Advanced Research on Information Systems Security, an International Journal

Hackers Cybercrime - Computer security: Ethical Hacking - Learn the attack for better defence

Roberto Arnone [a]*

[a]*IPCA – Polytechnic Institute of Cávado and Ave, Barcelos, 4750, Portugal*

[a]*Email: a17653@alunos.ipca.pt*

Abstract

Today cybercrime is at a record high, costing businesses and individuals billions of dollars every year. What is even more frightening is that this figure represents just the last five years with no hope of it ever ending. The evolution of technology and the increasing accessibility of smart technologies means that there are many access points to users' homes to exploit. Cybercrime is on the rise in the world of technology today. Criminals using the technologies of the World Wide Web exploit the personal information of Internet users to their advantage. They happily use the dark web to buy and sell illegal products and services. They even manage to gain access to classified government information. While law enforcement tries to address the growing problem, the number of criminals continues to grow, taking advantage of the anonymity of the Internet.

Keywords: Cybercrime; hackers; Internet; information; computer technology.

* Corresponding author.

1. Introduction

In the old days, the teams of OPC and PTC had to rely in fingerprints, eyewitnesses and occasionally in the need of the guilty to confess the crime. However, nowadays, forensic science has made an extraordinary progress in this area, with new technologies. If we record a big step in new scientific technologies in the forensic area, the identification of people has become very important for many years. The history of justice has been avid of new scientific discoveries, in order to allow the progression of research and criminal investigation. The multiple scientific areas like legal medicine, ballistics, toxicology, entomology, biology, and chemistry, have been helping in the scientific and technical police area, the deepest part of investigation [1]. At the same time, new ways of crime appear which forces PTC to update their tools to fight crime. What crime? Cybercrime. What is cybercrime? Cybercrime is defined as a crime when a computer is the object of the same crime or, when it's used as a tool to commit an offense. A cybercriminal can use a device to have access to the personal data of a user, confidential commercial information, government information, or to disable a device, sell information is also called a cybercrime. Cybercrime has created a huge threat to the internet users, with millions of information stollen from the same users in the last years. It has had a huge impact in the economy of multiple countries. The President of IBM Ginny Rometty has described cybercrime as the ''biggest threat to every profession, every industry and business in the world''. Some shocking statistics related to cybercrime determine a global cost of 6 billion dollars. The purpose of this paper reflects the distinction of several cybercrimes, using some technological tools for hacking that will be exemplified. Then, carry out a media analysis to approximate the means and methods used to be able to confront.

2. Cybercrime categories

Cybercrime can be spitted in two categories:

- Crime aimed at networks or devices virus; Malware; DDOS attacks.
- Crimes that use devices: Phishing; E-mails; Cyberstalking or cyberbullying; Identity theft.

Cybercriminal inserts in three big categories: Individual cybercrimes, asset cybercrime, and government cybercrime. The types of methods used, and the levels of difficulty vary by category asset: Wren a criminal, illegally, has banking information or credit card of a person. The hacker steals the banking data to have access to funds, to make online purchases or to run phishing schemes to incite people to share their information. They can also use malicious software to have access to a Web page containing confidential information. - Individual: This category involves a person that distributes illegal or malicious information, online. It can be related to cyberbullying, distribution, pornography, and traffic [2]. The Government: It's the least common cybercrime, but it is the most serious one. A crime against the government is also known as cyber terrorism. Government cybercrimes includes the piracy of governmental websites, military websites, or advertising broadcast. These criminals are often terrorists or other countries government enemies [3].

3. Brief history

The malicious link with hackers has been documented for the first time in the 70's, when the first computer phone became the target. The technology experts known as ''phreakers'' found a way to pay the long-distance calls through a series of codes. They were the first hackers, learning how to operate the system, modifying the hardware and software to steal long distance phone time. This made people realize that the computer systems are vulnerable to criminal activities and that the more complex the systems are the more exposed they're to cybercrimes. Later in the 90's, when a huge project called ''Operation Sundevil'' was exposed. The FBI agents confiscated 42 computers and over 20 thousand floppy disks used by criminals to cover the usage of illegal credit cards and phone services. This operation involved over 100 FBI agents, and it took 2 years to locate some suspects. However, this was seen as a great effort as it showed the hackers that they were being watched and sued. The Electronic Frontier Foundation was created to face the threats to the civil freedom when the law enforcement makes a mistake or gets involved in unnecessary activities to investigate a cybercrime. Its mission was to protect and defend the consumers against illegal processes. Although useful, it also opened doors to escape from hackers and anonymous browsing, where numerous criminals practice their illegal services. Crime and cyber criminality became a bigger problem in our society, even with the current criminal justice system. In both public web space and the Dark web, cybercriminals are highly skilled and hard to find.

