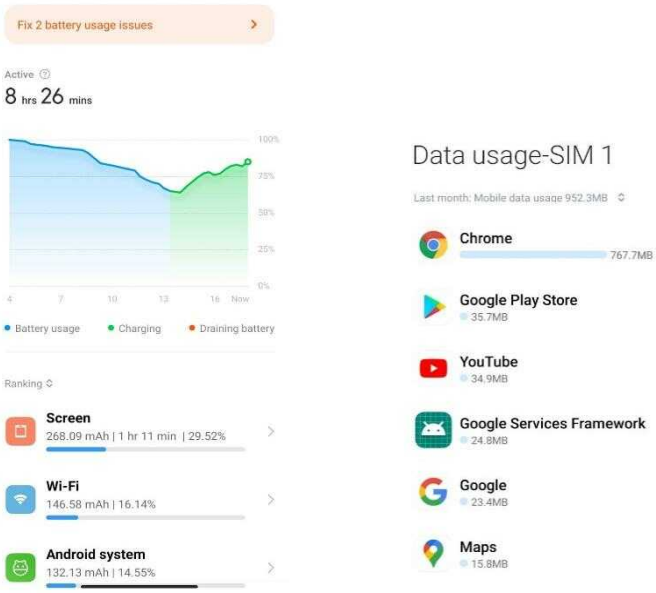


Fig. 4. Battery and mobile data usage in *Device settings*

In **Fig. 4**, the user charges the phone before reaching 50%, so it is not possible to see the full waste that the battery would have. However, it is still possible to see how much the screen and Wi-Fi consume; even if you are not aware of the consumption in *mAh (Milliamp-Hours)*, you can see the percentage and reflect on whether this consumption has occurred (if the screen has been on for a long time or if the Wi-Fi has been activated). Many malwares may have made use of these and other resources, and the user may not have perceived it; is convenient to observe and analyse it. The same happens with mobile data usage; it is normal for video or gaming apps, for example, to have a higher consumption. If we have identified a big change in applications that do not require internet or an unknown application, we need to take action.

In Dual Sim smartphones, such as the one shown in **Fig. 4**, the usage of the other card (SIM 2, in this case), which is not used as the main card for mobile data usage, should also be observed, as unknown or excessive usage may have occurred in the background.

6.1 Remove malware

Even if you take precautions, you can still fall victim, because now there are multiple ways for malware to enter a device without leaving traces. If you see signs that your

device may be infected, it is best to perform a factory reset because you don't know the extent of the attack and what it does. This can be done from the console that can be accessed in the phone's power-on process or from the phone's settings. The result of this is that all data except system and manufacturer applications are deleted; the /data, /sdcard and /cache partitions are deleted.

Before this, if you do not want to lose the information on the device, you can make a backup, but to do this you must switch the smartphone on in *Safe Mode* (see **Fig. 5**). This mode starts the system only with the system and manufacturer's applications and does not run third-party applications. In this way, we can safely back up our data and, if we have identified the malware-causing application, uninstall it.

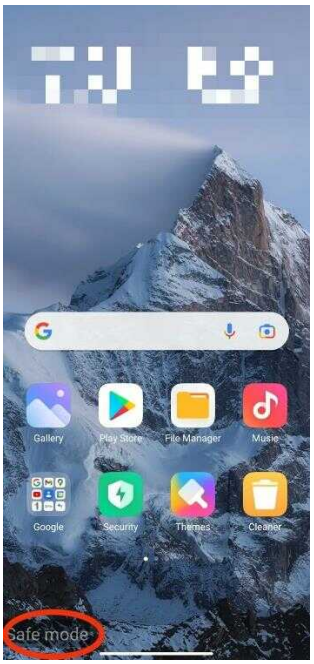


Fig. 5. Smartphone started in *Safe Mode*

7 Conclusion

Many changes have occurred in society with the existence of technology, but they will continue to happen, and people must adapt to them. It is essential that people are taught about all that technology brings with it, both the good and the bad; people need to know how to protect themselves from these possible attacks or, at the least, to avoid great harm. The smartphone has become, for many people, another part of the body with which they can carry out most daily actions and which has all their data; moreover, people are not aware of the information we have inside a mobile phone,

both our own and that of those around us. There are cases like Joker, Flubot or many others with important consequences, so worrying about the security of a device has to become a regular routine in our lives; browsing safely, checking permissions given to apps and being aware of any suspicious activity are small actions that can avoid big problems.

References

1. Cell phone sales worldwide 2007-2021. Published by S. O'Dea, Dec 16, 2021
   URL: https://www.statista.com/statistics/263437/global-smartphone-sales-to-end-users-since-2007/
2. 2020 Threat Summary by Alexander VukcevicAvira Operations GmbH, part of NortonLifeLock Inc. (2021)
   URL: https://www.avira.com/en/blog/2020-threat-summary
3. Gartner Says Worldwide Sales of Smartphones Grew 9 Percent in First Quarter of 2017, Gartner, Inc. (2017)
   URL: https://www.gartner.com/en/newsroom/press-releases/2017-05-23-gartner-says-worldwide-sales-of-smartphones-grew-9-percent-in-first-quarter-of-2017
4. Vanegas, C. A. (2012). Desarrollo de aplicaciones sobre Android. Revista vínculos, 9(2), 129-145. [Spanish]
   URL: https://revistas.udistrital.edu.co/index.php/vinculos/article/view/4275/5967
5. Puente Arribas, D., Daguerre Garrido, J. I., & Costales de Ledesma, R. (2021). Malware Analysis on Android. [Spanish]
   URL: https://eprints.ucm.es/id/eprint/66842/1/COSTALES%20DE%20LEDESMA%2064210_RAMON_COSTALES_DE_LEDESMA_Malware_Analysis_on_Android_784051_190326 1751.pdf
6. Programming on portable mobile devices [Spanish]
   URL: https://sites.google.com/site/swcuc3m/home/android/generalidades/2-2-arquitectura-de-android
7. PHA Family Highlights: Bread (and Friends) (2020)
   URL: https://security.googleblog.com/2020/01/pha-family-highlights-bread-and-friends.html
8. FluBot - Malware Analysis Report (2021)
   URL: https://raw.githubusercontent.com/prodaft/malware-ioc/master/FluBot/FluBot.pdf
9. Heras Cáceres, I., & Sierra Liras, D. (2015). Sistema de detección de malware en Android. [Spanish]
   URL: https://eprints.ucm.es/id/eprint/33026/1/memoria_TFG.pdf

Mobile Forensics: A comprehensive analysis

Natália Freitas[1]

[1] Lusófona University, Porto - Portugal
natyrf2000@gmail.com

Abstract. The objective of this paper is to analyze different attacks and techniques when it comes to digital forensic analysis. There are different threats, some with more associated dangers, which are described in depth throughout this work. The techniques detailed are compared with real-life practical cases. There are many people using popular messaging apps, which consequently comes with an increase in the number of attacks with this technology.
This in turn, increases the potential of certain data to be used in court, becoming important evidence, which creates the need for investigators to use specific mobile forensic techniques: however, this is not always possible due to numerous restrictions in the field. The paper is focused on these topics, based on the research of scientific papers. The conclusion is that this area of study has yet to grow, to become something with a larger impact, more commonly used.

Keywords: digital forensic, mobile, messaging apps, analysis, court evidence.

1 Introduction

Nowadays, our world is surrounded by technology, and this inevitably brings a new branch of studies and work on our everyday life. In this case, Forensic Science has the need to "evolve" into something else, so it can answer to different problems associated with technology. In brief, Forensic Science focuses on gathering and examining information about an event or crime. When it comes to analyzing digital information, this is known as digital forensics, and nowadays it applies to computers, mobile phones, tablets, or any electronic devices. So, Mobile Forensics is a branch of digital forensics, and consists of methods that describe how to take evidence from phones and how to analyze the information [1]. It can involve real-life implications or happen solely on the online ground.

Mobile devices aren't foolproof, and they can be exploited in different ways, even without tampering with them: their usage as it is can be malicious. They can hold photos, location access, or even just messaging apps, which can contain sensitive information, for example.

They can also propagate malware, to steal the sensitive information mentioned above.

