Cybersecurity and Cybercrimes in Portugal

Justino Silva

Lusofona University of Porto, Portugal
jdps96@gmail.com

Abstract. With the development of technologies, not everything that originated from them is good. This paper intends to share knowledge regarding cybersecurity, as well as cybercrimes. Basic security principles of cybersecurity, as well as types of cybercrime will be addressed. Most users are inexperienced and susceptible to cyber-attacks, so it is important to warn them to protect themselves to avoid being cybercrime victims. This paper also addresses the state of cybersecurity in Portugal, and one of the most recent cybercrimes that damaged the world.

Keywords: Cybercrimes, Cybersecurity, Cyber Threats, Cyber-attacks, WannaCry.

1 Introduction

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

Most people don't realize that the Internet isn't safe and use it daily in their devices like phones and computers, unaware of the dangers it has. The need for cybersecurity is increasing, because with the Internet of Things being developed, the drawback is that our everyday objects now feature an IP (Internet Protocol) address for Internet connectivity, which an intruder can access its control, stealing personal data or causing catastrophic damage. [2]

Computer crime can be summarized as a criminal activity which involves an unauthorized access, illegal interception, data interference, abusage of devices, forgery, blackmail, fraud, and others, to a system in order to steal confidential data or cause damage. Cybercrime can cause harm to any organization. As the use of technology is increasing day-by-day, the crime is also increasing gradually. [3]

In this paper, we start by defining the meaning of security, complementing with the basic security principles that define a secure system.

Next, we define what are cybercrimes, splitting them in different types, and show the most common types of cybercrime. In this chapter we also present a cybercrime that occurred in 2017, forcing all governments to invest in cybersecurity education and implementation.

After this chapter, we focus in Portugal specifically, showing some research results, that give us and idea of the state of cybersecurity in this country. The main reason of the creation of this paper was to inform about this last chapter referring to Portugal, in order to show that security is a very important topic that is often forgotten until it is too late, and the message should be shared with everyone, so people get the information that they are missing.

2 Cybersecurity and Cybercrimes

2.1 Cybersecurity

The author [4] defines cybersecurity as 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.

Implementing effective cybersecurity measures is particularly challenging nowadays because there are more devices than people, and attackers are becoming more innovative.

According to [5], there are four basic security principles:

- Access - Using physical and software controls to protect your hardware or data from intrusion.
    - For hardware, access limits usually mean physical access limits.
    - For software, access limits usually mean both physical and virtual means.
- Authentication - provides a means to identify a person or entity. Setting up all authentication features such as a password system in your platform operating systems to verify that users are who they say they are.
    - Authentication provides varying degrees of security through measures such as badges and passwords. For example, ensure that personnel use employee badges properly to enter a computer room.
- Authorization - defines what an authenticated user or entity can do. Use authorization to ensure company personnel can only work with hardware and software that they are trained and qualified to use.

  For example, set up a system of read/write/execute permissions to control user access to commands, disk space, devices, and applications.
- Accounting - Customer IT personnel can use software and hardware features to monitor login activity and maintain hardware inventories.
    - Use system logs to monitor user logins. Track system administrator and service accounts through system logs because these accounts can access powerful commands.

- Periodically retire or archive log files when they exceed a reasonable size, in accordance with the customer company policy. Log files can become very large over time, so it is essential to maintain them.
- Use component serial numbers to track system assets for inventory purposes. Oracle part numbers are electronically recorded on all cards, modules, and motherboards.

2.2 Cybercrimes

Cybercrime consists of a criminal act that is committed online by using electronic communications networks and information systems. It is a border less problem that can be classified in three broad definitions: [6]

- Crimes specific to the Internet, such as attacks against information systems or phishing (e.g. fake bank websites to solicit passwords enabling access to victims' bank accounts).
- Online fraud and forgery. Large-scale fraud can be committed online through instruments such as identity theft, phishing, spam and malicious code.
- Illegal online content, including child sexual abuse material, incitement to racial hatred, incitement to terrorist acts and glorification of violence, terrorism, racism and xenophobia.

