Smart Innovation, Systems and Technologies 255

Álvaro Rocha
Carlos Hernan Fajardo-Toro
José María Riola Rodríguez *Editors*

Developments and Advances in Defense and Security

Proceedings of MICRADS 2021

KES International

Springer

Smart Innovation, Systems and Technologies

Volume 255

The Smart Innovation, Systems and Technologies book series encompasses the topics of knowledge, intelligence, innovation and sustainability. The aim of the series is to make available a platform for the publication of books on all aspects of single and multi-disciplinary research on these themes in order to make the latest results available in a readily-accessible form. Volumes on interdisciplinary research combining two or more of these areas is particularly sought.

The series covers systems and paradigms that employ knowledge and intelligence in a broad sense. Its scope is systems having embedded knowledge and intelligence, which may be applied to the solution of world problems in industry, the environment and the community. It also focusses on the knowledge-transfer methodologies and innovation strategies employed to make this happen effectively. The combination of intelligent systems tools and a broad range of applications introduces a need for a synergy of disciplines from science, technology, business and the humanities. The series will include conference proceedings, edited collections, monographs, handbooks, reference books, and other relevant types of book in areas of science and technology where smart systems and technologies can offer innovative solutions.

High quality content is an essential feature for all book proposals accepted for the series. It is expected that editors of all accepted volumes will ensure that contributions are subjected to an appropriate level of reviewing process and adhere to KES quality principles.

Indexed by SCOPUS, EI Compendex, INSPEC, WTI Frankfurt eG, zbMATH, Japanese Science and Technology Agency (JST), SCImago, DBLP.

All books published in the series are submitted for consideration in Web of Science.

More information about this series at http://www.springer.com/series/8767

Álvaro Rocha · Carlos Hernan Fajardo-Toro ·
José María Riola Rodríguez
Editors

Developments and Advances in Defense and Security

Proceedings of MICRADS 2021

Springer

Editors
Álvaro Rocha
ISEG
University of Lisbon
Lisbon, Portugal

Carlos Hernan Fajardo-Toro
Fundación Universitaria Konrad Lorenz
Bogota, Colombia

José María Riola Rodríguez
Escuela Naval Almirante Padilla
Cartagena, Colombia

ISSN 2190-3018 ISSN 2190-3026 (electronic)
Smart Innovation, Systems and Technologies
ISBN 978-981-16-4883-0 ISBN 978-981-16-4884-7 (eBook)
https://doi.org/10.1007/978-981-16-4884-7

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Preface

This book contains a selection of papers accepted for presentation and discussion at the 2021 Multidisciplinary International Conference of Research Applied to Defense and Security (MICRADS'21). This conference had the support of Escuela Naval de Cadetes "Almirante Padilla," Armada de Colombia, COTECMAR and AISTI (Iberian Association for Information Systems and Technologies). It took place online in Cartagena, Colombia, August 18–20, 2021.

The 2021 Multidisciplinary International Conference of Research Applied to Defense and Security (MICRADS'21) is an international forum for researchers and practitioners to present and discuss the most recent innovations, trends, results, experiences, and concerns in the several perspectives of defense and security.

The Program Committee of MICRADS'21 was composed of a multidisciplinary group of more than 200 experts from 39 countries around the world and those who are intimately concerned with Research Applied to Defense and Security. They have had the responsibility for evaluating, in a "double-blind review" process, the papers received for each of the main themes proposed for the conference: (A) systems, communication and defense; (B) strategy and political–administrative vision in defense; and (C) engineering and technologies applied to defense.

MICRADS'21 received 117 contributions from 12 countries around the world. The papers accepted for presentation and discussion at the conference are published by Springer (this book) and by AISTI and will be submitted for indexing by ISI, EI-Compendex, SCOPUS, and/or Google Scholar, among others.

We acknowledge all of those who contributed to the staging of MICRADS'21 (authors, committees, workshop organizers, and sponsors). We deeply appreciate their involvement and support that was crucial for the success of MICRADS'21.

Cartagena, Colombia
August 2021

Álvaro Rocha

Contents

Part II Computer Networks, Mobility and Pervasive Systems

Part III Analysis and Signal Processing

Part IV Wearable Technology and Assistance Devices

Part V Simulation and Computer Vision in Military Applications

Part VI Weapons and Combat Systems

Part VII Chemical, Biological and Nuclear Defense

Part VIII Health Informatics in Military Applications

Part IX Defense Engineering

Part X Leadership and e-Leadership

Part XI Planning, Economy and Logistics Applied to Defense

Part XII Strategy, Geopolitics and Oceanopolitics

Part XIII Information and Communication Technology in Education

About the Editors

Álvaro Rocha holds the title of Honorary Professor and holds a D.Sc. in Information Science, Ph.D. in Information Systems and Technologies, M.Sc. in Information Management, and B.C.S in Computer Science. He is a professor of Information Systems at the University of Lisbon—ISEG and a researcher at the ADVANCE (the ISEG Centre for Advanced Research in Management. He is also a president of the Iberian Association for Information Systems and Technologies (AISTI), a chair of the IEEE Portugal Section Systems, Man, and Cybernetics Society Chapter, and an editor-in-chief of both *Journal of Information Systems Engineering and Management* (JISEM) and *Iberian Journal of Information Systems and Technologies* (RISTI). Moreover, he has served as a vice-chair of experts for the European Commission's Horizon 2020 program and as an expert at the COST—intergovernmental framework for European Cooperation in Science and Technology, at the Government of Italy's Ministry of Universities and Research, at the Government of Latvia's Ministry of Finance, at the Government of Mexico's National Council of Science and Technology, and at the Government of Polish's National Science Centre.