3.1 Typology of cybercriminal attacks:

- Money transfer fraud- Low risk, low cost but highly profitable, the fake money transfer fraud remains the main threat, with companies having huge losses.
- Phishing: The cybercriminals explore the massive use of global communication to obtain access to information about any other subject to trick the victims (ex.: COVID-19).
- Ransomware: These cybercrimes aim companies, industries, hospitals, medical centres, and public institutions. Nowadays, ransomware is growing significantly, because the cyber criminals believe that in times of crisis, in many countries, their chances increase.
- The interception of e-commerce data- is a consequent and imminent threat to online shoppers, undermining trust in internet payment systems.
- Criminal computer software- As a service, they allow a greater number of offenders, even if they do not have computer skills, to have the tools and services used by cybercriminals, so that everyone can become a cybercriminal with a minimum of ''investment''.
- Cyber Frauds- With the increase of internet transactions, and development of telework, the cyber criminals adapted their online scamming and phishing activities to the point of posing as representatives of law enforcement agencies, government and health officials or others to incite and trick their victims into disclosing personal information.

The ''Malwares''- Still relevant to the cyber criminals since cryptocurrencies are going up in value [4]

4. Cryptocurrency and modus operandi

Cyber-attack involving cryptocurrencies have become more recurrent during the Covid-19 pandemic, necessitating careful attention and particular collaboration from cybersecurity companies, governments, and society in 2021. The first step is to understand the modus operandi of this type of aggression, to know how to prevent and defend. Note that the problem occurs on a global scale, and they have the tendency to increase more and more. The most used modus operandi of events involving cryptocurrency are:

- Phishing
- Fake profiles.
- Fake apps.
- Use of malware.
- Data theft
- Phishing, the chosen form:

The most common form is still phishing, an attack in which the criminal sends an e-mail, SMS or a social media message containing a malicious link that, once clicked, takes the victim to a fake website. Thus, all encryption transactions that this person performs on the site will be sent to the criminal´s wallet.

5. Fake profiles

This modality that has become quite common is the spoofing of profiles on social networks, posing as important people in the world of crypto-currency trading. These profiles offer fake opportunities, for example, if the victim deposits a certain amount in crypto currencies into the wallet of the supposed trader, they will receive the doubled amount in certain days. The person making the deposit will, of course, never receive the amount and will still have lost the deposited amount.

6. Fake Apps

One can also find, fake applications for mobile devices, which link into the other applications. However, when the victim installs one of them on his device, all trades made through the fake app will be diverted to the criminal responsible. Sometimes, even an app with all the requirements for legitimacy is used to divert funds. In March, an app found in the Apple Store, which is supposed to be used to top up the balance of Bitcoin accounts on the devices of the company Trezor, was used to divert more than 600,00$ from official stores, or from the application provider's own websites.

7. The Malware

The most sophisticated attacks involve the use of malware to carry out the theft of cryptos. These malwares are developed exclusively for this purpose. They can act in forms of dedication: they can replace legitimate pages accessed by the victim with fake versions controlled by the user: they can exchange transaction addresses copied

from any page to the clipboard with addresses defined by the criminals; they can steal the victims' access key to crypto-currency wallets; they can even hijack computer resources from the victim's system to extract crypto-currencies, but without the victims' knowledge [5].

8. What is a hacker?

Computer security, an important field in our time, is still too often left aside by companies or individuals until the day they realize that their systems have been visited by a hacker, that their confidential data (logins, passwords, banking information, payrolls,…) have been stolen or copied, that they were being spied on, (…) Hackers are not just those Web criminals, as portrayed in the media, who spend their days hacking into systems and software in order to sink companies or ruin the economy. Certainly, some hackers like to destroy and steal confidential data for the purpose of a challenge, for money or for pleasure. But not all hackers are like this.

