A Review on Cyber Attacks and Its Preventive Measures

Valdemar Sousa

Lusofona University of Porto, Portugal
valde_sousa@hotmail.com

Abstract. Today and on the current Internet, cyberattacks are a headache for all users of the World-wide network, businesses and digital security experts fight every day and try to find solutions so that data or information is not affected for these attacks. With this there is no "medicine" that solves all cyberattacks, but preventive measures that try to avoid major damage to those who suffer an attack. This paper focuses on summarizing a bit of what are cyberattacks and realizing better than they are capable, and also preventive measures that can ensure greater security for Internet users.

Keywords: CyberAttacks, Preventive, Measures, Internet, Crimeware, CyberPrevention, CyberDetection

1 Introduction

We are currently witnessing great transformations in our society, more specifically at the technological level. In the world where we live the Internet has a fundamental role in creating a new space, where we do not need physical presence to commit something illicit.

All data stored on a computer or network represents a three-dimensional model in which the virtual user can move. [1]

In this paper, we will address one of the events that in recent years has taken over the Internet, cyberattacks.

In fact, the network society promotes that there is a development and innovation with regard to the Internet, but it is also the promoter of various dangers, including cybercrime.

There are several sectors that constantly suffer from this type of tendency, including governmental institutions, large companies and also security forces, because in these areas there is information that would be very advantageous for the Could get caught.

Cyberattack is an attempt to damage or disrupt a computer system, or obtain information stored in a system through hacking. [2]

In this paper we will address a little more thoroughly this trend of cyberattack, showing which cyberattacks most used, also some preventive measures where we will demonstrate and try to dispose possible solutions in which the common user this great and complex network can "defend".

2 Cybercrime and Cyber Attack

2.1 Cybercrime

The internet is not an impartial field, it is a space in which viruses, worms, crackers in which they pierce firewalls and access confidential data in which this information can be worth many millions in monetary terms. Computer security specialists work hard every day to keep our privacy intact and to increase the difficulty of a cyberattack on our machines.

Cybercrime is the name given to cybercrimes that encompass any activity or practices in a network, are computer crimes practiced through computers, against them or through them. In another perspective, cybercrimes can be assessed as a conduct of unauthorized access to computer systems, destructive actions, data modification, communication interception, child pornography dissemination, copyright infringement, Terrorism, among others [3].

The term cybercrime had its first appearance in a G-8 meeting (group composed of the 7 richest countries in the world and Russia) close to the end of the years 90. This meeting had the purpose of addressing the methods used to combat the Elicits practices that occurred on the Internet.

The transactional predominance is one of the strong characteristics of cybercrime, which hinders investigations and the clearance of evidence against the accused. Another feature of cybercrime is the increase of personal computers, which facilitates anyone in the world to perform illicit practices, anywhere on the planet and without leaving home.

The practice of cybercrime is so common, that, according to Norton, a company specializing in digital security, about 65% of the cybercriminals have been victims of some kind of cybercrime, where the greatest difficulty in fighting, is faced with the lack of efficient laws and punishments In several countries in the fight against criminals.

In a summarized way, cybercrime uses technology as a way to divert information online, whether it's a computer or smartphone. The development of this theme, was not an instantaneous act, was having evolutionary changes [4].

Some curiosities about cybercrimes:

- Cybercrime has already surpassed illegal drug trafficking as a criminal money maker.
- Every 3 seconds, an identity is stolen.
- Without sophisticated security measures, a PC can be infected within 4 minutes after connecting to the Internet.