Carlos Hernán Fajardo-Toro holds Ph.D. in Computer Science and M.Sc. in Supply Chain Management from the University of Vigo. He holds bachelor's degree in Business Administration at Icesi University—Colombia. He was a professor at the University of Vigo, and currently, he is a professor at Konrad Lorenz University and leader of the research group of engineering at UNITEC in Bogotá Colombia. He is also a member of IEEE Computational Intelligence Society and the Iberian Association for Information Systems and Technologies (AISTI). He has developed consulting work for the process of redesign of processes and digitization in different entities, collaborating with the lifting and proposal of the information system of the intelligence division of the Colombian police—DIPOL. He is also in projects for the development of expert systems with the Colombian National Navy.

José María Riola Rodríguez holds Ph.D. in Naval Architect from the Polytechnical University of Madrid (UPM), is a retired Captain of the Royal Navy of Spain, and holds a Degree in Psychology from the UNED University. He was a specialist for Managers in the European R+D+i program at the Spanish Office for Science and Technology (SOST) and a national representative at the European Defense Agency (EDA) and Science and Technological Organization (STO). He was a professor at the Higher Technical School of Naval Architects (ETSIN) of the Polytechnical University of Madrid during more than 20 years, and he is currently a professor and research group leader at the Admiral Padilla Naval School (ENAP). Among his works can be highlighted a seakeeping engineer at El Pardo Hydrodynamics Model Basin (CEHIPAR), director at the Watch and Technological Foresight System (SOST) of the Ministry of Defense, designer of the F-110 Frigates, and expert evaluator at the European Commission Sixth Research Framework and Horizon 2020 programs.

Part I
Cybersecurity and Cyberdefense

Chapter 1
An Analysis of Cyber Espionage Process

Richard Rivera, Leandro Pazmiño, Fernando Becerra, and Jhonattan Barriga

Abstract The recent increasing cases released worldwide on espionage require a knowledge systematization study in this area. This paper presents a general scheme of cyber espionage process based on a literature review of remarkable cases which generated news about this topic and includes the malware report analysis made by security vendors. To understand the aspects involved and the approaches employed, we defined a general model to cover all phases used by cyber espionage. Our model considers two main aspects: first, the technical aspect driven by the rapid advance of information and communication technologies (ICT), as well as the software engineering level used by cybercriminals to create sophisticated malware; second, the human aspect influenced by the power struggle between nations and politicians, also considering the lack of technological knowledge or training in organizations. As a result, it allows the attackers using social engineering as the most effective mean for systems intruding.

1.1 Introduction

Computer security has become an area of international, academic, technological, social, and economic importance for all nations. Malware development has become more sophisticated, and today, it is used as a tool to deploy cyber espionage [1].

R. Rivera (✉) · L. Pazmiño · F. Becerra
Escuela de Formación de Tecnólogos, Escuela Politécnica Nacional, Quito, Ecuador
e-mail: richard.rivera01@epn.edu.ec

L. Pazmiño
e-mail: leandro.pazmino@epn.edu.ec

F. Becerra
e-mail: fernando.becerrac@epn.edu.ec

J. Barriga
Facultad de Ingeniería de Sistemas, Escuela Politécnica Nacional, Quito, Ecuador
e-mail: jhonattan.barriga@epn.edu.ec

Á. Rocha et al. (eds.), *Developments and Advances in Defense and Security*,
Smart Innovation, Systems and Technologies 255,
https://doi.org/10.1007/978-981-16-4884-7_1

Therefore, this topic should be an academic research field for computer science. In [2], it is mentioned that in 2020 there was an increase in cybersecurity attacks due to the appearance of the COVID-19. The increment targeted social engineering and malware; these types of attacks increased more than 86%. Attackers are taking advantage of this fear to get profits. Thus, we note the urgent need to carry out a systematized study of the existing knowledge of cyber espionage [3].

In a frequently cited statement from May 2013, General Keith Alexander, US National Security Agency Director, at that time described cyber espionage as "the greatest transfer of wealth in history" [4]. Traditional espionage dates back a long time, even now it continues to be studied as part of history. It has caused events of worldwide controversy. Currently, traditional espionage and cyber espionage support each other in large espionage operations. In recent years, due to the great development of information systems, malware development has grown as well with new and more complex encryption and obfuscation techniques. They have established the cyberspace as a large field where individuals, organizations, and nations could gain advantages illicitly accessing to confidential information using espionage techniques. However, this is not the only opportunity it offers to potential aggressors since it can also be used as a vehicle for any kind of illegitimate activities [5]. It could cause several damages including information leakage, privacy and financial losses, systems functionality deterioration, facilities destruction, legal and even war confrontations, among others.

