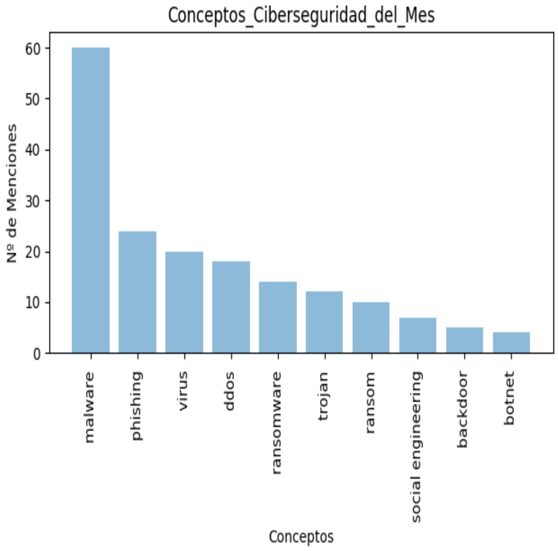
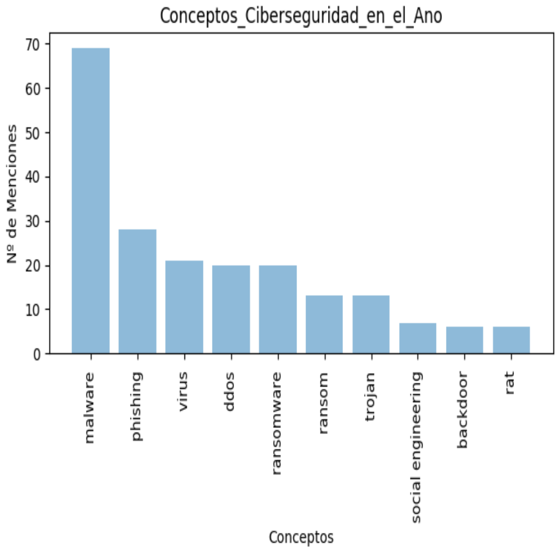
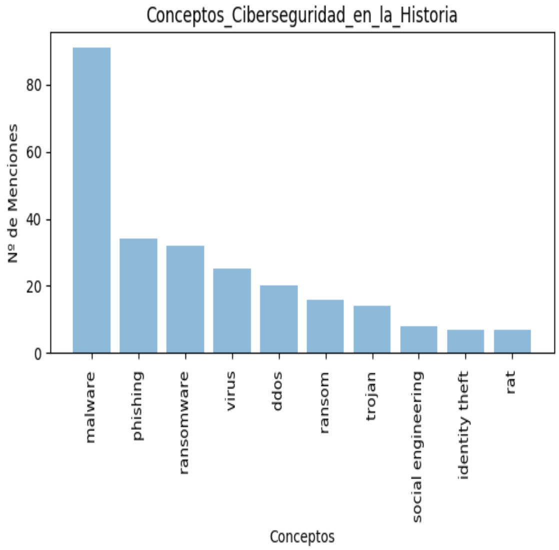
Informe de Ciberseguridad 2019-03-12