These dangers and actual crimes bring up the need of using different forensic tools, which have several constrains that can difficult this work: hardware differences, security settings, and even the cost [2]

2

Starting with section 2, general attacks/threats on mobile devices are described, including how to prevent and detect them.

Next up, section 3 focuses on the proposed forensic model for mobile forensics, and section 4 compares the previously mentioned model with others that are used on the field.

Following this, section 5 presents a practical case, based on research on WhatsApp data extraction methods, and section 6 contains all the conclusions and reflections achieved after finishing this work.

Finally, section 7 includes all the references used throughout this paper.

b

2 Different Threats on Smart Devices

Mobile platforms are regularly attacked and targeted due to their security issues, and here are different types of threats that we can face when it comes to Smart Devices:

2.1 General Threats

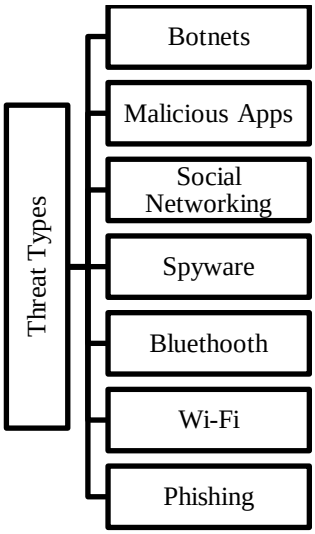


Fig. 1. Threat Types

Botnets:

.

They are networks that are formed by malware-compromised machines, usually used to conduct large-scale illegal activities. [3]

These are also called “zombie systems” and each zombie represents each individual connected computer. They can cause Denial of Service attacks or send spam, usually without the owner of the device noticing these actions.

Malicious Applications:
. Attackers can transfer malicious attacks with the form of apps usually seen as “ordinary”, such as games, so the user downloads them, without knowing what the app really does on their device.

Social Networking:
. Social networks have made it easier for attackers to spread their malicious links, on which people click out of pure curiosity or are unable to identify that it’s a malicious link.

Spyware:
. Spyware is malicious software with actions of different levels of maliciousness, and it attempts to monitor the behavior of users. The collected information is sent back, where it might be used for targeted ads, or marketing studies [4].
Moreover, the malware authors can see messages, hear calls, and track GPS information from the owner of the device.

Bluetooth:
. The Cabir worm is one of the first that propagated through Bluetooth, even though the users have their settings configured properly.

Wi-Fi:
. The attacker intercepts connections between Wi-Fi hotspots and smart devices, taking advantage of the latter.

Phishing:
. Phishing attacks usually target vulnerabilities that are present due to human factors [5].
Mobile phishers use vulnerable telephone connections, for example, through emails, SMS, or even MMS [6]

2.2 Preventive Measures

To mitigate malware and app abuse, there should some measures applied to each one of the threats.

Application Developers. They must make sure that the app is properly coded when it comes to security issues and include encryption on their services [6].

Smartphone User Level. To avoid certain situations, the user should be informed on these matters, at least on the surface. This gives the user the general sense to examine if the permissions requests are trustworthy or not when installing an app, for example. They should also have good security options on their device [6].

2.3 Malware Detection Techniques

These are generally classified into 3 types:

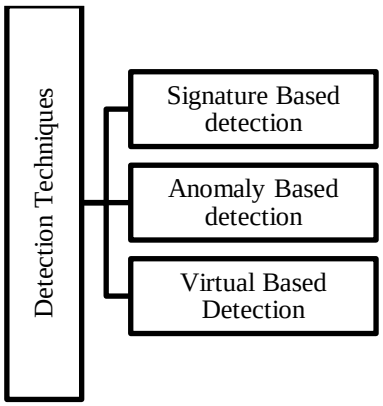


Fig. 2. Malware Detection Techniques

Intrusion detection and Prevention System (IDPS) has three main stages:

1. System details: network, application, OS behavior, etc.
2. Monitored data re-analyzed: allows the investigator to identify malicious occurrences.
3. Collect detected malicious data and initiate preventive measures, such as shutting down the devices or locking systems [6].

3 Proposed mobile forensics model

This model for mobile forensics is based on the most important phases for mobile forensics but there isn't a forensics model that is accepted or considered "correct", since different models can be applied to different situations.

3.1 Preparation:

This is the most important phase, as it allows the investigators to discover the nature of the case, and with this the team starts setting up their workstation. They also have a briefing on the situation, and they should be aware of different devices, their general hardware and software configurations of the ones involved. [7]

3.2 Handling Evidence & Securing the evidence:

This step is focused on making sure that the device found has the proper authorizations for the team to start investigating: if this isn't assured, there might be data losses. [1]

Accordingly, there are some important guidelines and challenges associated with this step:

Acquisition. Performing this at the scene avoids problems such as battery depletion, damage and more. First, it's determined if the device has been identified and next, if the device is on, there's only the need to bypass PIN/password [8].

There are various issues that can come up during acquisition:

- Selection of the Correct Acquisition Tool (experimenting with different tools to find out which one works best with certain devices is something recommended) [8][9]
- PIN/Password bypass (can be obtained from the service provider) [8] [9]

3.3 Documentation

This phase is connected to all the others since the investigators should document everything throughout the investigation and consequently, the documentation should include:

- Legal Authority letter
- Photographs and manual documents of digital evidence
- Information about the mobile device if obtained from owner
- Report of the findings
- Chain of Custody
- Formulated strategy for the investigation

3.4 Preservation

The phase of preservation aims to keep the evidence's integrity. Having in mind that we are dealing with electronic devices, it's important to know that humidity and other factors might have an adverse impact and therefore jeopardize the entire investigation, so there are some special arrangements to overcome these "challenges":

- Phone found in a liquid (battery should be removed, and the device should be sealed in an appropriate container) [8][9]

- Identification of Phone (the team should discover the type of device, operating system, and other attributes, to find out how to create a forensic copy of the contents of the device) [8][9]
- On-Off State Challenge (depending on the power state, there are different approaches) [8]

3.5 Examination and Analysis

The aim of this phase is to make the evidence visible: we might have a ton of information, but if it isn't properly arranged, it won't make much sense.

With this, the investigators analyze all the data to figure out which pieces can be used as evidence, and after determining what data is relevant, there is a data retrieval process.

Analysis is seen as technical review and recreating the crime scene is part of it. It allows for the investigators to basically do a timeframe analysis, since it might have a significant impact on the judgement.

As the final step, there is the making of a comprehensive report, which includes everything from the beginning to the end, with the results. [2][7]

3.6 Presentation

The court depends on this phase, and it consists of presenting the final report to the court of law. Nevertheless, if the report has any flaws when it comes to evidence, a culprit may be released, and the report itself might be challenged during its presentation, by the other side. In brief, the documentation must be solid at this time.

3.7 Review

This is the final phase, and it's dedicated to the investigators, as it allows them to improve their analytical skills. All the steps mentioned above are analyzed.

4 Comparison with other Models

The following table compares the model from above with others, specifically the phases that they include.

Table 1. Comparison of Proposed Model with others

Proposed Model	**NIST Guidelines**	**DEFSOP**	**Model for Windows devices**	**HDFI model**
Preparation	-	+	+	+
Handling Evidence & Securing the evidence	+	-	-	-
Data Acquisition	+	+	+	+
Documentation	+	-	+	+
Preservation	+	-	+	+
Examination and Analysis	+	+	+	+
Presentation	+	+	+	+
Review	-	-	+	-

This shows how there are different approaches (none of which are wrong) and they are applied to different situations. The proposed model has the advantage of including all the phases, which makes the investigations more concise.

5 Practical case with the usage of research tools

WhatsApp is one of the many existing messaging apps, and it has been equipped with an encryption feature [2]. There are many threats when it comes to the use of these apps, which were detailed before in this paper, so we can take a simple example: a pedophile can use this app to conduct his wrong-doings and even have incriminating conversations, and once he is pressed with charges, the investigators need to extract information from the app. This creates the need of using an extraction tool for WhatsApp.