9. The sociological profile of hackers

The hacker is the subject of many images that affect how he is perceived in society. You need to draw a sociological and ethnographic portrait of the hacker in order to understand his motivations when engaging in hacking. Although hackers seem to be essentially ''tinkerers'' driven by the desire to manufacture and implement computer projects, they also seem to have a common desire to share to computer scientists. The discourses of hackers, from a cybernetic inspiration reveal themselves to animate a myth of information for all participating more broadly in a utopia of communication. Indeed, they lead some actors to emphasize a ''glorious age of the digital'' in discourses that are both fantastical and revolutionary [6] Therefore as the individuals we are going to analyse are hackers, it is necessary to define what we mean by this term, borrowed from a strong imaginary of hacking. If several definitions exist that do not reveal the same characteristics of the hacker, we will remember, the one that comes from canonical text such as ''The Jargon File'', ''The New Hacker Dictionary'', ''The Cathedral and the Bazaar'' and the General Public License (GPL). These texts have created a common sense about the individual, as well as the collective, identity of hacker culture and the responsibilities involved when one becomes one. Originally, according to the New Hacker Dictionary [7], the term ''someone who makes furniture with an axe'', but also, Hack translates as ''tampering''. In short, a hacker is an expert or an enthusiast of all kinds. He can be both an astronomy hacker and a computer hacker.

If we look at digital technologies, we can think of this as a person who likes to explore the details of programmable systems, as opposed to most users who, prefer to learn only the bare minimum; who programs with enthusiasm (even obsessively) or who loves programming rather than simply theorizing about it; a person who can appreciate the value of hacking; a person who can program well; who enjoys the intellectual challenge of overcoming circumventing computer limitations in creative ways. Therefore, the hacker is not considered a ''password hacker'' or a ''network hacker''. The correct term for these people would be ''Cracker2' [8]. The ''cracker'', on the other hand, is the one who exploits the activities of systems and information about technology to commit crimes. He is the malicious hacker. According to Lloyd Blankenship:[9]'We exploit… and you call us criminals. We seek knowledge… and you call us criminals (…). Yes, I am a criminal. My crime is curiosity''.

10. Hacker Delineations

First, there are the ‘’newbies’’: these are usually teenagers who were fascinated by the achievements of some hacker and started to learn everything they could in the computer field. The intermediaries, former ‘’newbies’’ who have acquired a sum of knowledge in computer security, programming, and networking. The ‘’White Hat Hackers’’, hacking elites who program all day and only look for flaws in systems, software… Other profiles of hackers who work on the ‘’dark side’’ of hacking. They prefer to take advantage of flaws and exploit them for fun and/or money. The ‘’Blades’’, individuals of unimaginable nullity, who use only ready-made programs (especially software used for nuclear bombs, mail bombing…) and who never stop boasting of being the best hackers in the world, of having penetrated systems such as those of NASA, of governments (…) are found mostly on IRC and ICQ. The ‘’Black Hat Hackers’’, elites that rather destroy any system that fell in their hands [10].

11. Other profiles that we do not classify as the other hackers

The ‘’phreakers’’: These are the people who infiltrate telephone systems. With their knowledge of switched telephone networks and electronics, they can build electronic systems (called ‘’Box’’) with well-defined functions such as the possibility of calling the other side of the world without disbursing money, of calling a company account… The ‘’Crackers’’: these are people who hack into paid software so that they can use it indefinitely without spending any money. These are important elements, because there are also people who link to find flaws in computer programs. The ‘’Hacktivists’’: these are the hackers that use their knowledge to defend what they think about and fight for a goal (Human Rights, non-commercialization of the internet…).

11.1 The world’s best-known hackers

John Draper as known as ‘’Captain Crunch’’. John Draper is considered the pioneer of hackers. Son of a US Air Force Engineer, he discovered in 1969 that a whistle, recovered from Cap’N Crunch cereal boxes, allows to obtain the specific tone of 2600 hertz. The same one that was used in AT&T to activate long-distance lines. By whistling into the handset Draper- who earned the nickname ‘’Captain Crunch’’- can make free phone calls. He named his technique: ‘’phreaking’’, a contraction of ‘’telephone’’ and ‘’freak’’. He will build the ‘’Blue Box’’, a device capable of reproducing this tone, and inspire the first computer hackers [11].