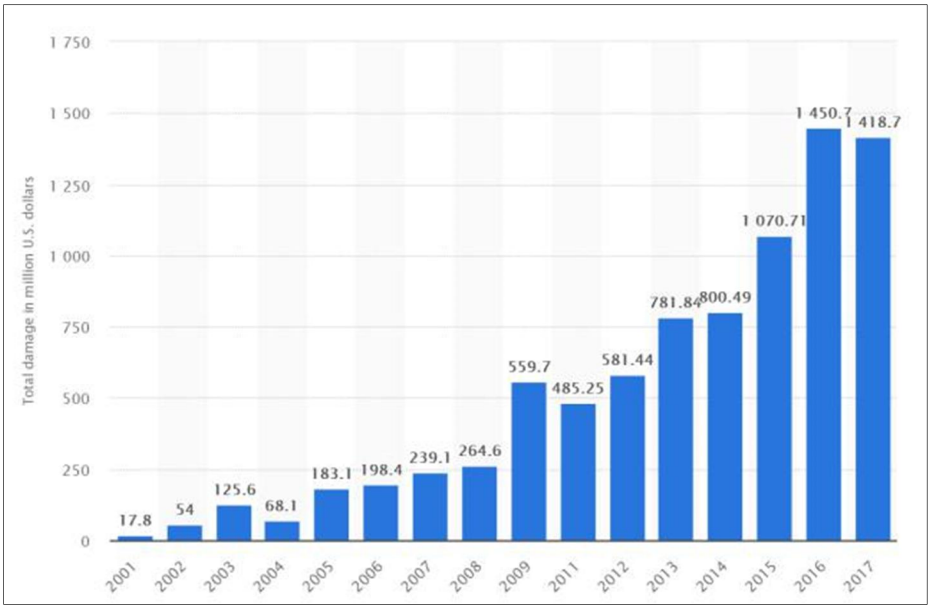

Fig.1. Amount of monetary damage caused by reported cybercrime to the IC3 from 2001 to 2017 (in million U.S. dollars) [5]

2.2 Cyberattack

Cyberattacks are an increasingly common reality in the current Internet, it is a reality that does not yet have a global and effective response in order to combat and avoid them. There are several terminologies used to designate a crime that is practiced by a computer connected to the Internet, such as cybercrimes, digital, computer, computer fraud, among others.

Cyberattack is the deliberate exploration of computer systems and technology-dependent networks. In other words, it is an unlawful, non-ethical or unauthorized conduct involving the automatic processing of data or transmission of data [6], is one that is performed by people with the objective of obtaining information or benefits using technological tools connected to the Internet and disturbing the functioning or structure of those being attacked.

Cyberattacks use malicious code to change your computer's coding, logic, or data, resulting in consequences that can compromise your data and lead to cybercrime, such as information and identity theft, a cyberattack is also Known as an attack from a computer network.

Cyberattacks have numerous consequences:

- Identity theft, fraud and extortion
- Malware, pharming, phishing, spamming, spoofing, spyware, trojans e virus
- System infiltration
- Unauthorized access

- Password sniffing
- Abuse of Instant Messaging
- Among others

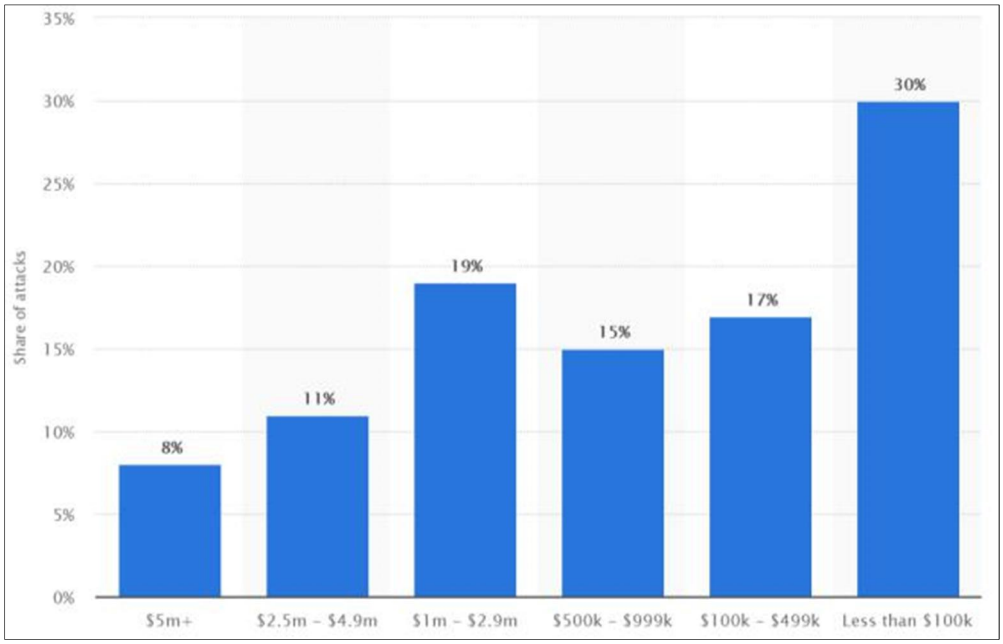

Fig.2. Average financial damages of cyberattacks caused to businesses worldwide as of April 2018 (in U.S. dollars) [7]