These cyber espionage illegal activities require a way to be marketed. As a result, the actors involved in those cybercrimes prefer using communications to keep their anonymity. It can be done using Tor to browse through specific and specialized pages on the deep Web where this type of illegal activities can be marketed.

The methodology used within this work is a review of recent literature. We know that the most notable cyber espionage research is mainly performed by security service providers, and therefore, our research paper presents three main contributions. First, an analysis of the approaches used in cyber espionage. Second, an analysis of the role that malware plays in espionage. And third, an approximation of the general process used by most of the cyber espionage cases.

1.2 Cyber Espionage

Cybercriminals are always looking for new techniques and methods to carry out their illicit activities, and therefore, each day there are increasingly better approaches to cyber espionage. Although more advanced techniques are being developed, two clear aspects remain: the human and the technical. The human aspect is motivated to initiate espionage by power, politics, economy, and manipulating people's knowledge applying social engineering to achieve their objectives. On the other hand, the technical aspect is used by espionage to develop sophisticated and complex malware. To study these approaches, we have taken these aspects to perform a detailed analysis of the role played by them in cyber espionage, also including a new approach from the service perspective, which is gaining notoriety, and it is entitled as espionage-as-a-service (EaaS) [6].

Social Engineering The weakest link of the information security chain is the human being undoubtedly. So far, there are no known controls to protect users from this type of attack. In fact, these attacks are so effective that they do not require technical expertise to obtain valuable information. In [7], it is mentioned that social engineering is a social and psychological process when an individual extracts information of a target organization. Even a small portion of information gathered represents a door to compromise the confidentiality, availability, and integrity of the victim organization's information. It is emphasized at [8] that the main target of this type of attack is people, so the attackers use persuasion and influence to manipulate their victims. Additionally, this attack is classified into the following:

- **Physical approaches.** The attacker performs tasks to search physical information, such as searching the trash for "dumpster diving". Robbery and extortion are other types of attacks that fit into this classification.
- **Social approaches.** It is based on creating a relationship with the victim and using persuasion to obtain as much information as possible.
- **Social engineering reverses.** In these attacks, the victim asks for help to the attacker. To do so, the attacker sabotage victims' systems and then contact them to offer solving the problem, and finally, the attacker does so, but asks to the victim for sensitive information (for instance access credentials).
- **Technical approaches.** The objective is to search for personal information of the victim over the Internet using tools like Maltego or gathering information from social networks [9].
- **Socio-technical approaches.** These attacks are the most powerful, since attackers use bait (abandoned USB devices, Web sites, or e-mails) to take advantage of people's curiosity and obtain valuable confidential information. A social engineering attack is mainly composed of four phases: (i) research, (ii) building a trustful relation, (iii) exploiting the trust obtained, and (iv) using information [7].

These phases are recurrent until fulfilling the objective of using the collected information.

Espionage-as-a-service The development of technologies, infrastructures, and services oriented to the cloud have created a market of technological services in constant growth. At first, the basic model of services in the cloud was only presented in three modalities: platform-as-a-service (*PaaS*), infrastructure-as-a-service (*IaaS*), and software-as-a-service (*SaaS*). Based on this, the *XaaS* model has been established as "*Everything-as-a-service*". In other words, everything, or anything as-a-service, all the information and communication technology services were traditionally offered on site. Now, these services are delivered over the Internet for instance: monitor-as-a-service with its acronym (*MaaS*), communications (*CaaS*), and security (*SecaaS*). In addition, attacks could also be offered as-a-service, and it is the case of espionage-as-a-service with its acronym (*EaaS*). This model was proposed in [10], based on the raising cases of espionage in recent years related to the aerospace and defense industries. It proposes the following five phases:

- **Phase 1.** Objective, the actors who offer the EaaS service may be the cybercriminals who will carry out the attack by themselves. In some cases, the actors may have a buyer for the information gathered, in others, they already collected the information and look for a buyer.
- **Phase 2.** Recognition, the actor of the EAAS model employs various recognition techniques to identify attack vectors. The actor will be looking for a specific technology or product that the customer wants to acquire and is willing to pay for the service provided.
- **Phase 3.** Infiltration, there are many ways to infiltrate a high-value network, even if it is well-defended like using a phishing attack against an easy target such as compromising a vendor and attacking the target with trusted credentials. In these attacks, the attacker can impersonate an employee if it is necessary using some of the techniques mentioned above in social engineering.
- **Phase 4.** Extraction, once the information has been obtained, it is essential to leave the network without being detected. Professional cybercriminals will want to continue keeping access to victims' networks for many years, so they will take patience and time to find and test the best methods for exploiting security holes.
- **Phase 5.** Sale, stolen technology buyers will consider this expense as the cost of knowledge transfer because they could obtain third-party technologies at a lower cost. As well as many services of the *XaaS* model, a trial version of the products is offered. First, actors can offer a sample of the data stolen to initiate future relationships with potential customers.

1.2.1 The Role of Malware in Cyber Espionage

Malware is malicious software intentionally designed to gain access or cause damage to computers or even networks. These malicious programs [11] can perform a variety of functions. They include stealing, encrypting, or deleting sensitive data, altering, or hijacking core computing functions and monitoring users' computer activity without their permission. Malware uses deceitful vectors to execute or install itself on victim's machines such as unauthorized download. It is distributed using vulnerability exploitation and performs a silent installation on the victim machine [12]. Malware is usually developed by cybercriminals [13].