Kevin Mitnick as known as ‘’Le condor’’ is, without a doubt, the most well-known hacker in the world. In 1980, 17 years of age, he physically breaks into the Pacific Bell telephone exchange and hijacks the phone lines for personal use. He served three months in a reformatory. In 1983, from the University of Southern California, he remotely accessed a Pentagon computer via Arpanet, the forerunner of the Internet. That will get him back in a juvenile detention centre for six months. Other exploits will follow, including access to Fujitsu, Motorola, Nokia, or Sun Microsystems’ systems. On the run from 1989 to 1995, he was finally arrested by the FBI and sentenced to 5 years in prison. Kevin Mitnick is now a computer security consultant.

Gary McKinnon as known as ‘’Solo’’ is a British hacker. Convinced that the US Army uses extra-terrestrial technology, he began searching for evidence, hacking into 97 computers from NASA, Air Force, and the Pentagon, between 2001 and 2002. His multiple intrusions constitute the ‘’the largest military hack of all time’’, according

to U.S officials. McKinnon allegedly locked or damaged systems, causing $700,000 in damage. He is defending himself today against extradition proceedings to the United States where he risks 70 years in prison.

Kevin Poulsen as known as ‘’Dark Dante’’… 17 years ago he began his hacking career, performing several intrusions into the Arpanet network. This ancestor of the internet was usually reserved for the army, corporations, and large universities. Other exploits follow, including and intrusion into the Army MASNET network. In 1989, he was arrested, but escaped shortly before appearing before the judge. During his 17 months on the run, he will accomplish his greatest feat. Poulsen takes control of all the telephone lines at KIIS-FM radio to make sure he wins the first prize in a contest organized for listeners: a Porsche. Arrested in 1991, he serves 51 months (4 years) in prison. Today he is the editor of Wired magazine.

Vladimir Levin known as ‘’Vlad’’… This Russian mathematician is famous for having carried out the greatest ‘’virtual’’ theft. In 1994, he broke into the SWIFT International banking network and accessed several large accounts of the American Bank ‘’Citibank’’. Levin electronically diverts more than $10 million, which he transfers to accounts in the United States, Israel, Finland, Germany, and the Netherlands. Three accomplices were supposed to physically recover the stolen money. But they will all be arrested during their attempts to withdraw the stolen money. The investigation goes back to Levin, who was arrested in London in 1995. Extradited to the United States, he was sentenced to three years in prison in 1998.

Julian Assange is the co-founder and editor-in-chief of Wikileaks (see article on Hacktivists). Previously, the Australian hacktivist was known as "Mendax" at International Subversives. He is the inspiration behind the operational rules of this group of hackers: prohibition to damage the visited computers, prohibition to modify the data hosted on those systems, and mandatory sharing of the information that was gathered. This does not prevent him from being arrested in 1992 by the Australian courts for 31 acts of hacking. These include intrusions into the USAD's network and in the telecommunications operator Nortel. Assange receives a symbolic fine of 2100 dollars and is released for good behaviour [12]. Often, most hackers are from an age group of under 30. The so-called vulnerability hunters are generally young- more than two thirds are between the ages of 18 and 29, according to OPC estimates.

While these characteristics are common to hackers driven by the pursuit of celebrity and those driven by profit, some evidence suggests that a disproportional number of profit-motivated hackers are older- Some teenage hackers become criminals, other heroes. During the summer, many students are forced to work in their summer vacations, so they can finance themselves. Before that, small jobs were the ideal solution to receive a small income while spending some time away from parents and home. Now, there is another option, albeit controversial, hacking. From finding "bugs" to help companies, to innovating new solutions for hacking into servers.

"In Australia, a judge congratulated and punished a 17-year-old who had managed to hack Apple's system twice, the first time in just 13 years. A $500 bond and exemplary conduct for nine months. It was the sentence given by the magistrate David White, specifying: "He is evidently a computer genius, but that doesn't give him the right to abuse his talents. The young man stated in court that he had done computer hacking in the hope of finding a job. It didn't work..."[13].