According to the "Convention on Cybercrime" adopted by the Council of Europe in 2001, it can be highlighted as cybercrimes:

- Infringements against the Confidencialidade, integrity and availability of data and computer systems
    - Illegal access to a computer system;
    - Unlawful intercetation of data or telematic communications;
    - Attack on data integrity (own conduct of a hacker subgroup, known as a cracker);
    - Attack on the integrity of a system;
    - Production, marketing, obtaining or possession of applications or access codes that allow the practice of the above-mentioned crimes.
- Computer infractions

- Falsification of data

- Infractions relating to the content:
  - Child pornography
  - Racism and xenophobia

- The attack on intellectual property and the rights associated with it
  - Public display of movie without permission of the Rightsholder

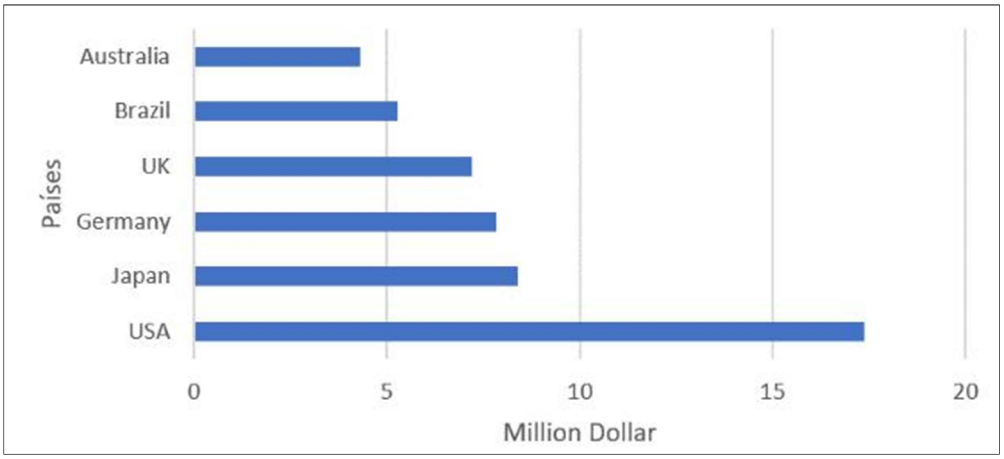

Fig.3. List of countries which have the average cost of cybercrime in the world

2.2.1 The Most Common Types of Cyberattack

With the frequency of use and sophistication of the Internet, service providers have as one of their main missions control denial of service (DoS) attacks and distributed denial of service (distributed denial) attacks of Service-DDoS), which are increasing increasingly. The internet is part of a worldwide infrastructure, which has a unique feature, that of not having boundaries that defend it from the attacks. Some of these attacks are quite harmful and can cause ample blackouts on the internet.

The DOS/DDoS attack is an attempt to make an overload happen on a device or server, so that the resources are unavailable to users, in other words, it is an attack that aims to disconnect from the Internet an equipment that is connected to it. For the attack to be performed, the attacker uses a range of techniques, using software, sending several packages to the target, for the purpose that is overloaded and unable to respond to any package requests, so put, users do not Access to the data to which the server was attacked.

The target can be a server, a router, or other equipment at times with the physical destruction of the hardware that was attacked.

DoS, it is the attack in which a computer with an Internet connection is used to flood a server with packets, the purpose of this attack is denial of service and the bandwidth overhead.

DDoS, it's practically similar to a DoS attack, but with very different results, because instead of using a computer and a connection, they use multiple computers and so many other connections. The computers behind this type of attack are part of the botnet. The main difference between DOS and DDoS is the target server, with DDoS, the server will be overloaded by thousands of requests when compared to DOS that the overhead is significantly lower.