The most common types of cybercrime are:

- Malware – Malware is malicious software that exploits a network´s vulnerability and accesses it in order to install something like spyware, ransomware, virus, worms. Once inside the system, this software can block access from the user(ransomware), obtain information(spyware), render the system inoperable [7]
- DDOS (Distributed Denial of Service) – A Denial of Service works by overwhelming an online service, in order to overload the system and make it shut down or reboot. A DDoS is a DoS on a larger scale, the attacker uses various IP addresses so there are less chances of the attack failing, and tracking the perpetrator is harder. [8]
- Botnets - Botnets are hacked networks where the computers connected to them are being remotely controlled by hackers. The hackers then use those computers to access the network's database or to perform crimes like a DDoS or steal data. [9]

- Phishing – phishing attacks work by either making the user click a fraudulent link that appears to be from an official source and it automatically installs malware, or the user deliberately types personal information on a fraudulent website. [10]

- Virus – a virus is a malware that infects a computer, and it's usually disguised as a creditable source. As a biological virus, it spreads itself on the computer and to other computers, causing hardware and software problems. [9]

- Ransomware – ransomware is a malicious software that can for example be planted on a fraudulent link or email, that once clicked infects the computer and encrypts parts of the data or even all of it, blocking the user from accessing it. The software then displays a pop-up message where it informs the victim that his machine is encrypted and asks for payment, usually in Bitcoin. Once the ransom is payed, ideally a decryption key is shown on the screen. [11]

- Sextortion – sextortion is blackmail using sexual information in return of sexual favours or money from the victim. Either the criminal contacts the victims using an online social network for adults, by assuming the identity of an attractive man or woman, or he hacks them, then proceeds to record and save nude pictures and videos from the victims, which then threatens to release online unless they either pay a ransom or appeal to the blackmailers demands. [12]

A cybercrime can happen to anyone, or anything, that is online. The two main reasons are either for money, where the hackers ask for a ransom, or just to destroy data or even the system itself.

According to [13], 53% of the cyber-attacks resulted in damages of 500,000 dollars or more. As referred in the same study, here's a graphic that shows the top 10 malicious file extensions in emails, in the year of 2017.

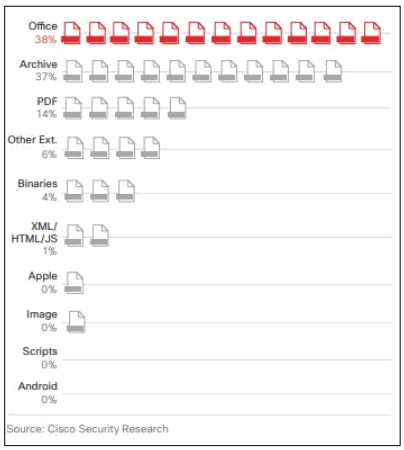

Fig. 1. Top 10 malicious file extensions [13]

- 38% refer to Office formats such as Word, PowerPoint or Excel
- 37% refer to Archive files, such as compresses files in .rar or .zip format
- 14% refer to PDF files

The user, when seeing these types of files on an email that looks legit, will open them without questioning because it looks official.

2.3 A recent and dangerous Cybercrime that failed

In 2017, the world was attacked with a ransomware named WannaCry. It was a worm that spread by exploiting vulnerabilities in the Microsoft's Windows Operating System, most precisely those that weren't up to date as of March 14, 2017, and once installed, encrypted files and demanded a payment in exchange of the decryption key. It had two primary components, a module for self-propagation and a ransom module to handle the extortion process. The ransom could be between 300 dollars and 600 dollars. Each file was encrypted using separate AES encryption key, and each key was separately encrypted using 2048-bit RSA encryption. [14]

The first ransomware ever appeared in 1989, the AIDS Trojan, it spread in floppy disks and to pay the ransom, people had to send 189$ to a post office in Panama. [15]

WannaCry resulted in over 200,000 organizations affected around the world, spread over 150 countries.