5.1 Research Tools

(The hardware and software used to experiment on the extraction of WhatsApp Artifacts from an Android-based device can be seen in Table 2.) [2]

Table 2. Research tools and devices

No.	**Tool and Device**	**Information**
1	Samsung Galaxy S4 GT-19500	Smartphone used in the experiment
2	WhatsApp	Messaging App
3	Workstation with and operating system for Windows	Computer for extraction and analysis
4	USB Cable	Connects device and computer
5	Android Debugging Bridge	Software that supports communication
6	WhatsApp Key/DB Extractor	Extraction Tool
7	Belkasoft Evidence	Extraction and Analysis Tool
8	SQLite Studio	Analysis Tool

5.2 Results

When using the Belkasoft Evidence Software, the investigators can retrieve videos, images, and document artifacts. When it comes to the WhatsApp Key/DB extractor, the investigators only managed to retrieve text message artifacts and images, including information such as the message sender, message content, and time of sending or receiving the messages.

Both the extractions were repeated to ensure the results are similar and based on the results they have different strengths. WhatsApp Key/DB extractor dominates when it comes to retrieving text messages and the information associated with them, and Belkasoft Evidence excels in the extraction abilities for images, videos, and documents. [2]

Table 3. Forensic Tools Comparison

Artifact Type	**Belkasoft Evidence**	**WhatsApp Key/DB Extractor**
Text Message	-	+
Image	+	+
Video	+	-
Document	+	-

All this reinforces the idea that using different research tools is beneficial, since it allows us to obtain more concise and detailed evidence.

6 Conclusion

Technology became part of our life, and it's being used all the time: for the good and the bad. There are countless attacks that can be carried out, and technology only opens the possibilities.

People with malicious intent will always find new ways of getting their way, and Mobile Forensics aims to recover digital evidence to put an end to their antics. It might have similar processes to Digital Forensics, but it has its own peculiarities that are vital.

Subsequently, the need of having tools capable of extracting data or deleted data is also very real. A suspect in a trial might even delete the data in a phone that connects him with some sort of offense and being able to give evidence of his actions is important to have him prosecuted.

7 References

1. Lohiya, Ritika & John, Priya & Shah, Pooja. (2015). Survey on Mobile Forensics. International Journal of Computer Applications. 118. 6-11. 10.5120/20827-3476.
2. Umar, Rusydi & Riadi, Imam & Zamroni, Guntur. (2018). Mobile Forensic Tools Evaluation for Digital Crime Investigation. International Journal on Advanced Science, Engineering, and Information Technology. 8. 949-955. 10.18517/ijaseit.8.3.3591.
3. Silva, Sergio & Silva, Rodrigo & Pinto, Raquel & Salles, Ronaldo. (2013). Botnets: A survey. Computer Networks. 57. 378–403. 10.1016/j.comnet.2012.07.021.
4. Egele, Manuel & Kruegel, Christopher & Kirda, Engin & Yin, Heng & Song, Dawn. (2007). Dynamic Spyware Analysis.. 233-246.
5. Khonji, Mahmoud & Iraqi, Youssef & Jones, Andy. (2013). Phishing Detection: A Literature Survey. IEEE Communications Surveys &amp Tutorials. PP. 1-31. 10.1109/SURV.2013.032213.00009.
6. Duraisamy, Balaganesh & Chakrabarti, Amlan & Midhunchakkaravarthy, Divya. (2018). Smart Devices Threats, Vulnerabilities and Malware Detection Approaches: A Survey. European Journal of Engineering Research and Science. 3. 7. 10.24018/ejers.2018.3.2.302.
7. Sadiq M, Iqbal MS, Naveed K, Sajad M (2016) MOBILE DEVICES FORENSICS INVESTIGATION: PROCESS MODELS AND COMPARISON. ISJ Theoretical & Applied Science, 01 (33): 164-168.
8. Raghav, Shivankar & Saxena, Ashish. (2009). Mobile Forensics: Guidelines and Challenges in Data Preservation and Acquisition. 5 - 8. 10.1109/SCORED.2009.5443431.
9. Ayers, R., Brothers, S. and Jansen, W. (2014), Guidelines on Mobile Device Forensics, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.SP.800-101r1
10. "CWAGWEB – Best Practices for Seizing Eletronic Evidence" https://www.cwag-web.org/wp-content/uploads/2018/05/BestPracticesforSeizingElectronicEvidence.pdf, last access 15/12/2021
11. Dawson, Maurice & Wright, Jorja & Omar, Marwan. (2016). Mobile Devices: The Case for Cyber Security Hardened Systems. 10.4018/978-1-4666-8751-6.ch047.
12. Marturana, Fabio & Bertè, Rosamaria & Me, Gianluigi & Tacconi, Simone. (2011). A Quantitative Approach to Triaging in Mobile Forensics. 10.1109/TrustCom.2011.75.

10

13. Alhassan, John & Oguntoye, R. & Misra, Sanjay & Adewumi, Adewole & Maskeliunas, Rytis & Damasevicius, Robertas. (2018). Comparative Evaluation of Mobile Forensic Tools. 10.1007/978-3-319-73450-7_11.

Benefits, Issues and Best Practices of using Web Services

Rui Rebelo

Lusófona University of Porto, Portugal
ruypedro2011@hotmail.com

Abstract. Over the years, mobile devices have become an acquirement on our daily lives. Compared to other devices that can have access to web services, mobiles had a big growth in the last few years. With this being said, we can conclude that hackers can easily reach or steal an enormous amount of information and use it to manipulate or threat other people. Web services are a solution used to integrate systems and it can also be useful when it comes to communication between different applications. This technology allows new applications to communicate with older ones and that systems developed in different platforms can be compatible. These systems are components that allow applications to send and receive data. Like every software or application web services also have failures.
In this paper I will study the main threats of IT security, involving mobile devices, as well as the Benefits, Issues and Best Practices of using Web Services, by choosing one practical case to show the using of web services, approaching some known flaws and measures taken as well as some fears and preventions.

Keywords: Benefits, Issues, Best Practices, Web Services, Threats, IT Security, Mobile Services.

1 Introduction

In the last couple of years, the use of the internet has had a big growth in our daily lives in all possible areas. The mobile devices are the most used to access the internet since it's easily portable and facility of acquisition. According to [1] a study that was made in a school in Pune City, 97% of the students use mobile devices, called smartphones, and only 3% do not use them.

As we all know, almost every daily needs can be done on mobile devices, such as talking to a distant person, accessing our emails, a document that was sent to us or even our bank account, among many other utilities that mobiles provide. Having that in mind, there are a lot of existing threats, not only of mobiles being the most used electronic devices but also because many people save personal information, such as credit card details, social security number, among other relevant information that can be used to harm others.

In section two we will mention some of the most used mobile operating systems
In section three, we will see the most important threats in the security area and whether these threats had a big growth during the last couple of years, based on previous studies.
In section four we will focus on the advantages and disadvantages, best practices of web services
And finally, a practical case were we can see how to make an XML Injection very easily.

2 Most used mobile operating systems

As we all know, in the beginning, when phone were news, they worked differently from what we are used to currently. They weren't that developed since they were used for phone calls only. As years gone by, these devices have evolved allowing for example gaming, taking pictures, listening to music, among any other activities that we thought not possible. But for this to be possible, all the mobile devices have the need to have installed an operating system. But what is an operating system?

Operating systems began to be used in computers to mediate between the hardware and the software, which means managing and controlling the resources and computing capability of a computer and allow users an interface to work with the physical computer's structure.[2] But in the beginning that interface was not "so good to the eyes", since it was just a simple command line where we executed lines of code to do the work. After a couple of years the first operating system appeared with a graphical interface and multitasking support, which is almost the same thing that we all have in our machines right now. And this leads us to another question, what mobile operating systems have in common with computer operating systems? In fact, those to different operating systems have a lot in common, because they were created to do the same task which is to mediate between the hardware and software. The only big difference is the size of the machine where they are implemented. As we also know, there is a big panoply of mobile operating systems but according to [1] when studies were made in a certain school 28,50% of the students said that they use Samsung which uses android as operating system, 21,62% said that they uses Apple's iPhone which uses IOS as operating system, which makes these two, the most used mobile operating systems. In the following we are going to talk a little bit about these two operating system's history.