In large-scale cyber espionage where nations or actors with good resources take place, it is worth to introduce the case of the United States and Israeli Stuxnet worm [14]. It was designed to attack and destroy Siemens' supervisory control and data acquisition systems (SCADA). The system was used by Iran in the enrichment of uranium [4], and it is an example of cyber espionage with a specific target and destructive purpose. This worm is considered one of the most advanced malwares ever made for espionage. Other malwares were developed for more sophisticated espionage, and these malwares are Duqu, Flame, and Gauss which are the successors of Stuxnet [15].

To analyze a relevant case, in 2014 Symantec [16] security experts spent around eight months investigating one of the most sophisticated developments of computer spy malware ever seen to date. It was known as Regin, and it provides powerful tools to its creators to spy on governments, infrastructure operators, companies, researchers, and individuals. Attacks on Telcos appeared to be designed to gain access to calls routed through their infrastructure. Regin is a complex tool, and it has a modular design to allow the addition and removal of different malware functionalities. Loading and modularity features have been seen before, but Regin showed a high level of engineering and software development. For example, the tool has dozens of modules including functions such as remote access, screenshots, passwords theft, network traffic monitoring, and recovery of deleted files.

The development of this malware must have taken months or even years, implying a significant investment of resources. It has been created by nations or cyber-crime organizations with a high level of sophistication and well suited for persistent surveillance operations [17]. An analysis performed to Regin by Symantec [16] stated that this malware did not operate on a specific target nor focus on any specific industry sector. Its infections were performed in a variety of organizations, including telecommunications companies, private and small business, government entities, and research institutes.

In 2019, the President of the United States of America reached a nuclear agreement with Iran, meanwhile many U.S. companies and government agencies received attacks from both Iranian and Chinese hackers. These attacks were analyzed, detected, and mitigated by its Security Agency and by the company Fire-Eye [18]. Those attacks were aimed at obtaining confidential military information and commercial agreements.

The frequent attacks carried out in cyber espionage are advanced persistent threat (APT) malware type such as [19, 20], which have the potential of a persistent attack by remaining hidden and maintaining backdoors in systems to maintain espionage if possible. Other malwares used are typical trojans with functionalities of key loggers, backdoors, and spyware. Depending on the attacker's purpose and knowledge, they can use more advanced techniques as in the case of Reign.

1.3 General Process of Cyber Espionage

In [1], Wangen presents six phases of a malware espionage attack. Cyber espionage process is executed in most cases to fulfill the goals of the attackers, where the typical attack vector and main tool used for espionage is malware, but also social engineering techniques may be the starting point of a cyber espionage attack [29]. Hence, our work extends the phases considered by Wangen, to present a general process for cyber espionage attacks. Most of the related work about cyber espionage is performed by security vendors [16–18], where they explain technically espionage cases and techniques applied by espionage groups. Considering previous research works about cyber espionage [1, 10, 15, 16, 21–30], we have analyzed 20 relevant cases of cyber espionage to identify and create a general process, and as a result, we established the following nine phases: reconnaissance, preparation, attack, infiltration, information gathering, maintenance, information leakage, information sale, and escape.

Table 1.1 summarizes relevant cyber espionage cases. For each case or cyber espionage group, first it presents the year of publication of the case report. Then, it describes whether the cyber espionage case comprises each of the nine phases previously mentioned. Most of the cases comprise all these phases, except information sale phase, due to some reports of these cases do not mention the purpose of information leakage. But due to the nature of these types of attacks, it is considerable to argue that the sale of information may be one of the main targets of cyber espionage. The most recently reported cases do not present information about the attribution of the attack or the purpose of the information theft, probably because they are very recent cases, and the investigation is still ongoing. Finally, it shows the main attack vector, which in most cases is malware of various types, such as backdoor, trojan, remote access trojan (RAT), multi-featured malware, and spyware. There are other cases that indicate social engineering techniques such as spear phishing, e-mail attachments, spam campaigns, among others. Figure 1.1 shows an approach that encompasses the most common phases of the process used to carry out cyber espionage, and they are described below.

Reconnaissance In the first phase of this process, the attacker conducts a thorough investigation of the target to gather useful information for later use in espionage. This information may include: emails, IP addresses, employee names, and any information that can help to deploy the attack. Due to the nature of this information, social engineering and more sophisticated techniques can be used to detect the technical vulnerabilities of the target. This phase requires effort and individuals with computer security skills, even though some activities to perform reconnaissance are automated.

Preparation Depending on the objective, it can have two attack vectors based on different techniques. First, social engineering, its success relies on the preparation of the attack which requires a considerable amount of resources, time, knowledge of human psychology, language, culture, among others. Second, computer exploitation, the success of it depends on the sophistication of the malware used and the technical knowledge of the attackers to exploit possible vulnerabilities previously detected over the targeted computer systems.