One of the most affected services was the National Health Service in the United Kingdom, infecting the computer system of 47 hospitals, forcing operations and doctor's appointments to be cancelled for a lot of patients. In the end, the hackers only managed to profit less than 70,000 dollars converted from bitcoin. [16, 17]

3 A focus in Portugal

As mentioned in [18], according to Microsoft, as of 2017, there was found malware in 8.3% of the analysed computers in Portugal, 7.0% of those were Trojans.

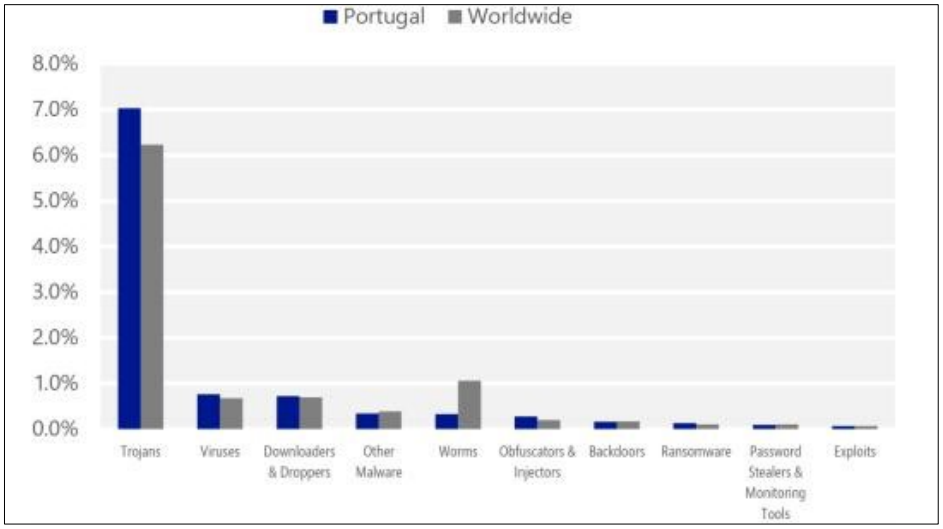

Fig. 2. Percentage of malware in the amount of analyzed Computers in Portugal as of March 2017 [18]

Source: Website Builder Expert (2017)

In the same document, we can see a study from Website Builder Expert, also in 2017, that shows the most vulnerable countries to Cyber Threats, and the countries with the greatest number of cybercrime victims.

EU COUNTRY	CYBERCRIME VULNERABILITY SCORE				
1. MALTA	42%	11. SLOVENIA	38%	21. SWEDEN	32%
2. GREECE	41%	12. CROATIA	37%	22. ITALY	31%
3. ROMANIA	41%	13. DENMARK	36%	23. FRANCE	31%
4. SLOVAKIA	40%	14. LATVIA	35%	24. UK	31%
5. SPAIN	40%	15. CZECH REP	35%	25. NETHERLANDS	30%
6. LITHUANIA	39%	16. POLAND	34%	26. GERMANY	30%
7. CYPRUS	39%	17. IRELAND	33%	27. ESTONIA	30%
8. PORTUGAL	39%	18. LUXEMBOURG	32%	28. FINLAND	29%
9. HUNGARY	39%	19. AUSTRIA	32%		
10. BULGARIA	38%	20. BELGIUM	32%		

Fig. 3. UE's countries in greatest danger to cybercrimes [18]

Source: Website Builder Expert

In the previous table, we can see that Portugal occupies the eight position on the most vulnerable countries to cybercrimes.

The same study also shows that on the top five countries with the most percentage of cybercrime victims, Portugal is on the third place.