According to [3], the android was initially created by Android Inc. and after that bought by Google. It was released for the first time in 2007 as Android Open Source Project. Android is a fairly young platform, its use takes place very quickly. Each major release is named in alphabetic order after a dessert or sugary treat.

Proceedings of the Digital Privacy and Security Conference 2022 | 10.11228/dpsc.04.01

According to [4], it all started in 1976 in a small garage in Los Altos, California, with three names well known, being Steve Jobs, Steve Wozniak and Ronald Wayne. Initially, the name would not be the one as we know it for but iPhone OS instead. Later in June 2010, after Apple had made some big changes in their devices, for example, to implement a store called as App Store, allowing users to buy and download applications to their devices, which led to a name changing being it now IOS. But so user could download and install the applications some adjustments were needed so that the device was capable of handling a large amount of programs.

3 Mobile principal threats of IT Security

The easy access of these devices brought us the possibility to use them in isolated environments but also in network environments. It also brought us a lot of advantages as well as some disadvantages. For devices' network or system to be safe, it has to ensure confidentiality, integrity and availability which means, only some users of the system can access sensitive information. It assures us that the information was not modified or destroyed and also that the information will not be available to users who are not logged in. But all computed devices have threats in the security area and mobile devices are not an exception. But what is a threat in the computer area? A threat as the name suggests is something that can damage the device or steal some important information from your device, sometimes forcing people to pay a large amount of money to recover that information. According to [5] this activity is caused by a person to carry out criminal acts that would harm who they steal the information from.

With this type of activity users have to be cautious since they can download a virus or any other type of threat without knowing. These devices that we carry all the time in our pockets store a lot of important information. Even if the companies provide a lot of security, as mentioned before, users are still being exposed to a big number of possible attacks. According to [6] some of these attacks will be presented in the following:

(i) Phishing-in-the-app: We discovered one way that criminals can bypass the Play Market's source code checks was by not including anything malicious in the app itself. This app is nothing more than an embedded website, which make users believe they are having the perfect experience, not knowing that they are being a victim of phishing.

(ii) Supply chain compromise: Following a lead from an online message board, we discovered a Trojanized version of a legitimate app that had been included in the factory firmware. The original application, called Sound Recorder, was modified to include lines of code that were not necessary for its purpose. This additional code was used to intercept and secretly send SMS.

(iii) Cryptominer code in games or utilities: The SophosLabs team have, in the normal course of looking for mobile malware, encountered a significant jump in the number of apps that, without notifying the user, included cryptominer code in the app. The cryptominer is a way to earn digital coins that can be converted to real money. To earn the coins users need to solve mathematical puzzles. To do this quickly, hackers implement code in applications that users will download. The code would run whether or not the app itself was running, and functioned as a constant drain on the phone's battery.

(iv) Advertising click-fraud embedded in apps: Advertisement fraud is, surprisingly, one of the most profitable criminal enterprises nowadays, and mobile apps appear to be a key part of this subtle crime. This type of crime occurs frequently in mobile applications. Sometimes, when we are playing a game on our mobile device, advertising appears almost instantly without our meaning to. This type of advertising may contain some type of fraud that is not visible. This crime can be very profitable in monetary terms.

According to OWASP [7], companies should start the process of ensuring that their applications minimize ten risks. Below, we will present the ones we think are most important.

(i) Broken Access Control: Access control is used to make sure that users cannot act beyond their permissions. When this access control is broken the hacker will gain access to unauthorized information and will be able to change or destroy it.[8]

(ii) Cryptographic Failures: The first thing to determine is the level of protection the data should have. If this data doesn't have any kind of protection, it is much easier for hackers to have access to them. For example, passwords, credit card numbers, health records, personal information, and business secrets require extra protection, mainly if that data falls under privacy laws, for example, General Data Protection Regulation (GDPR).[9]

(iii) Injection: There are many types of injection like SQL, NoSQL, OS command, Object Relational Mapping (ORM), LDAP, and Expression Language (EL) or Object Graph Navigation Library (OGNL) injection. To detect if the application is vulnerable it's necessary to review the source code. Normally the injection is performed in the URL or in some input space that will be used for some query.[10]

(iv) Security Misconfiguration: An application is vulnerable if, for example, unnecessary features are enabled or installed, like unnecessary ports, accounts, or privileges that should be disabled.[11]

Proceedings of the Digital Privacy and Security Conference 2022 | 10.11228/dpsc.04.01

(v) Software and Data Integrity Failures: These failures are related to code and infrastructure that does not protect against integrity violations. This normally happen when the application uses plugins or libraries from untrusted sources. [12]

(vi) Server-Side Request Forgery: These failures occur whenever a web application searches for a remote resource without validating the user-supplied URL. It allows the hacker to force the application to send a crafted request to an unexpected destination.[13]

Other threats that can happen more frequently than we think is the loss of the device, its theft or even the accidental or malicious misuse of it. The accidental misuse of the device, can happen, for example, when we are exploring the device definitions and we change some important information, that should not be changed. Malicious use of the device can happen, for example, if we lend the device to someone and that same person changes something having access to the device in a way the owner does not know.

4 Benefits, issues and best practices of web services

Web services were implemented to solve the problem that was communication between applications that were developed a long time ago with new ones and also to communicate with others that were developed in different platforms. These services are used to allow changing data.

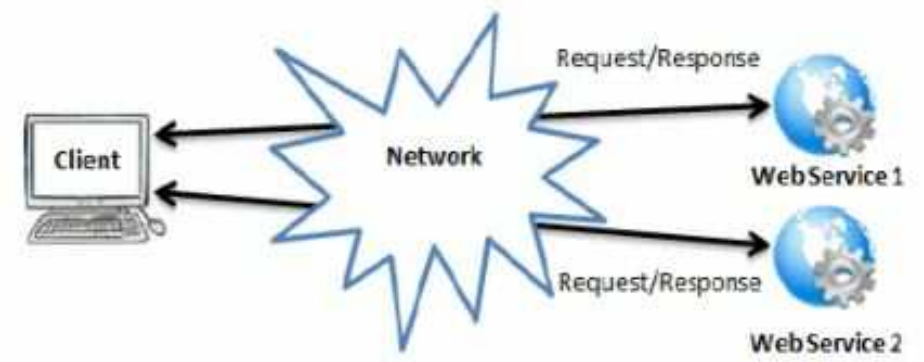


Fig. 1. Conceptual model of web services [14]

For the fact that applications have their own language, these services translate the communication to an intermediate format, being one of them XML. According to [15] XML is a simple text-based format for representing structured information: documents, data, configuration, books, transactions, invoices, and

Proceedings of the Digital Privacy and Security Conference 2022 | 10.11228/dpsc.04.01

a lot more. It was derived from an older standard format called SGML (ISO 8879), in order to be more suitable for Web use. As every system or application, web services also need to have many security measures like authentication, confidentiality, integrity and availability to ensure the best security and reliability.

4.1 Benefits

According to [16], web services provide several technological and business benefits, such as:

(i) Application and data integration
(ii) Versatility
(ii) Code re-use
(iv) Cost savings

As mentioned before, web services provide application and data integration because they allow applications to communicate between them and none of the parts need to know how the other is implemented or in what format the data is stored.

The versatility allows people to access the web service via a web-based client interface. The client can even combine data from multiple web services. For example a user being able to combine a product's price from different sellers and see which one is the least expensive and save some money.

The re-use of code can be very helpful because a lot of clients can use the same portion of code to do different tasks. Instead of having to create different services for different things, portions of a service can be simply re-used allowing the client to have some flexibility.

All three benefits mentioned before lead us to a fourth benefit that is cost savings. The need to create applications to connect with others can be very expensive and web services solve that issue easily so that cost is removed and money can be used to add additional value to the main application. Web services also take advantage of ubiquitous protocols and Web infrastructure that already exist in every organization, so they require little if any additional technology investment.

4.2 Issues

According to [17], the threats in web services can be through message or service level. The service level threats can involve UDDI, which is a protocol that defines how clients communicate with UDDI registers and it's also a specific set of replicated global records.[18] These threats can also involve WSDL which is a

Proceedings of the Digital Privacy and Security Conference 2022 | 10.11228/dpsc.04.01

language based on XML used to create services contracts. These contracts have all the information needed to create a client able to communicate with the web service.[19] Can also involve XML. In the following we are going to present some of the service level threats in a short form (the full text can be found at [17]):

(i) WSDL and UDDI attack: An attacker can access any public information available WSDL file and tamper with it. The former scans the WSDL file and exposes the operational information, ports, etc. The last one tampers the data and can even gain access to confidential information.