Attack Once the attacker has analyzed vulnerabilities of target, selected the attack vector and the techniques with the highest success factor, the attack is carried out. Next, the attacker will attempt to obtain access credentials to the target's systems. Whether through malware, backdoor, or APT, the attacker could wait for some time to continue with the next phase or start with this one immediately, the latter can occur when the attacker believes he can be discovered. Once the attack has succeeded, internal reconnaissance is performed to escalate privileges. Most commonly, the intruder will try to get users and passwords that allow access to more resources by

Table 1.1 Phases in previous espionage cases

Cyber espionage cases	Year	Phases									Main attack vector
		Reconnaissance	Preparation	Attack	Infiltration	Information gathering	Maintenance	Information leakage	Information sale	Escape	
Mandiant's APT1 [22]	2006	✓	✓	✓	✓	✓	✓	✓	✗	✓	Several malware families
GhostNet [23]	2009	✓	✓	✓	✓	✓	✗	✓	✓	✓	Malware (RAT), phishing
Stuxnet [15]	2010	✗	✓	✓	✓	✓	✓	✓	✗	✓	Malware (multi-feature)
Flame [15]	2010	✓	✓	✓	✓	✓	✓	✓	✗	✓	Malware (RAT)
Bundes Trojaner [31]	2011	✓	✓	✓	✓	✓	✓	✗	✓	✓	Malware (trojan)
Icefog [27]	2011	✓	✓	✓	✓	✓	✓	✓	✗	✓	Malware, social engineering
Mahdi [1]	2012	✓	✓	✓	✓	✓	✗	✓	✗	✓	Malware, social engineering
Shamoon [30]	2012	✓	✓	✓	✓	✓	✓	✗	✗	✓	Malware, social engineering
Gauss [15]	2012	✓	✓	✓	✓	✓	✗	✓	✓	✓	Malware (RAT)
Red October [29]	2013	✓	✓	✓	✓	✓	✓	✓	✗	✓	Malware, social engineering
Hacking team [24]	2013	✓	✓	✓	✓	✓	✓	✓	✓	✓	Malware (multi-feature)
Careto [26]	2014	✓	✓	✓	✓	✓	✓	✓	✗	✓	Malware, social engineering

(continued)

Table 1.1 (continued)

Cyber espionage cases	Year	Phases									Main attack vector
		Reconnaissance	Preparation	Attack	Infiltration	Information gathering	Maintenance	Information leakage	Information sale	Escape	
Dragonfly-energetic bear [28]	2014	✓	✓	✓	✓	✓	✓	✓	✗	✓	Social engineering
Regin [16]	2014	✓	✓	✓	✓	✓	✓	✓	✓	✓	Malware (spy)
Fancy bear-APT28 [18, 32]	2014	✓	✓	✓	✓	✓	✓	✓	✗	✓	Malware (spy)
Oceanlotus-APT32 [33]	2017	✓	✓	✓	✓	✓	✓	✓	✗	✓	Malware, social engineering
Sowbug [34]	2017	✓	✓	✓	✓	✓	✓	✓	✗	✓	Malware (backdoor, trojan)
Slingshot [35]	2018	✗	✓	✓	✓	✓	✓	✓	✗	✓	Router vulnerability
Chafer-APT39 [36]	2018	✓	✓	✓	✓	✓	✓	✓	✗	✓	Malware (backdoor)
Double dragon-APT41 [37]	2019	✓	✓	✓	✓	✓	✓	✓	✗	✓	Malware

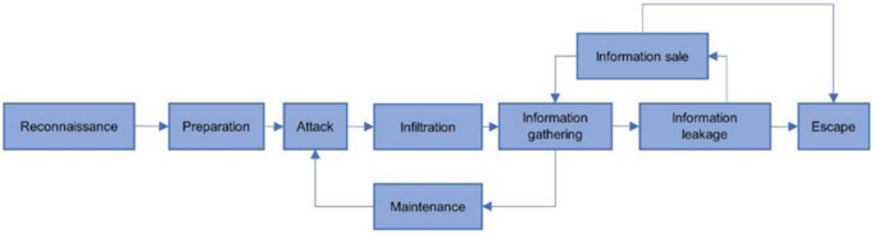

Fig. 1.1 Cyber espionage process

cracking common password hashes or performing brute force attacks. During the infiltration, the intruder tries to collect information from the systems, similar to foot printing but performed locally, to learn about the victim's environment. There are even several tools typically used in ethical hacking that can facilitate this task (e.g., nmap, dnsenum, and dimitry).

Infiltration This phase is crucial because an error could lead to the detection of the intruder. As the final part of this step, once the attackers have the necessary permissions, they could install key loggers or other specific malware that suits the attacker's needs, such as installing new backdoors on multiple systems, creating a VPN connection using legitimate credentials, authenticating on Web portals. All this in order to silently maintain its presence within the systems.

Information gathering Once the attacker knows the environment he is spying on, he must know what type of information he is looking for, such as images, text documents, e-mail files, and databases. It is important to know the language of the victim to facilitate the identification of files and directories of the systems. A specific type of malware to help in this task is advanced key loggers. They have functionalities that allow capturing the activities executed by the user, such as VoIP conversations, screen captures, typing any character, among others.