Santiago Lopez, a 19-year-old from Argentina, had better luck. He was the first to receive more than a million dollars on the Hacker One Bounty Bug platform (a platform that rewards the discovery of security flaws in the computers systems of the participating companies). Hacker One claims to have detected about 1,800 bugs through hacking. “These have made it possible to strengthen the security of the companies involved” [14].

"Marcus Hutchins, a young British Hacker who put an end to "WannaCry", a ransomware that in 2017 took revenge on the systems of some hospitals and other companies around the world. A few months later, Hutchins spoke out about it again after he was arrested for hacking during his teenage years. Hutchins has pleaded guilty and is awaiting sentencing [15].

In this context, we are looking at contemporary hackers, not those of the 60s or 70s. However, we hypothesize that these hackers, or so-called "web pioneers," have largely influenced the mindset of contemporary hacker groups and free software communities. In this analysis of the behaviours of hackers today, they show that they form a social group (a set of people with common characteristics or goals), in which a strong moral is established through various types of discourse: partisan texts or those that are the result of a more collaborative work. The OPC in the investigations position with reservation, given the diversity of hackers that exist today. In fact, the ethos of hackers has not stopped subtly changing, in a constant interaction with the evolution of practices, techniques, and general representations of the social world. Contemporary hackers are not the hackers of the 1970s. Although, the journalist Steven Levy [16], tried to liberate the "fundamentals" in the early 1980s by condensing the hacker ethos into six major principles. It is difficult to claim that these principles are the same for today's hackers, although if hackers are computer lovers, they are first and foremost hackers invested in an illicit culture. Of course, generalizations of this type are open to criticism and the reality is more complex. In fact, we need to know if the many differences between hackers are more significant than the few principles they have in common. In short, the gender, age, level of education, profession, nationality, and housing. Very quickly, we see that these criteria are radically different from one hacker to another. It seems, at first glance, that there is no single "type" of hacker, but rather a multiplicity [17].

12. Penal Framework

The violation of a series of computer databases of an organization, institution, or individuals indicates illicit conduct. After the investigation that proves the crime of computer violation, hackers who disclose the modus operandi and any documents that reveal illicit activities of organizations, or organized criminal groups, do not exonerate their conviction for the illicit act, even if we consider the information of interest to the OPC.

In Portugal, there is no "whistle-blower" status. The promotion of evidence disclosed to them may even be considered null and void. In Portugal there is no specific legislation on the protection of "whistle-blowers", but there are defined instruments of European Law that provide for the creation of "whistleblowing" channels through which individuals who undertake tasks in a particular organization can report with defined guarantees of anonymity and prohibition of reprisal. According to the European Parliament, with the integration of the Internet into our daily lives, Internet users have become vulnerable to criminals who often operate from other continents. Considering the rapid increase in cybercrime, in 2007, the European Commission prepared the ground for a

comprehensive policy to combat it [18].

“Having in the meantime of Directive 2013/40/EU of the European Parliament and the Council of 12 August 2013 on attacks on information systems and replacing Council Framework Decision 2005/222/JAI ... Stresses that the significant increase in cases of ransomware, botnets and unauthorized interference in computer systems has an impact on the security of individuals, the availability and integrity of their personal data, as well as the protection of privacy and fundamental freedoms and the integrity of critical infrastructure, including but not limited to the supply of energy and electricity and financial structures, such as the stock exchange; recalls, in this context, that the fight against cybercrime is a recognized priority under the European Agenda for Security of 28 April 2015(…)”[19].

13. How to fight cybercrime

Before we get to the heart of the matter, we need to know how hacking a system works. If the word "hacking" can be scary or annoying, remember that before you can secure a system, you always must do penetration tests (called Pen-Test) to target the flaws. In addition, to effectively thwart a person, one must think like them or know their limitations: this applies to hackers as well, and knowledge of their limitations through knowledge of hacking techniques. Basically, to protect a system, you must put yourself in a hacker's shoes. The logical sequence of an attack starts by searching for information about the system, targeting both public sources and the system itself. And then we must try to get in without anyone noticing. Once we get to this point, we must try to find information that will allow us to obtain administrator rights. Additionally, we will need to install backdoors (programs that will allow us to easily get back into the target system). Finally, we must hide and delete these facts and gestures in the system. It seems that in the modern age of technology, hackers are taking over our systems and no one is safe.