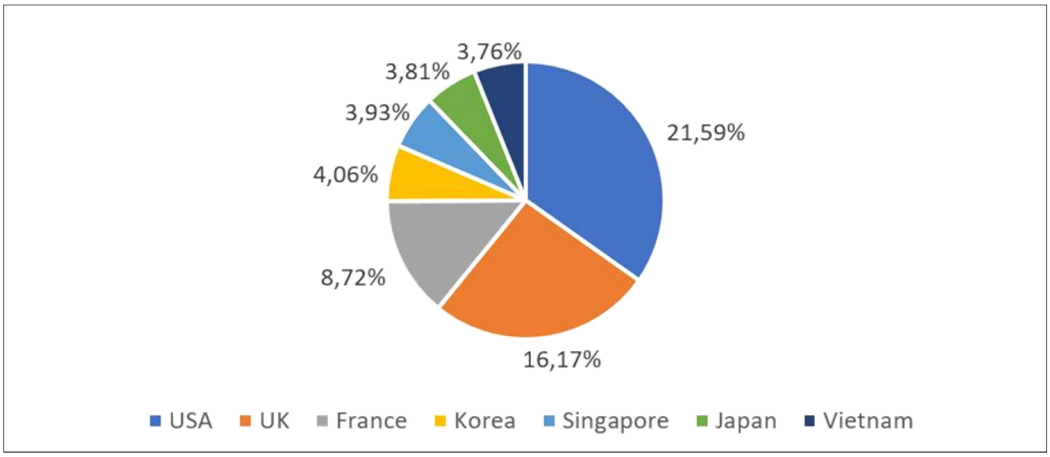

Fig.4. The list of countries from which highest percentage of Global Denial of Service Attacks (DDoS)

2.3 Tools Used in Cyberattack

In the current Internet, hackers help themselves in software to commit their actions, these help themselves in software used to practice cybercrime, called Crimeware. Crimeware is a software that is used to commit a criminal act, and is generally considered with a non-desirable software.

The software tools used in cybercrime are sometimes referred to as crimeware. Like cybercrime itself, the crimeware termination achieves a wide range of different malwares, or potentially malicious software. Crimeware is a class of malware designed specifically to automate cybercrime [8].

David Jevans created the term "Crimeware" in February 2005 in a response from the Anti-Phishing Working Group to the FDIC article "ending the identity theft of account Invasions", published on December 14, 2004.

2.3.1 Crimeware: Bots

The term "bot" is approximated by robot, is one of the most sophisticated software types of crimeware that the internet currently faces.

Bots are like Trojans and worms, perform a variety of automated tasks on behalf of hackers, who are safely located. Bots can perform various tasks, from sending spam to the detonation of Internet sites.

Bots can invade computers in many ways, sometimes they are scattered over the internet, looking for vulnerable and unprotected computers to infect [9]. When you reach your goal and find an exposed computer, quickly infect the machine found and report to your "master". Your main goal is to stay hidden until you receive some kind of task transmitted by your master.

The service provider informs you that your computer is sending spam to other Internet users [10]. Bots are part of a network of infected computers called "botnet", these networks are created by attackers repeatedly infecting victims ' computers.

2.3.2 Crimeware: Trojans and Spyware

One of the most popular methods among hackers is Trojan horses and spywares.

Trojan Horse Software presents itself to the computer as a useful program, while in fact wreaking havoc and damage. Trojan horses are the first part of an attack, and your goal is to remain hidden during a download. These can not be scattered alone, such as a virus or worm [11].

Spyware is the term used for programs that secretly observe and monitor the activity of a computer, storing information that may be sold to entities that benefit from this information. Spyware can be installed in several ways, most of the time it is improperly installed and bundled with other software's that install purposely [12].

3 The Concept of Cyber Prevention and Detection

The internet is a large network where there are multiple computers interconnected by other smaller networks, and they communicate with each other. The computers communicate with each other through an IP address, where a series of information is exchanged and there arises the biggest problem, because there is a large amount of personal information that crosses this network, being the disposition of thousands of people who Have access to the Internet, and when they are not available by the user themselves, are sought by other users and then committing the so-called cybercrimes [13].