	% 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. UE's countries with the most victims of cybercrimes [18]

Source: Website Builder Expert

Portugal's National Cybersecurity Centre was created in 2014, formally assuming the powers of national authority over cybersecurity subjects. It also deals with national management and coordination of response to cyber incidents, also ensuring international cooperation in this subject. [19]

The official website to CNCS informs the public about cyber threats, displaying alerts of vulnerability in compromised computer programs and smartphone apps. It also shows news about cyber conferences, or job vacancies in the area of cybersecurity, or even cybersecurity learning courses. There's also an option to notify the organization about a criminal cyber act suffered, but it should also be notified to the police.

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.

Cybersecurity can be a pretty rewarding job, with salaries reaching as high as 62,000€, as an IT Security Engineer in a bank for example. [20]

As of an ENISA study shown in [21], here's a table that represents the top 15 cyber threats in the last four years prior to 2018. The top three greatest threats occupy the same positions in every year, being them Malware, Web-based Attacks and Web application Attacks. This clearly shows that these are well built and are hard to cypher and fight.

	2014	2015	2016	2017
1	Malicious code: Worms / Trojans	Malware	Malware	Malware
2	Web-based attacks	Web based attacks	Web based attacks	Web based attacks
3	Web application / Injection attacks	Web application attacks	Web application attacks	Web application attacks
4	Botnets	Botnets	Denial of service	Phishing
5	Denial of service	Denial of service	Botnets	Spam
6	Spam	Physical damage / theft / loss	Phishing	Denial of servisse
7	Phishing	Insider threat accidental)	Spam	Ransomware
8	Exploit kits	Phishing	Ransomware	Botnets
9	Data breaches	Spam	Insider threat	Insider threat
10	Physical damage / theft / loss	Exploit kits	Physical manipulation / damage / theft / loss	Physical manipulation / damage / theft / loss
11	Insider threat	Data breaches	Exploit kits	Data breaches
12	Information leakage	Identity theft	Data breaches	Identity theft
13	Identity theft / fraud	Information leakage	Identity theft	Information leakage
14	Cyber espionage	Ransomware	Information leakage	Exploit kits
15	Ransomware / Rogueware / Scareware	Cyber espionage	Cyber espionage	Cyber espionage

Fig. 5. Greatest Cyber Threats in Portugal [21]

Conclusion

It is very easy to stay outdated in technologies, so it is very important we try to refine our knowledge every day in order to keep up with the times. Most times, systems get hacked only because they are outdated. Often businesses keep the same hardware and software unchanged for decades, thinking they are saving money instead of buying new equipment because the old works, but they end up paying even more when they get hacked, updating all the equipment, plus the security system and to recover lost data. Portuguese schools and hospitals or health centers, for example, are using outdated technology. Health facilities with outdated technology, are always at a higher risk of machine malfunctions, which puts human lives at risk, and schools that nowadays don't have functioning computers can't provide its students with means of learning computer sciences and other subjects alike.

People should start worrying a lot more about their safety online, mainly when they just type their personal data anywhere, and when they upload their photos online. It makes it easier for hackers to get the information they need about someone to hack them.

This paper was hard to conceive because cybersecurity is still a very recent term, and Portugal is only starting now to invest in it, so the information available is either scarce and in small detail, or it requires to be purchased. Still, I believe there's a lot to learn and uncover about cybersecurity. Maybe it's because most of cyber criminals are self-taught, and most of the information about this subject is hidden to the public because it would help the authorities to reverse engineer solutions to cybercrimes faster.

It is good news that Portugal is creating cybersecurity-oriented degrees and post High School technical courses, in order to create cybersecurity jobs and improve the country's national security. But, in order to take the next step, I believe that basic security should be taught in schools as early

as elementary school, because nowadays, kids begin using devices at a very young age, so it is fundamental that they should know how to stay protected online.