(ii) Malicious Code Injection and Identity Spoofing: This occurs when an attacker is able to inject malicious code and spoil the functionality of the service. Identity Spoofing occurs when the attacker takes off the identity of the service requester or the service provider.

(iii) XML Schema Tampering: The attacker can modify the original XML Schema and make it erroneous, causing the service to end up with failures.

(iv) Session Hijacking: An attacker can steal the token from the user and gain unauthorized access to the resources provided. This leads us to false request or replies and, because of that, we can say that the session was hijacked.

(v) Message Injection or Alteration: Messages traded between the server and the client can be modified or malicious messages can be added. This can provide the hacker many privileges.

(vi) Replay of Messages: The attacker captures a valid message traded between the user and the server and replays it later thus leading him to access sensitive information via unauthorized access. Usually this is the first step to hijack the session and tamper with the services.

(vii) Message Confidentiality and Eavesdropping: Interception of messages is always a threat to web services. Traditional security mechanisms are not sufficient to secure the web services against such threats.

4.3 Best Practices

As seen before, web services have benefits, as well as some issues. In the following we are going to present some general measures to use in web services and then some measures to solve the issues that can happen. As mentioned earlier, some of the best security practices are ensuring the confidentiality, integrity, and availability. These web services also need other type of security that is not just digital security. They also need a physical one, which means that these same web services need to be in data centers, which location is only known to a small number of people. Access to these data centers must be registered and accredited to be allowed.

According to[20], protecting credentials and session cookies is one of the most difficult tasks for a developer. In the following, some preventive measures that can be applied are going to be presented in a short form (the full text can be found on [20]):

(i) Using Secure Socket Layer: All the credentials should be stored in an encrypted form, for example, an attack to the database or some file system should not compromise credentials.

(ii) Expire Session after Inactivity: Forcing an automatic logout, after a reasonable time can be a good idea. This way an abandoned session will not be active for a long period of time and thus reduces the chance that a hacker has to find an active session.

(iii) Do Not Make Session Identifiers Viewable: This problem occurs in the GET method. The GET variables are always in the path string of the browser. With this, printing one of these pages will show always the identifier because most of the time, and most of the browser print the URL in the header. To prevent that we should use POST method.

(iv) Provide Secure Logout: As the name suggests we should provide the user a safe logout, that when used, the session will be inactivated. For example, when an users logs out, his session should be saved in the database and then deleted, or that same session should be marked as disabled. Using this when someone uses that session to login, the server can assume that this session is not valid.

(v) Use Strong Encryption on All Transmissions: The non use of encryption will turn the system almost completely insecure. The malefactor will be able to observe the communications done. But if the data is already encrypted this is not and issue since the data is rendered unreadable.

(vi) One-Time Cookie: One time cookies are generated by the reverse proxy server for each request of the user. This is a better alternative to authentication cookies that does not require volatile state in web browser.[21]

(vii) Schema Validation: The Schema Validation can prevent attacks. It uses messages that are not conform to the Web Service description. These attacks are called deviation from message syntax. If we validate the messages that are arriving to the XML, the attacks can be discovered.[22]

5 Practical case: Web Service XML Injection

According to [22], XML Injection tries to modify the XML structure of a SOAP message or other XML document. The injection is performed by inserting content

Proceedings of the Digital Privacy and Security Conference 2022 | 10.11228/dpsc.04.01

like operation parameters, for example, "<" or ">". This attacks are possible if these characters are not escaped appropriately.
An XML Injection attack was performed also on [22]. This attack was performed against a .NET Web Service. This service has two parameters a and b, both int type. The next image shows the SOAP message how the service was invoked.

```
<Envelope>
    <Body>
        <HelloWorld>
            <a> <b>1</b> </a>

            <b> 2 </b>
        </HelloWorld>
    </Body>
</Envelope>
```

Fig. 2. Web Service attack [22]

This message could be the result from an XML Injection attack. 1 was inserted as a parameter content without escaping "<" and ">". This should not be accepted, because it violates the Web Service schema, but in the .NET accepted this message. The resultant parameter values were a=1 and b=0. Thus the attacker was able to modify the value of b just modifying the content of a. With that presented, it is easy to think about how many scenarios are capable of being created and how much restricted data the hacker can access if the changes are bigger than the ones made.

To detect these attacks is to validate the schema on the SOAP message, and if possible include also data validation. If these methods were implemented, the example shown above would not be possible to execute.

6 Conclusion

Along this paper we present numerous issues and threats and some methods to prevent them. These problems and threats are the result of being able to circumvent some implemented measures as well as being able to explore existing vulnerabilities.

With this being said, companies using web services and users are now aware of the security risks while they are using it. Nevertheless, there is still a lot to be done, such as implementing better security measures or hiring white hackers to discover vulnerabilities in web services. In the case of mobiles, the verification of applications made available to consumers, by a person, rather than just a

system. With the increasing demand for web services, new mitigation methodologies and studies are underway, proving that the security area is one of the most important.

References

1. Vaidya, Alpana & Pathak, Vinayak & Vaidya, Ajay. (2016). Mobile Phone Usage among Youth. International Journal of Applied Research and Studies. https://doi.org/10.20908/ijars.v5i3.9483
2. Wang, Yingxu. (2004). Operating Systems. https://doi.org/10.1201/9781420039870.ch144
3. Gilski, P., & Stefanski, J. (2015). Android os: a review. Tem Journal, 4(1), 116.
4. Verma, Nishkarsh & Sambhav, Saurabh. (2020). Development of iOS: A Revolutionary Transformation and the Future. INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING & TECHNOLOGY. https://doi.org/10.34218/IJARET.11.6.2020.040
5. Tasril, Virdyra & Ginting, Meiliyani & Mardiana, Mardiana & Siahaan, Andysah Putera Utama. (2017). Threats of Computer System and its Prevention. International Journal of Scientific Research in Science and Technology.
6. SophosLabs 2019 Threat Report https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophoslabs-2019-threat-report.pdf. Last accessed 16 December 2021
7. OWASP, https://owasp.org/www-project-top-ten/. Last accessed 4 December 2021
8. OWASP https://owasp.org/Top10/A01_2021-Broken_Access_Control/. Last accessed 7 December 2021
9. OWASP https://owasp.org/Top10/A02_2021-Cryptographic_Failures/. Last accessed 7 December 2021
10. OWASP https://owasp.org/Top10/A03_2021-Injection/. Last accessed 7 December 2021
11. OWASP https://owasp.org/Top10/A05_2021-Security_Misconfiguration/. Last accessed 7 December 2021
12. OWASP https://owasp.org/Top10/A08_2021-Software_and_Data_Integrity_Failures/. Last accessed 7 December 2021
13. OWASP https://owasp.org/Top10/A10_2021-Server-Side_Request_Forgery_%28SSRF%29/. Last accessed 7 December 2021
14. Sarhan, Qusay & Gawdan, Idrees. (2018). Web Applications and Web Services: A Comparative Study. Science Journal of University of Zakho. https://doi.org/10.25271/2018.6.1.375
15. W3C, https://www.w3.org/standards/xml/core. Last accessed 4 December 2021
16. Cavanaugh, E. (2006). Web services: Benefits, challenges, and a unique, visual development solution. white paper, Feb, 10.
17. Aruna S, 2016, Security in Web Services- Issues and Challenges, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 05, Issue 09 (September 2016) https://doi.org/10.17577/IJERTV5IS090245
18. IBM, https://www.ibm.com/docs/pt-br/rsas/7.5.0?topic=standards-universal-description-discovery-integration-uddi. Last accessed 4 December 2021
19. Instituto Superior Técnico Universidade Lisboa, http://disciplinas.tecnico.ulisboa.pt/leic-sod/2017-2018/labs/05-ws/wsdl/index.html. Last accessed 4 December 2021