Cybernetic Prevention is the act of restricting, controlling, removing or preventing the occurrence of cyberattacks in computer systems. On the other hand, Cyber Prevention is responsible for detecting irregularities in the activities of the Internet user.

In current times, cyberattacks can capture a lot of information and even keep it out of the control of its owners, to protect this information it is very important to prevent and act against possible cyberattacks that may arise [14].

A good security engineer always has to in mind that "security is not a product, but rather a process", more than designing a system that solves some network gap, a strong encryption in a system, is to be designing a model in which all strategies and Med Safety, so that systems are more and more protected from threats.

On a computer or IT system, the security status goes through three processes: threats prevention, detection and response [15].

These three processes are based on various system policies and components, such as access and cryptographic controls, firewalls that play a very important role in preventing systems, intrusion detection systems (IDSs), and the response of Systems to the attacks.

Access and encryption controls can protect data from systems.

The firewall is by far the most common prevention system, with regard to network security, since, properly configured, provides essential safeguards and protects access to internal network services and to catch certain types of attacks, due to its packet filtering capability.

"Answer" is necessarily defined by the security requirements assessed in an individual system and can cover from simple update protections to notification of legal authorities, counterattack.

3.1 Prevention Tips

Keep your computer current with the latest patches and updates. The updates provided are useful for the computer to be protected and prevents attackers from leveraging software failures (vulnerabilities) that they could use to invade the system [16]. Using the "Automatic Updates" feature is a great start to keep seguro on-line.

- Make sure your computer is configured securely

A configuration Efficient Of the most popular applications on the Internet, such as the browser or email software, is one of the most important areas, and where the utmost attention to detail can help prevent an attack.

- Choose strong passwords and keep them safe

The passwords are a fact of life on the Internet, are for our information what keys are to the door of our house, they protect our property or our data, for the rest of the world. In the current generation of internet, "discovering" the password of another is a crime, because we can pass by someone else or acquire private data. As such, act with some seriousness at the time of electing one, as well as not sharing. Keep the password private and a way to ensure its effectiveness.

- Protect your computer with security software

Protecting your Pc with specific security software is essential to a basic online security, these software's include firewall and antivirus programs that can assist in the protection of possible cyberattacks. There are several software packages that encompass numerous combinations of protection, such as firewall, antivirus, anti-spyware Among other features such as antispam and parental controls that assist in the sudden counterattacks protection.

- Protect your personal information

On the Internet, to take advantage of many services, we inevitably provide personal information. As the disclosure of personal information is rarely possible, the following list contains some advice on how to share personal information securely online:

- Keep an eye on fake email messages.

- Do not respond to email messages requesting personal information.
- Avoid Fraudulent websites used to steal personal information.
- Attention to privity policies on websites and software.
- Save Email address, and not disclose unnecessarily.

4 Example of Cyberattack and Preventive Measures

4.1 Man on the middle

Regardless of the type of business, the goal of hackers is to steal information from Internet users, whether through individual or large-scale attacks. Almost always, offenders start by trying to introduce some kind of virus into the target computer, if for some reason it goes wrong, one of the most popular attacks is called "Man in the Middle", as its own name implies, the attacker sits between the client and the Server that is available to you.

During a "man in the middle" attack the communication between a and B is intercepted by the attacker, and relayed in an unlimited way, the attacker can retransmit the data without change, but also with change or block part of the data.

One of the most common strands of the attack is the attacker taking over a Wi-Fi router, interconnecting conversations with them. The practice of free Wi-Fi is the most common one for which an attacker can perform the attack, because these networks can have multiple users and network security is not so restricted.

Fig.5. “man in the middle” - normal communication and communication intercepted

4.1.1 Example

Communication between "A" and "B" where "C" is the attacker:

1 - "A" sends a message to "B" that is intercepted by "C". A “Hello B, send me the key” → C B

2 - "C" sends message to "B" (all points that was sent by "A") “C” → “Hello B, send me the key” → B

3 - “B” Responds with the key “C” ← [Key] ← B

4 - “C” Replaces the "B" key with yours and passes it to "a" A ← [Key “C”] ← C

5 - “A” Encrypts a message and with what believes that the key is “B” “A” → “Message” [Key “C”] → “C”

6 - The message was encrypted with the "C" key So "C" sees the content and modifies it if you want to “C” → "Message Changed" ["B" key] → “B”

4.1.2 Defenses

Although they cause great damage and are dangerous, there are different ways to defend themselves from the man in the middle attack, and most of them should be installed on the router and servers. A technique widely used, and that can help combat the attack is the encryption between client and server, in this case the server identifies the client due to its digital certificate and establishes the cryptographic connection, where the information is completely secure.