References

1. Conteh, N.; Royer, M.; "The Rise in Cybercrime and the Dynamics of Exploiting the Human Vulnerability Factor", International Journal of Computer, Volume 20, Number 1 (2016)
2. Bruijin, H.; Janssen, M.; "Building Cybersecurity awareness: The need for evidence-based framing strategies", Government Information Quarterly, January (2017)
3. Tiwari, S.; Bhalla, A.; Rawat, R.; "Cyber Crime and Security", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 4, April (2016)
4. "What is Cybersecurity", Cisco Security, Retrieved From: "https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html", Last Access: 10 December 2018.
5. "Basic Security Principles", Oracle Basic Security, Retrieved From: "https://docs.oracle.com/cd/E79568_01/html/E79571/glymd.html", Last Access: 10 December 2018.
6. "What is Cybercrime?", European Commission Migration and Home Affairs, Retrieved From: "https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-andhuman-trafficking/cybercrime_en", Last Access: 10 December 2018.
7. "What are the Most Common Cyberattacks?", Cisco Security, Retrieved From: "https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html", Last Access: 18 December 2018.
8. "Types of Cybercrime", Panda Security Mediacenter, Retrieved From: "https://www.pandasecurity.com/mediacenter/panda-security/types-of-cybercrime/", Last Access: 18 December 2018.
9. "Top 5 most prominent forms of cybercrime", CBR Online, Retrieved From: "https://www.cbronline.com/list/top-forms-cybercrime", Last Access: 18 December 2018.
10. "Common Online Threats and How to Protect Yourself", LastPass, Retrieved From: "https://blog.lastpass.com/2013/06/common-online-threats-and-how-to-protectyourself.html/", Last Access: 18 December 2018.
11. "Ransomware", Enisa Ransomware, Retrieved From: "https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/ransomware", Last Access: 18 December 2018.
12. "Online Safety", Interpol Cybercrime, Retrieved From: "https://www.interpol.int/en/Crime-areas/Cybercrime/Online-safety/Sextortion", Last Access: 18 December 2018.
13. "The attack landscape", Cisco Annual Report 2018, Retrieved From: "https://bit.ly/2sMN4Fi", Last Access: 18 December 2018.
14. "Ramson Wannacry", Symantec Security Center, Retrieved From: "https://www.symantec.com/security-center/writeup/2017-051310-3522-99", Last Access: 18 December 2018.
15. Mohurle, S.; Patil, M.; "A brief study of Wannacry Threat: Ransomware Attack 2017". International Journal of Advanced Research in Computer Science, Volume 8, No.5, May-June 2017, Department of Computer Science MITACSC, India, (2017).
16. "NHS cyberattack: Everything you need to know about 'biggest ransomware' offensive in history", The Telegraph News, Retrieved From: "https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-knowbiggest-ransomware-offensive/", Last Access: 20 December 2018
17. "What is WannaCry and how does ransomware work?", The Telegraph Technology Intelligence, Retrieved From: "https://www.telegraph.co.uk/technology/0/ransomware-doeswork/", Last Access: 20 December 2018.
18. Barros, G.; "A Cibersegurança em Portugal". Temas Económicos, Number 56, August 2018, Gabinete de Estratégia e Estudos, Ministério da Economia, Lisboa, Portugal, (2018).
19. "Centro Nacional de Cibersegurança", Fundação para a Ciência e a Tecnologia, Retrieved From: "https://www.fccn.pt/inteligent-transitions-in-ux-design/", Last Access: 20 December 2018.
20. "Security Salaries in Portugal", Glassdoor, Retrieved From: "https://www.glassdoor.com/Salaries/portugal-security-salarySRCH_IL.0,8_IN195_KO9,17_SDAS.htm", Last Access: 20 December 2018.
21. Barros, G.; "A Cibersegurança em Portugal". Temas Económicos, Number 54, August 2018, Gabinete de Estratégia e Estudos, Ministério da Economia, Lisboa, Portugal, (2018)