20. Nagpal, Bharti & Professor, Asstt & Chauhan, Naresh & Singh, Nanhay & Sharma, Pratima. (2019). Preventive Measures for Securing Web Applications Using Broken Authentication and Session Management Attacks: A Study.
21. Patel, Neel & Shah, Yash & Patel, Neil & Doshi, Manan. (2017). A Review on Prevention for Session Hijacking using One-Time Cookie.
22. Jensen, Meiko & Gruschka, Nils & Herkenhöner, Ralph. (2009). A survey of attacks on web services. Computer Science - R&D. 24. 185-197. https://doi.org/10.1007/s00450-009-0092-6

Review of Serious Games Applied to Information Systems Security Audit

Carlos Cunha[1] and Hugo Barbosa [2] [0000-0003-1205-8990]

1 Lusofona University, Porto - Portugal, carloseduardopinhodacostacunha@gmail.com
2 Lusofona University, Porto - Portugal | SIIS - Social innovation and Interactive Systems, School of Engineering of the Polytechnic of Porto, Porto, Portugal, hugo.barbosa@ulp.pt

Abstract. With the permanent evolution of the world, one thing that seems to resist the sign of the times is the classic education system. Many scholars refute this system saying that it is outdated and non-efficient, providing different solutions to remodel the current method. Among the vast options to provide a better learning experience, serious games stand out due to their benefits, such as immediate feedback, multitasking, and promoting collaborative work. This paper seeks to analyze the effectiveness of serious games when applied to a work-related situation, namely a hypothetical scenario connected with cybersecurity. To support this, there is the simple fact of an increasing number of cyberattacks, and their sophistication and effectiveness are ever-growing. A wide variety of cyberattacks and social engineering make so no company is safe. That's one of the main reasons why cybersecurity must never be overlooked in any company, since an attack can cause losses and, sometimes, may even render the company workless for hours. The course of developing a serious game is fundamentally the same as developing a normal game. But, when designing and developing the game mechanics, it's essential to never overlook the pedagogic component of it. Furthermore, after the moment of the announcement, release, and distribution, evaluation studies must be made, not only to analyze the satisfaction but also for the sharpening set of skills developed throughout the game. The game-based learning applied to cybersecurity has already hit the market, having a wide number of serious games solutions made available by companies.

Keywords: Serious Game · cybersecurity · Education · Training · Security Audit, Game-Based Learning, Simulation.

Proceedings of the Digital Privacy and Security Conference 2022 | 10.11228/dpsc.04.01

1 Introduction

Having fun and relaxing has always been the way of life of many people. Since the most remote times, human beings have developed unique ways to enjoy quality time, especially when trying to release stress. Ultimately, someone found out that competing towards an objective was a great way to entertain while sometimes developing soft and hard skills. With this, the concept of a game was born, and consequently, the idea of developing skills through games began to take place. The definition of games designed for a purpose beyond entertainment gave birth to what we know today as serious games.

Analyzing the serious games market, researchers point out a record maximum of 5.51 billion Euros in 2020, with studies expecting its value to reach 22.37 billion Euros by 2026. All this presents a new tendency of entities worldwide to invest in serious games due to their efficiency.

2 Serious Games

Throughout this section, it will be presented a small introduction to the concept of serious games, their historical moment in time of creation, their most notorious advantages, and a small guide of a framework for development.

2.1 Concept

Serious games are a branch of gaming industry, in which their primary goal is to promote learning and behavior change instead of entertainment. Meanwhile, this last point can mislead since serious games can be educational and exciting. Serious gaming has been developing itself in many areas such as military, education, marketing, healthcare, politics, and even city planning. The main point of serious games is the combination of learning strategies, knowledge, and game elements to teach specific skills, knowledge, and attitudes. Using the entertainment and engagement provided by the games, the players solve problems that simulate real-world situations. Serious games can be seen in every way as common games can, such as board games, electronic games, or card games.[1].

2.2 Origins

In 1970, Clark C. Abt publishes "Serious Game", a book where for the first time, the use of "serious games" as an oxymoron comes up. Abt is a researcher who worked for the U.S during the Cold War. One of his objectives was to train and educate using several computer games such as T.E.M.P.E.R. This game was used by military officers to study the Cold War conflict on a worldwide scale.

In this book, Abt sets the definition for a serious game: "*Games may be played seriously or casually. We are concerned with serious games in the sense that these games have an explicit and carefully thought-out educational purpose and are not intended to be played primarily for amusement. This does not mean that serious games are not, or should not be, entertaining*" [2].

Proceedings of the Digital Privacy and Security Conference 2022 | 10.11228/dpsc.04.01

2.3 Advantages

Among the vast benefits of game-based learning the following stand out:

- **Stimulates the mind** - Simple activities as playing any type of game can bring cognitive and psychological benefits, this way delaying natural aging. In some cases, game-based learning drives decision-making, which improves cognitive function and helps people learn valuable skills and lessons applicable to real life [3].
- **Improves self-esteem** - While playing, it is easier to interact with others, establish dialogue and overcome any kind of social and generational barriers. Therefore, the use of serious games for training improves the self-esteem of the student, who tries to explore and find alternative approaches to solve different situations in the process of learning [3].
- **Applicable to the real world** - Serious games applied for training enable students to understand new concepts and develop their skills throughout the game. Simulating real-life experiences creates a powerful interactive environment that makes it possible to practice, compete or cooperate, making students eager to learn and retain new information, leading to complete success when it is applied [3].
- **Permanent personal development** - Students are encouraged to develop their skills continuously and steadily over time, thanks to the gaming environment. Serious games for training favor skills as important as observation, motivation, overcoming criticism, strategic thinking, and, of course, soft skills. Meanwhile, games allow people just to simply be bad at them, making them realize that poor decisions or choices bring punishment to them. This way, they understand that rules are difficult to bypass and that these new concepts are meant to help them overcome themselves [3].
- **Instant feedback** - One of the benefits of game-based learning platforms is undoubtedly the possibility of obtaining immediate feedback from student performance. Serious games for training incorporate systems that permit constant monitoring. Thus, those responsible for the implementation of training can study the learning process in-depth, as well as its effect on the achievement of objectives [3].
- **Interactive nature** - Multimedia devices are very present in nowadays society and that makes people familiar with gaming elements – such as achievements, rankings, rewards, competition, levels, among others. The interactive nature of serious games enables students' engagement since all these playful elements contribute towards learning in a fun way, appropriate to the lifestyle of new generations, and favoring communication and coordination for problem-solving purposes [3].
- **Collaborative Learning** - Among the most important benefits of serious games for training is collaborative learning. People who learn through playing, usually do so in a collaborative environment, in which they work together to achieve a goal. By encouraging cooperation through the game, students increase their task satisfaction, feeling part of the team and are involved in achieving common goals [3].

Proceedings of the Digital Privacy and Security Conference 2022 | 10.11228/dpsc.04.01

2.4 Framework for development

With the already huge market of games, the market of serious games followed not only in market but in design methodologies. Through existing frameworks and methodologies there is a set of default steps that can be applied to most serious games.[4]

1º - Preliminary analysis Having a good project management from beginning may prevent catastrophic damage later on in the project, and game development is no exception. This step consists in setting the pedagogic goals for the game, study the target audience an technical constrains from the development.

1. Evaluating technical resources such as time,equipment, budget and technical skills. All these aspects have a serious impact in the game and should be analyzed to maximize success rate.
2. Defining all the pedagogic objectives. All soft and hard skills required and gained through the game should be identified. These skills will be tested through game mechanics.
3. Identifying target audience and context of play. Understanding target player base and the context where the game will be played can have play a major role in the success of the game.
4. Defining the pedagogic and game mechanics. Choosing appropriate mechanics is crucial when it comes to choose what genre the game will be. [4]

2º - Design The design component of the framework is all about building conceptual models, creating a balance between entertainment and the pedagogic component. Providing consistency between pedagogic mechanics and game mechanics will provide a engaging gameplay for the players. Also, progressive level difficulty is essential within the game, this provides that players develop new techniques and skills by themselves since the skills they had where not sufficient. This helps to build a more engaging gameplay but also stimulates player's creativity. A direct consequence of this is that the learning will be more effective.[4]

3º - Development This stage should provide technical guidance to develop the game while respecting the constrains discovered in the first step. The aim with the development of the game is to provide the best balance between time,skills and budget:

1. Support from a third party. Some companies who have more experience can provide either a full game or a vital support in the development of custom games. Though being a pricey solution, it will save a lot of time.
2. Off-the-shelf Game. A game that already exists can be used with a serious purpose, but the players will not be able to play the game without any type of guidance and instructions to complete the pedagogic objectives. Meaning the players will not be able to play the game by themselves.