The average wait time, or the time it takes a company to detect a cyber breach, is over 200 days. Most Internet users don't think about the fact that they may have been hacked and many rarely change their credentials or passwords. This leaves many people vulnerable to cybercrime and it is important to be informed. Today, many hackers are hired by large companies to test their computer security devices.

14. Tools used

In just a few years, Kali Linux has become a very popular tool for penetration testing. The goal of Kali Linux is to provide a distribution that brings together all the tools needed for security testing of an information system, including penetration testing. What does the name mean? This tool was born in 2006 as Backtrack Linux, but after a major redesign in 2013, it was given the name Kali. Based on Debian Testing, Kali includes over 300 security tools, including the big ones like Metasploit, Nmap and Air crack-ng, but also a wide variety of more obscure and specialized tools. Maintained and managed by cybersecurity experts, Kali Linux is optimized for penetration testing. But beyond the legal framework, hackers don't care about this framework, so Kali Linux can be considered as a weapon for the network, which, according to those who use it, can mean financial cost [20], [23]. Kali is a specialized Linux distribution for experienced Linux users who need an offensive and secure penetration testing

platform. It is essential to be familiar with Linux in general, to have at least a basic level of competence in administering a system. Kali is the right choice for most offensive security tasks. Advanced users may have an opinion about which alternatives to Kali they prefer, but newcomers to the field of intrusion testing should familiarize themselves with Kali before considering other options [20], [24].

15. Conclusion

While computer hackers are a source of great security concern for individuals, businesses, and public agencies around the world, hacking and the informal hacking culture remains largely a black box for lawmakers and potential hacking victims. The mystery that largely surrounds hacking prevents us from finding effective solutions to the security problems it poses. Our analysis does, however, at least provide hypotheses as to ways to manage this problem. Analysing computer hacking considering economics reveals several propositions. First, it is important to recognize that there are different types of hackers, characterized by diverse motivations. For this reason, the effective method for reducing the risk posed by hackers in general will consist in adapting legislation to target the different categories of hackers differently.

Referring to the theory of deviant behaviour, we determine the causes that explain the nonconformity of hacker behaviour, as well as the social reaction to their conduct. According to the criteria defined by Becker when he analyses jazz musicians, hackers are deviant individuals [21], [25]. Knowing that a person is considered depraved when he transgresses a norm, this implies the existence of a norm that prohibits it and therefore a moral entrepreneur.

In this analysis we have not done more than touch on the numerous and complex issues concerning hacking. We have not given due attention to the good pirates who are motivated neither by fame nor by profit, but who voluntarily alert security system flaws to managers of vulnerable computer systems, [26].

While the activities of these hacks are equally illicit, they probably play an important role in preventing malicious hacker attacks.

16. References

[1] A. Pereira, CSI Criminal. Edições Universidade Fernando Pessoa, 2008.

[2] Tribunal Regional Federal da 3a Região, Investigação e prova nos crimes cibernéticos, Escola de Magistrados Brasil, Carderno de estudo, 2017. Acedido: Jul. 03, 2021. [Online]. Available: www.trf.jus.br/emag

[3] Tribunal Regional Federal da 3a Região, «Investigação e prova nos crimes cibernéticos», Escola de Magistrados Brasil, Carderno de estudo, 2017. Acedido: Jul. 03, 2021. [Online]. Available: www.trf3.jus.br/emag

[4] INTERPOL, Les cyberattaques ne connaissent pas de frontières et évoluent rapidement. 2021. Accessed: Jul. 03, 2021. [Online]. Available: https://www.interpol.int/fr/Infractions/Cybercriminalite/

[5] INTERPOL, Un rapport d'INTERPOL dresse la liste des principales cybermenaces en Asie du Sud-Est. 2021. Accessed: Jul. 03, 2021. [Online]. Available: https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2021/Un-rapport-d-INTERPOL-dresse-la-liste-des-principales-cybermenaces-en-Asie-du-Sud

[6] F. Schobert, F Les hackers ou l'institution de mœurs dans le cyberespace, 2018.

[7] E. S. Raymond e G. L. Steele, The new hacker's dictionary. Mit Press, 1996.