Another caution that the user should take into account is Internet browsing and choose to browse websites that use the HTTPS protocol, because this protocol is encrypted that prevents the hacker from accessing the information.

Access to free Wi-Fi networks is the oasis for hackers, because there are inexperienced users at the level of digital security, in these networks is where there are the greatest number of attacks man in the middle. Whenever the user uses Wi-Fi networks that are not encrypted, one of the forms of defense is to create a VPN service. This VPN service ensures that data circulating on the network is not exposed in these unsafe environments. The VPN encrypts the connection, and in which hackers will not have access to the IP.

5 Conclusion

The new technologies, more specifically the Internet, have lots of positive points, such as globalization making computer equipment indispensable in our daily life, but with this information circulation so fast and the learning it offers, the Internet also has its less good points, such as cybercrime and cyberattack. With the ease of access that the Internet offers and the increase in the number of users, many of them without any knowledge at the computer level, the most serious problems begin to appear.

However, because of this increase in users, opportunities for digital crime practices also grow, where more experienced users are taking on less experienced users to commit crimes, in which attackers take their Benefit.

Therefore, to combat these attacks, we need preventive measures and good practices in the use of this great global network, the Internet.

In this paper, the concept of cybercrime and cyberattack were studied, and we discussed some tools that attackers use to take possession of the information circulating in the "arteries" of this great global network, the Internet.

In the end, we conclude and discuss the tools and preventive measures that, adopted by users, hinder the work of attackers and thus protecting private information.

References

1. “all of the data stored in a large computer or network represented as a three-dimensional model through which a virtual-reality user can move” Collins English Dictionary – Complete & Unabridged 2012 Digital Edition.
2. Collins English Dictionary, Corpyrigth HarperCollins Publishers.
3. Pinheiro, P. P. Direito Digital. 4. ed. São Paulo: Saraiva, (2010).
4. DONNER et. al. Low self-control and cybercrime: Exploring the utility of the general theory of crime beyond digital piracy. Journal Computers in Human Behavior, (2014).
5. https://www.statista.com/statistics/267132/total-damage-caused-by-by-cyber-crime-in-the-us/
6. Neto, M. F. and Guimar˜aes, J. A. C., Crimes na internet: elementos para uma reflexão sobre a ética informacional. Revista CEJ, 7(20). ISSN 2179-9857, 2003.
7. https://www.statista.com/statistics/881158/average-financial-damages-via-cyber-attacks/
8. Markus Jakobsson, Zulfikar Ramzan, Crimeware: Understanding New Attacks and Defenses, 2008
9. Shuchi Juyal and Ruchika Prabhakar, “A comprehensive study of DDoS attacks and defense mechanism”, Journal of Information and operation management, 2012.
10. Soumya Tiwari , Anshika Bhalla and Ritu Rawat, “Cyber Crime and Security”, International Journal of Advanced Research in Computer Science and Software Engineering, 2016.
11. Wadhwa, A. and Garg, A., Studying and Analyzing Virtualization While Transition from Classical to Virtualized Data Center. International Journal of Computer Applications, 2015.
12. Seema Vijay Rane and Pankaj Anil Choudhary, “Cyber Crime and Cyber Law in India”, Cyber Times International Journal of Technology and Management, September 2012.
13. INELLAS, G. C. Z., Crimes na Internet. São Paulo: Editora Juarez de Oliveira, 2004.
14. Enrique García, www.larepublica.co, 20 de julho de 2018
15. Wadhwa, Amit. "Comprehensive Analysis of Security Issues and Solutions While Migrating to Cloud Environment." International Journal of New Innovations in Engineering and Technology 4.4 (2016)
16. Wadhwa, Amit. "Comprehensive Analysis of Security Issues and Solutions While Migrating to Cloud Environment." International Journal of New Innovations in Engineering and Technology 4.4, (2016)