Proceedings of the Digital Privacy and Security Conference 2022 | 10.11228/dpsc.04.01

3. Off-the-shelf Game with modifications. Some games let developers and players customize the game the way they want. If this happens a modification for the game can be implemented, letting the pedagogic part of the game be experienced alone. Implementing this solution may not consume much time or budget but it can be a challenge for the development team.
4. Assisted development. To relieve some pressure of video game development and improve the production, assisted methodologies may be implemented. This may be in form of tool kits that simplify the development process, requiring minimum amount of programming. The downside is that the options for customization are limited and complex scenarios may be very difficult to implement.
5. Full Development. This happens when the team has appropriate knowledge, time and resources and builds the game from scratch. In this methodology, the development team is fully responsible for all stages of game development.[4]

4º - Game assessment A crucial part of the development and could be compared to a user acceptance in general software development. This ensures that the game meets expectations regarding technical and pedagogic aspects. Developers can undercover bugs, improve gameplay and even modify game mechanics if really needed.[4]

5º - Deployment In this stage, there are rules that apply for the deployment of a serious game. Players are supervised and play sessions have limited time and are framed within the pedagogic plan. This stage is crucial for the game as a commercial product, the use of marketing campaigns, demonstrations and dedicated websites are among the techniques used by other companies.[4]

6º - Player assessment Finally, to determine the success of the game teaching new skills, its necessary to evaluate players. Some game mechanics can be implemented in order to track and evaluate players directly while playing. If pedagogic mechanics are perfectly implemented, players should acquire expert skills upon completion of the game.
Test surveys and questionnaires could be used in a way that does not require external intervention.[4]

3 Cybersecurity

According to [5], cybersecurity defines the practice of protecting systems, networks, and programs from digital attacks. These attacks are usually aimed at accessing, changing, or destroying sensitive information, extorting money from users, or interrupting normal business processes. Besides this, [5] also claims that implementing effective cybersecurity measures is proving more challenging due to the rise in the number of devices and attackers being innovative. An

Proceedings of the Digital Privacy and Security Conference 2022 | 10.11228/dpsc.04.01

effective cybersecurity approach has multiple layers of protection spread across computers, networks, programs, or data that one intends to keep safe. In an organization, the people, processes, and technology must complement one another to create an effective defense from cybercrime. Organizations are responsible for structuring an effective framework capable of dealing with attempted and successful cyberattacks. Technology is also essential for giving organizations and individuals the computer security tools needed to protect themselves from cyberattacks. Five main entities must be protected: end-point devices (computers, for example), smart devices, router devices, networks, and cloud servers.

In today's connected world, everyone benefits from advanced cyber-secure programs. At an individual level, a cyberattack can result in losing everything, from identity theft, extortion attempts, to loss of crucial data. On the other hand, critical services, and infrastructures, as power plants or hospitals need reassurance when fighting cyberattacks. That's the main reason why securing these, and other organizations are essential to keep our society normal functioning [6].

3.1 Types of Cyberattacks

Cybercrime is an ever-changing practice, but almost every type of attack can fall in-to these main categories:

- **Phishing** - Phishing is the practice of sending fraudulent emails that resemble reputable sources, like an online bank access point. The aim is to steal sensitive data like credit card numbers and login information. It's the most common type of cyberattack [7].
- **Ransomware** - Ransomware is a type of malicious software designed to extort money by blocking access to files or even the whole system through advanced encryption, paying the ransom won't guarantee the release of the files [8].
- **Malware** - Malware is intrusive software designed to gain unauthorized access, steal, or erase data, or cause significant damage to a computer system.
- **Social Engineering** - Social Engineering is a strategy used to trick someone to reveal sensitive information. Soliciting a monetary payment or gaining access to a computer, and therefore its data, are among the vast type of socially engineered attacks. The combination of social engineering and any of the attacks listed above can make people more likely to trust an external link, download malware, or even trust a malicious source of information [9].

3.2 COVID-19 and Cybersecurity

In consequence of the rise in cyberattacks and the fear of their information be leaked, some patients may not be as talkative about certain aspects of their medical history and/or condition, this can impact the quality of care [10].

Proceedings of the Digital Privacy and Security Conference 2022 | 10.11228/dpsc.04.01

4 Applying Serious Games to CyberSecurity

When it comes to cybercrime prevention, every measure that a person or a company takes is vital. Cyber attacks get even more sophisticated and different every hour, so there is no true way to be completely safe from them. Although regular back-ups, updated software, proper insurance that protects against cybercrime, and a well-designed data breach emergency plan can protect against a good range of cybercrimes, there is always a human element. Restrict administrative policy (the fewer people have access to sensitive data, the better) and a background check on every employee (identify criminal pasts) will always be vital to train staff.

All employees should have continuous training about cybercrime and how dangerous it can be at personal and business levels. Staff should have good knowledge about strong authentication, always making sure passwords agree to these traits:

- **It's long enough**, making it harder on brute-force attacks
- **Uses special characters** (lowercase, uppercase, numerals, and symbols)
- **Avoid complete words**, to avoid a dictionary-based attack.
- **Change regularly the password**, using the same pass for a long period can make the password vulnerable.
- **It's not shared across devices**.

Beyond a good password policy, staff should also be able to identify and know how to act upon being the target of a phishing or social engineering attack. Employees should: always check the reliability of email senders and their format; always suspect when the email sender makes an unusual or unexpected request; hover links to make sure they lead to where they say they do; and scan every attachment sent before opening it.

Social engineering falls beyond just checking sources since attackers seek to exploit the employee's will to be at service and help people. An attacker will pose as a vendor or someone in need of help to trigger certain feelings in the employee making it easier to get information from them [11].

4.1 Cyber Security Skills Represented with a LM-GM model

The LM-GM (Learn Mechanics - Game Mechanics) model can be interpreted as of having two axes. The horizontal axis lie the learning and game mechanics analogous to a breath-first search. Side or leaf nodes represent functional mechanics supporting the core. The following table represents a LG-MG model applied to cybersecurity [12]

Adapting the model presented in "Learning Mechanics - Game Mechanics" to the cyber-security theme. To use the resulting customized Learning Mechanics-Game Mechanics (LM-GM) map, the first grid should be used as a transitional layer between cyber-security skills and game mechanics [4][12].

Proceedings of the Digital Privacy and Security Conference 2022 | 10.11228/dpsc.04.01

Cyber Security Skills		
Use of appropriate hardware	Proper hardware disposal	
	Backing up data on separate devices	
Software updates	Using appropriate encryption	Using security software (anti-virus)
	Avoiding remote access / online services	
Using strong passwords	Avoiding disclosing personal information	Avoiding untrusted / unknown networks
	Secure online payment / mobile banking	
Being able to identify potentially dangerous searches	Being able to identify social engineering	Being able to identify and react to cyber threats and cyber crimes
Controlling and monitoring people with physical / remote access to assets	Protecting access to critical assets (machines and networks)	Establishing usage rules
	Being able to identify legal from illegal use of a computer or software	

Fig. 1: LM-GM map changed to match Cyber Security Skills [4]

Proceedings of the Digital Privacy and Security Conference 2022 | 10.11228/dpsc.04.01

4.2 Applications

Applying serious games to the cybersecurity environment is nothing new. Since the games provide a safe environment for testing and learning it is easy to get creative and explore the world of cybercrime within the games. This subsection presents some innovative ideas for implemented commercial applications.

Escape Room An example of an application of a serious game to train employees is the escape room provided by the company InfoSequre. An escape room is a set of challenges (theme-based) that a group of players must complete escaping the room, normally in less than an hour. The security awareness escape room aims to introduce the topic of cybersecurity and engage some curiosity into the players, so it is more brought up in the office. One particularity of this project is the fact that the escape room is built on a trucks' trailer, so it is easier to get access [13].