Maintenance If the espionage will be conducted over a long period, the attackers must adapt to the changing environment. If one or more implemented backdoors are detected or compromised, attackers will identify and analyze the cause to prevent this from occurring with other backdoors distributed in the systems. Once they implement the appropriate measures such as creating new attacks to maintain their permanence in the attacked systems, they will check if they can perform more attacks or adapt their current infiltration to continue with the gathering information. Therefore, this is a continuous phase, meanwhile the espionage lasts.

Information leakage This phase occurs simultaneously with the previous one, or it takes place after collecting all the information needed. The attacker usually compresses the information using formats such as RAR or 7z, protects them with a password, or applies encryption algorithms. To extract information, the attacker could transmit using proxy networks, such as the Tor network (also known as deep web), to hide his identity. In other cases, information is transmitted using the backdoors implemented in previous phases or even uploading information on servers that are compromised for later download.

Information sale As discussed in the previous section, espionage is also offered as espionage-as-a-service. In this case, customers of the stolen information or technologies often try to manage their own R&D costs through this type of technology transfer, since the acquisition cost will be lower than their own R&D. Consequently, attackers use the stolen information as a bargaining chip with the interested party, to encourage future purchases and thus take advantage of the espionage processes they have in place.

Escape This phase can occur for several reasons. Normally, once the attacker finishes gathering the information he was looking for, so he proceeds to leave the systems, perhaps leaving some backdoors open for future espionage. On the other hand, if the attacker is detected and has to abandon the mission, then he will try to erase any possible trace that could compromise his identity before leaving the systems.

1.4 Discussion

With the new technological resources being developed continuously, it has been possible to find that cyber espionage has two aspects as its basis: the human and the technical [4]. Several techniques of cyber espionage emphasize the exploitation of the human aspect as the case of social engineering. This aspect is also influenced due to the constant struggle between organizations to control a specific market, and lately also, politicians and governments want to use espionage to find out ideas from their opponents, their campaign plans, among others [38]. An assessment performed by the U.S. intelligence service has concluded that their country is being targeted by a massive cyber espionage campaign, which represents a threat for the economic competitiveness of the nation. This assessment has identified China as the country that is aggressively trying to compromise computer systems from companies and institutions of the USA to maliciously obtain their data and use it for their own benefit.

1.5 Conclusions

All countries, companies, and individuals are exposed to a computer attack and even cyber espionage. It is imperative to understand its operation. The model considers in a general way some possible scenarios where this activity is performed, deeply analyzing the influence of human aspect and its relation to social engineering as well as technical aspects involved by analyzing the role of malware. Understanding the process presented in this work, will be useful for organizations and individuals to implement necessary security measures, to avoid compromising the confidentiality of their information, as well as to notice about the importance of training on information security awareness, since as this research shows, the common way to access intrusions for espionage is through social engineering techniques. The most relevant studies in recent years on cyber espionage have been developed by companies that sell security products or services. This is an issue that must be analyzed by the academic and scientific community because espionage has shown an accelerated growth boosted by technological advances and software engineering improvements used in a bad way to develop complex malware. In this paper, we have analyzed cases of cyber espionage in the period from 2006 to 2019. As future work, it is proposed to perform an analysis on the impact of COVID-19 in the deployment of new cyber espionage attacks.

References

1. Wangen, G.: The role of malware in reported cyber espionage: a review of the impact and mechanism. Inf. **6**(2), 183–211 (2015)
2. Lallie, H.S., Shepherd, L.A., Nurse, J.R., Erola, A., Epiphaniou, G., Maple, C., Bellekens, X.: Cyber security in the age of covid-19: a timeline and analysis of cyber-crime and cyberat-tacks during the pandemic. Comput. Secur. **105**, 102248 (2020)
3. Ding, Y., Zhou, X., Liu, J., Lin, F., An, J.: Security in cyberspace: issues, challenges and suggestion. In: International Conference on Cyberspace Technology, pp. 428–430 (2013)
4. Duvenage, P., Solms, S.: The case for cyber counterintelligence. In: 2013 International Conference on Adaptive Science and Technology (ICAST), pp. 1–8 (2013)
5. Maroto, J.P.: El ciberespionaje y la ciberseguridad. In: La violencia del siglo XXI. Nuevas dimensiones de la guerra, pp. 45–76. Instituto Español de Estudios Estratégicos (2009)
6. Walubengo, J., Mutemi, M.: Treatment of kenya's internet intermediaries under the computer misuse and cybercrimes act. Afr. J. Inf. Commun. **21**, 1–19 (2018)
7. Thornburgh, T.: Social engineering. In: Proceedings of the 1st Annual Conference on Information Security Curriculum Development—InfoSecCD, p. 133 (2004)
8. Krombholz, K., Hobel, H., Huber, M., Weippl, E.: Social engineering attacks on the knowledge worker. In: Proceedings of the 6th International Conference on Security of Information and Networks, SIN, pp. 28–35. ACM, USA (2013)
9. Niekerk, B., Maharaj, M.: Social media and information conflict. Int. J. Commun. **7**, 23 (2013)
10. Taia. global: Espionage-as-a-service: The tries framework report—Taia global, Inc. (2015)
11. Sebastian, M., Rivera, R., Kotzias, P., Caballero, J.: Av class: a tool for massive malware labeling. In: Research in Attacks, Intrusions, and Defenses, pp. 230–253 (2016)
12. Guevara, R.R.: Tools for the detection and analysis of potentially unwanted programs. Ph.D. thesis, ETSI Informatica (2018)
13. Kotzias, P., Matic, S., Rivera, R., Caballero, J.: Certified PUP: abuse in authenticode code signing. In: ACM Conference on Computer and Communication Security (2015)
14. Langner, R.: Stuxnet: dissecting a cyberwarfare weapon. IEEE Secur. Priv. **9**(3), 49–51 (2011)
15. Bencsath, B.: Duqu, flame, gauss: followers of stuxnet. In: RSA Conference Europe (2012)
16. Response, S.S.: Regin: top-tier espionage tool enables stealthy surveillance (2014)
17. Symantec: Istr20 symantec internet security threat report trends for 2015
18. FIREEYE: Apt28: a window into Russia's cyber espionage operations? (2015)