[8] F. Schobert, Les hacker's ou l'institution de mœurs dans le cyberespace, 2018.

[9] L. Blankenship, The conscience of a hacker, Phrack, Volume One, (7). (cf. p 15), 1986.

[10] Polizia Giudiziaria, Rapporto - Indaga su un crimine doloso, 2002. Accessed: Jul. 03, 2021. [Online]. Available: http://www.carabinieri.it/editoria/rassegna-dell-arma/la-rassegna/anno-2002/n-1---gennaio-marzo/studi/la-polizia-giudiziaria-militare-nel-territorio-e-fuori-dal-territorio-dello-stato-problematiche.

[11] L. Simon, Six grandes figures du hacking». 2017. Accessed: Jul. 08, 2021. [Online Available: https://info.arte.tv/fr/six-grandes-figures-du-hacking

[12] L. Simon, «Six grandes figures du hacking». 2017. Accessed: Jan. 01, 2022. [Online]. Available: https://info.arte.tv/fr/six-grandes-figures-du-hacking

[13] R. Opie, Adelaide teen hacked into Apple twice hoping the tech giant would offer him a job, Posted Mon 27 May 2019 at 5:23am. Accessed: Jul. 10, 2021. [Online]. Available: https://www.abc.net.au/news/2019-05-27/adelaide-teenager-hacked-into-apple-twice-in-two-years/11152492

[14] M. Kan, 19-Year-Old Makes Over $1 Million Hunting Software Bugs, March 1, 2019. Accessed: Jul. 10, 2021. [Online]. Available: https://www.pcmag.com/news/19-year-old-makes-over-1-million-hunting-software-bugs

[15] B. Krebs, "MalwareTech" Hutchins Pleads Guilty to Writing, Selling Banking Malware, this entry was posted on Friday 19th of April 2019 05:58 PM, 2019. Accessed: Jul. 10, 2021. [Online]. Available: https://krebsonsecurity.com/2019/04/marcus-malwaretech-hutchins-pleads-guilty-to-writing-selling-banking-malware/

[16] S. Levy, L'éthique des hackers. Ecole des Loisirs, 2013.

[17] P. T. Leeson and C. J. Coyne, Une analyse économique du piratage informatique, Tracés. Revue de Sciences humaines, n. 26, pp. 203–231, 2014, doi: https://doi.org/10.4000/traces.5957.

[18] União Europeia - Rumo a uma política geral de luta contra o cibercrime. Accessed: Jul. 08, 2021. [Online]. Available: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM%3Al14560

[19] Luta contra a cibercriminalidade. Acedido: Jul. 07, 2021. [Online]. Available: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52017IP0366&from=EN

[20] R. Nastase, Introduzione all'Hacking: Imparare le basi di Kali Linux e Hacking, Italian Edition Nicolae Afrasinei (Translator) Format: Kindle Edition. 2018.

[21] H. Becker, Outsiders. Etude de Sociologie de la Déviance, Paris, Editions Métailié. Paris, Editions Métailié, 1985.

[23] N. M. Coelho, M. Peixoto and M. M. Cruz-Cunha, "Prototype of a paranoid mobile operating system distribution," 2019 7th International Symposium on Digital Forensics and Security (ISDFS), 2019, pp. 1-6, doi: 10.1109/ISDFS.2019.8757551.

[24] N. Coelho, B. Fonseca, and A. Castro, "Paranoid operative system methodology for Anonymous & Secure Web Browsing, doctoral project," Atas da 17ª Conferência da Associação Portuguesa de Sistemas de Informação, 2017, doi: 10.18803/capsi.v17.127-143.

[25] N. R. Mateus-Coelho, B. R. Fonseca, and A. V. Castro, "POSMASWEB: Paranoid Operating System Methodology for Anonymous and Secure Web Browsing," Handbook of Research on Cyber Crime and Information Privacy, pp. 466–497, 2021, doi: 10.4018/978-1-7998-5728-0.ch023.

[25] N. Mateus-Coelho, M. M. Cruz-Cunha, and P. Silva-Ávila, "Application of the Industry 4.0 technologies to mobile learning and health education apps," FME Transactions, vol. 49, no. 4, pp. 876-885, 2021, doi: 10.5937/fme2104876M.