Virtual Reality Experience Virtual Reality (VR) is a computer technology developed to bring the user into a virtual-simulated environment. Stimulating multiple censorial systems, VR experiences demonstrate to be very immersive and educational. InfoSequre, the same company that provides the escape room experience, made a virtual reality game, which sets 2 teams against each other competing for which one detects the greatest number of phishing emails and consequently prevents cyber accidents. The fastest team wins the game, and the results are then announced by a security awareness professional who will discuss with the players, so no doubt remains after the game [14].

Interactive Game This online interactive game, created by The Fugle Company, lets you play as the Chief information officer (CIO) of Fugle that is getting ready to launch a bio metrically authenticated mobile payment application when suddenly, his company is targeted by a cyberattack. The game lets you choose which measures to take preventive and proactively, unfolding the story as the player makes different decisions that can lead to a bad ending or a good one. Some choices also require you to spend virtual currency reflecting on the budget before making any decision [15].

In the end, every choice made is revisited by a security specialist explaining each option and why it would succeed or fail [15].

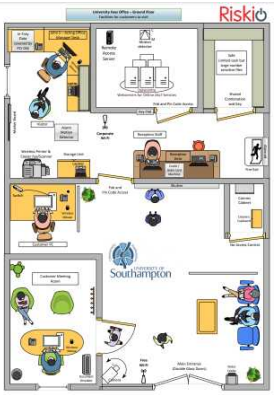
5 Board Game Riskio as an example of a serious game applied to cybersecurity

The game is designed to educate players to better manage risk situations and know what decisions to make when faced by certain types of attacks. The objective of Riskio is to give players a safe playground where they can identify threats to the organization data, learn what could be done and reflect if that's the best

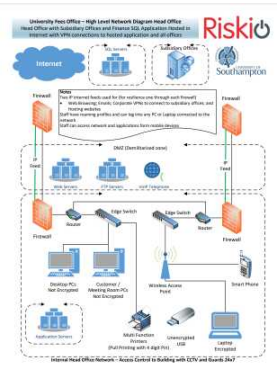
decision to make. This game does not require players to have any previous experience in software development, making it easier to play with a wide variety of people with different tech related skill [16].

5.1 Game Setup

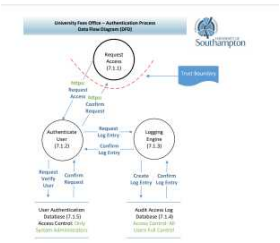
Riskio can be played in up to three boards (see Figure 2), each representing a different case scenario to protect – Office Diagram (illustrated on Figure 2a), Network Diagram (transposed on Figure 2b), and Data Flow Diagram (visualized in Figure 2c) [16].



(a) Office Diagram



(b) Network Diagram



(c) Flow Diagram

Fig. 2: Riskio Game Boards

The game is composed of a Game Master (GM), who's someone that has a piece of a vast knowledge of cybersecurity and is responsible for setting up the game, shuffling the three decks (see Figure 3) - attack (illustrated on Figure 3a), defense (transposed on Figure 3b), and information (visualized in Figure 3c) -, and explaining the game to new players. This game is played by rounds and has a recommended number of players varying between 3 to 5 individuals. From this group, the player on the left of the GM will be chosen to be the first attacker and at the end of each round, it will go clockwise. At the start of the game, every player is given a hand of defense cards, a personal deck from which they will choose to strengthen their defenses for the upcoming attacks. The players will take turns trying to set up an attack while the other players present valid defenses [16].

5.2 Attack phase

The attacker draws from one of the 6 small decks on the board. Each of these decks represents different kinds of cyberattacks. It is given a moment to the

(a) Attack Deck (b) Defense Deck (c) Information Deck

Fig. 3: Riskio Decks

player to think, build up a strategy and describe to the GM how that attack would occur. After judgment, the GM is going to evaluate the attacker's performance and either valid or not his attack. He will be awarded up to 3 points if it is successful [16].

5.3 Defense Phase

After the attacker declares his attack, it is time for every defender to defend. Each defender must choose a defense card from their deck at hand and place the card facing down until every defender is ready. When that occurs, the GM will ask each defender to describe how they would defend against the attack. If the validation of the defense card presents to be successful, then the defender wins up to 3 points. When every defense is evaluated, the round ends [16].

5.4 Optional Bonus Round

At the end of each round, the GM can be innovative and start a different round, in which he will be the attacker, and every player will be the defender. The attack card is drawn from the informative deck at his disposal. After hearing every defender's security scenario, he will appreciate and reward up to 3 points, similar to the defense phase [16].

6 Conclusions and Research Perspectives

Throughout this paper is revealed some advantages of adopting serious games to make people more aware of cybersecurity-related problems. Studies were presented to demonstrate that workers learned new technical terms and developed new skills, improving their perception when engaging in cybersecurity situations.

It is fair to affirm that the market of serious games is going to continue growing and, therefore, in the following decades to enhance even more. New applications, new games are going to be developed, and their applicability is going to increase, due to the need to improve the workforce's cybersecurity skills.

References

1. T. Susi, M. Johannesson, and P. Backlund, "Serious games - an overview," 11 2015. [p. 2]
2. C. Abt, *Serious Games*. University Press of America, 1987. [p. 2]
3. "Serious games for training: 8 benefits that will surprise you : Gamelearn: Game-based learning courses for soft skills training." `https://www.game-learn.com/en/resources/blog/serious-games-for-training-benefits/`. (Accessed on 12/12/2021). [p. 3]
4. A. Le Compte, D. Elizondo, and T. Watson, "A renewed approach to serious games for cyber security," in *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, pp. 203–216, 2015. [p. 4, 5, 7, 8]
5. "What is cybersecurity? - cisco." `https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html`. (Accessed on 01/14/2022). [p. 5]
6. "What is a cyberattack? - most common types - cisco." `https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html`. (Accessed on 12/13/2021). [p. 6]
7. "What is phishing? examples and phishing quiz - cisco." `https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html`. (Accessed on 12/13/2021). [p. 6]
8. "What is ransomware? - definition and protection tips - cisco." `https://www.cisco.com/c/en/us/solutions/security/ransomware-defense/what-is-ransomware.html`. (Accessed on 12/13/2021). [p. 6]
9. "What is a social engineering attack & how to stop it — avg." `https://www.avg.com/en/signal/what-is-social-engineering`. (Accessed on 12/13/2021). [p. 6]
10. C. M. Williams, R. Chaturvedi, and K. Chakravarthy, "Cybersecurity risks in a pandemic," *J Med Internet Res*, vol. 22, p. e23692, Sep 2020. [p. 6]
11. "Best practices for how to train employees for cyber security." `https://www.coxblue.com/8-tips-and-best-practices-on-how-to-train-employees-for-cyber-security/`. (Accessed on 12/16/2021). [p. 7]
12. "sv-lncs." `https://arxiv.org/ftp/arxiv/papers/1805/1805.08053.pdf`. (Accessed on 12/17/2021). [p. 7]
13. "Security awareness escape room — infosequre." `https://www.infosequre.com/security-awareness-escape-room`. (Accessed on 12/14/2021). [p. 9]
14. "Security awareness vr experience truck — infosequre." `https://www.infosequre.com/security-awareness-virtual-reality-experience-truck`. (Accessed on 12/14/2021). [p. 9]
15. "About — targeted attack: The game – defend your data. choose wisely. succeed or fail.." `http://targetedattacks.trendmicro.com/about-the-game.html`. (Accessed on 12/14/2021). [p. 9]
16. S. Hart, A. Margheri, F. Paci, and V. Sassone, "Riskio: A serious game for cyber security awareness and education," *Computers and Security*, vol. 95, p. 101827, 2020. [p. 10, 11]

Papers in alphabetical order

Authors in alphabetical order

Conference EOI :10.11228/dpsc

DPSC2022 Proceedings EOI: http://eoi.citefactor.org/10.11228/dpsc.04.01

PRIVACY AND SECURITY CONFERENCE 2022

PRIVACYANDSECURITYCONFERENCE.PT