19. Bonfante, G., Marion, J., Sabatier, F., Thierry, A.: Analysis and diversion of duqu's driver. In: 2013 8th International Conference on Malicious and Unwanted Software: The Americas (MALWARE), pp. 109–115 (2013)
20. Sood, A.K., Enbody, R.J.: Targeted cyberattacks: a superset of advanced persistent threats. IEEE Secur. Privacy **11**(1), 54–61 (2013)
21. Caso, J.: The rules of engagement for cyber-warfare and the Tallinn manual: a case study. In: 2014 IEEE 4th Annual International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), pp. 252–257 (2014)
22. Center, M.I.: Apt1: exposing one of China's cyber espionage units. Mandian.com (2013)
23. Deibert, R.J., Rohozinski, R., Manchanda, A., Villeneuve, N., Walton, G.: Tracking ghost-net: investigating a cyber espionage network (2009)
24. Hacking Team: Hacking Team: Remote Control System. https://web.archive.org/web/20180324235809. http://hackingteam.it (2013)
25. Mandiant, A.: Exposing one of China's cyber espionage units Feb. 2013
26. Min, B., Varadharajan, V.: Feature-distributed malware attack: risk and defense. In: Europe—an Symposium on Research in Computer Security, pp. 457–474. Springer (2014)
27. Nath, H.V., Mehtre, B.M.: Static malware analysis using machine learning methods. In: International Conference on Security in Computer Networks and Distributed Systems, pp. 440–450. Springer (2014)
28. Response, S.I.: Dragonfly: cyber espionage attacks against energy suppliers (2014)
29. Wilkinson, C., Eriksen, C., Penman, T.: Into the firing line: civilian ingress during the 2013 "red October" bushfires. Aust. Nat. Hazards **80**(1), 521–538 (2016)
30. Zhioua, S.: The middle east under malware attack dissecting cyber weapons. In: 2013 IEEE 33rd International Conference on Distributed Computing Systems Workshops, pp. 11–16. IEEE (2013)
31. Kubitschko, S.: Hackers' media practices: demonstrating and articulating expertise as interlocking arrangements. Convergence **21**(3), 388–402 (2015)
32. FIREEYE: Apt28: at the center of the storm (2017)
33. FIREEYE: Cyber espionage is alive and well: apt32 and the threat to global corporations (2017)
34. Broadcom: Sowbug: cyber espionage group targets South American and Southeast Asian governments (2017)
35. SECURELIST: The slingshot apt faq (2018)
36. FIREEYE: Apt39: an Iranian cyber espionage group focused on personal information (2019)
37. FIREEYE: Double dragon apt41, a dual espionage and cyber crime operation (2019)
38. Li, F., Lai, A., Ddl, D.: Evidence of advanced persistent threat: a case study of malware for political espionage. In: 6th International Conference on Malicious and Unwanted Software (MALWARE), pp. 102–109 (2011)

Chapter 2
Portuguese Concerns and Impact on Behaviour About Cybersecurity: A Comparison with the European Average

João Vidal Carvalho and Avelino Victor

Abstract The advancement of the Internet has great potential for the well-being of citizens and business growth, but this new paradigm also entails cybersecurity challenges that can have high economic impacts. The growth of Internet use is also leading to a general increase in cybercrime concerns as well as the number of users' victims of this permanent threat. This reality is also very present in Portugal as well as in other European countries. In this context, it is important to know some indicators associated with cybersecurity, to take the best measures/actions in a reasoned way, and to combat this phenomenon. This article presents the results of a study carried out in 2019 by the European Commission, whose analysis helps to understand the Portuguese positioning in the concerns and attitudes about cybercrime, to the average of the European Community citizens. Analysing this study, it was possible to perceive that the Portuguese's concerns about cybercrime are in line with the average of the European citizens, although the percentage of Portuguese that takes attitudes and actions to combat cyber-threats is a little bit above the average recorded by citizens of European countries.

2.1 Introduction

The increasing use of a growing variety of devices that can access the Internet has contributed to the overall growth of Internet use. The online universe has grown dramatically in recent years. This phenomenon enhances the quality of life of an individual through the ability to access from any place and at any time the essential

J. V. Carvalho (✉)
Politécnico Do Porto, ISCAP, CEOS.PP, S. Mamede de Infesta, Portugal
e-mail: cajvidal@iscap.ipp.pt

A. Victor
Instituto Universitário da Maia, Instituto Politécnico da Maia, Maia, Portugal
e-mail: javemor@ismai.pt

Á. Rocha et al. (eds.), *Developments and Advances in Defense and Security*,
Smart Innovation, Systems and Technologies 255,
https://doi.org/10.1007/978-981-16-4884-7_2

information in services such as electronic administration, electronic health, education, leisure, and shopping. However, the consequent opening of databases and information systems of public administration and other business entities inevitably leads to the possibility of such openness being exploited by malicious organized individuals or groups [1]. The advancement of information systems and technologies (IST) and digital economy has great potential for the well-being of citizens and business growth, but this new paradigm also entails cybersecurity challenges that can have high economic impacts.

Simultaneously with the growth of Internet users in recent years, there has been an exponential increase in the use of social networks. Of all users who access the Internet, around 80% of them use some social network. In this context, there is an intensification in citizens' concerns in most of the different types of threats associated with cybersecurity [2], and consequently, concerns have increased on the part of the leaders of the member states of the European Union.

Cybersecurity has been on the agenda of top leaders of States and organization managers for some time. The changes resulting from a pandemic situation of a great increase in remote work created new opportunities for hackers and catapulted cybersecurity to the top of the agendas of state leaders. On the one hand, the weaknesses of the cyber universe have increased, because people who work remotely are not prepared to take care of the security of their computer and the new work environment. This combined with a set of significant and rapid changes that companies had to make in their IST environment to accommodate employees who started to work remotely. This pandemic has enabled cyber-threats to increase like never before, taking advantage of these changes to enter companies' computers, systems, and IST environments [3]. These factors have led to an increase in the number and visibility of cyber-attacks and have made cybersecurity an even more important topic for citizens and leaders.

The European Union is leading the effort to regulate defence against cyber-threats in both legal and strategic areas. Moreover, governments invest a lot of money to train technicians to defend systems against cyber-attacks [4] or to empower them in the case of an eventual cyberwar [5]. Through this effort, the European Commission sought to create legislation to criminalize such crimes, increase cybersecurity capacity, and promote the exchange of information between countries [1, 6]. As part of the European Community, Portugal is highly involved in this European strategy. In this sense, also in Portugal, there is a growing concern about cybersecurity, both at the state and at the citizen level. Nevertheless, it is important to understand how the Portuguese citizens face this new paradigm and specially to understand how far they are compared to other Europeans. This comparison is made at the level of concerns about cybersecurity as well as the behaviour they have to deal with this phenomenon. The analysis of this comparison will allow Portugal to position itself against the other European countries in this sensitive and important area for today's citizens and businesses. In sum, the study presented here analyses the Portuguese concerns and impact on behaviour about cybersecurity.

In this article, we will initially present the description of a study about cybersecurity carried out in Europe in 2019. In the next section, the citizens' concerns about cybersecurity will be compared between the Portuguese and the European average. Subsequently, the behaviour and attitudes of the Portuguese will be compared with other European citizens regarding measures to mitigate these cyber-threats. Finally, we will present the discussion about the results of the study, to identify measures that have mitigated this phenomenon.

2.2 Cybersecurity Study in Europe

The Special Eurobarometer series on cybersecurity is the most important resource for learning about cybercrime in Europe [7]. The importance of this resource stems from the treatment and analysis of representative data of different types of cybercrimes collected in the last seven years of the 28 member states of the European Community. The most recent report covers a wide range of threats and aims to understand European citizens' experiences and perceptions of cybersecurity issues. That is the survey adopted in this report analyses the nature and frequency of Internet use by citizens; their awareness and experience of cybercrime; and the level of concern they feel about this type of crime. In this paper, we analyse only the perceptions of Internet users to cybersecurity, whether they have experienced or been a victim of cybercrime, and the level of concern they feel about it.

This survey adopted in this report was carried out between the 8th and the 22nd October 2019, by TNS opinion and social,[1] carried out the wave 87.4 of the Eurobarometer survey, on request of the European Commission. The wave 87.4 covers the population of the respective nationalities of the European Union Member States, resident in each of the 28 member states and aged 15 years and over. In total, 27,607 respondents (1007 from Portugal) from different social and demographic groups were interviewed face-to-face at home in their mother tongue on behalf of the Directorate-General for Home Affairs. The methodology used is that of Eurobarometer surveys as carried out by the Directorate-General for Communication ("Strategic Communication" Unit).[2]

The findings from this survey update previous surveys that were carried out in 2013 [8], 2015 [9], 2017 [7], and 2018 [10]. The 2019 survey [11] repeats most of the questions asked in 2015 to provide insight into the evolution of knowledge, behaviour, and attitudes towards cybersecurity in the European Union.

The study presented in this paper focuses on respondents' concerns about various aspects of online security. It also discusses changes respondents have made to their behaviour as a result of concerns about security and privacy.

[1] TNS opinion & social is a consortium created between TNS political and social, TNS UK and TNS opinion.

[2] http://ec.europa.eu/public_opinion/index_en.htm.