Conceptos_Ciberseguridad_del_Mes


Conceptos_Ciberseguridad_en_el_Ano



malware: Malware (a portmanteau for malicious software) is any software intentionally designed to cause damage to a computer, server, client, or computer network. Malware does the damage after it is implanted or introduced in some way into a target's computer and can take the form of executable code, scripts, active content, and other software. The code is described as computer viruses, worms, Trojan horses, ransomware, spyware, adware, and scareware, among other terms. Malware has a malicious intent, acting against the interest of the computer user—and so does not include software that causes unintentional harm due to some deficiency, which is typically described as a software bug. Programs officially supplied by companies can be considered malware if they secretly act against the interests of the computer user. For example, Sony sold the Sony rootkit, which contained a Trojan horse embedded into Compact disc that silently installed and concealed itself on purchasers' computers with the intention of preventing illicit copying. It also reported on users' listening habits, and unintentionally created vulnerabilities that were then exploited by unrelated malware.One strategy for protecting against malware is to prevent the malware software from gaining access to the target computer. For this reason, antivirus software, firewalls and other strategies are used to help protect against the introduction of malware, in addition to checking for the presence of malware and malicious activity and recovering from attacks. https://en.wikipedia.org/wiki/Malware
phishing: Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising as a trustworthy entity in an electronic communication. Typically carried out by email spoofing or instant messaging, it often directs users to enter personal information at a fake website, the look and feel of which are identical to the legitimate site.Phishing is an example of social engineering techniques being used to deceive users. Users are often lured by communications purporting to be from trusted parties such as social web sites, auction sites, banks, online payment processors or IT administrators.Attempts to deal with phishing incidents include legislation, user training, public awareness, and technical security measures — because phishing attacks also often exploit weaknesses in current web security.The word itself is a neologism created as a homophone of fishing, due to the similarity of using a bait in an attempt to catch a victim. https://en.wikipedia.org/wiki/Phishing
ddos: In computing, a denial-of-service attack (DoS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to

the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.In a distributed denial-of-service attack (DDoS attack), the incoming traffic flooding the victim originates from many different sources. This effectively makes it impossible to stop the attack simply by blocking a single source. A DoS or DDoS attack is analogous to a group of people crowding the entry door of a shop, making it hard for legitimate customers to enter, disrupting trade. Criminal perpetrators of DoS attacks often target sites or services hosted on high-profile web servers such as banks or credit card payment gateways. Revenge, blackmail and activism can motivate these attacks.
https://en.wikipedia.org/wiki/Denial-of-service_attack
ransom: Ransom is the practice of holding a prisoner or item to extort money or property to secure their release, or it may refer to the sum of money involved. When ransom means "payment", the word comes via Old French rançon from Latin redemptio = "buying back": compare "redemption".
https://en.wikipedia.org/wiki/Ransom
identity theft: Identity theft is the deliberate use of someone else's identity, usually as a method to gain a financial advantage or obtain credit and other benefits in the other person's name, and perhaps to the other person's disadvantage or loss. The person whose identity has been assumed may suffer adverse consequences, especially if they are held responsible for the perpetrator's actions. Identity theft occurs when someone uses another's personally identifying information, like their name, identifying number, or credit card number, without their permission, to commit fraud or other crimes. The term identity theft was coined in 1964. Since that time, the definition of identity theft has been statutorily prescribed throughout both the U.K. and the United States as the theft of personally identifying information, generally including a person’s name, date of birth, social security number, driver’s license number, bank account or credit card numbers, PIN numbers, electronic signatures, fingerprints, passwords, or any other information that can be used to access a person’s financial resources.Determining the link between data breaches and identity theft is challenging, primarily because identity theft victims often do not know how their personal information was obtained, and identity theft is not always detectable by the individual victims, according to a report done for the FTC. Identity fraud is often but not necessarily the consequence of identity theft. Someone can steal or misappropriate personal information without then committing identity theft using the information about every person, such as when a major data breach occurs. A US Government Accountability Office study determined that "most breaches have not resulted in detected incidents of identity theft". The report also warned that "the full extent is unknown". A later unpublished study by Carnegie Mellon University noted that "Most often, the causes of identity theft is not known", but reported that someone else concluded that "the probability of becoming a victim to identity theft as a result of a data breach is ... around only 2%". More recently, an association of consumer data companies noted that one of the largest data breaches ever, accounting for over four million records, resulted in only about 1,800 instances of identity theft, according to the company whose systems were breached. An October 2010 article entitled "Cyber Crime Made Easy" explained the level to which hackers are using malicious software. As Gunter Ollmann, Chief Technology Officer of security at Microsoft, said, "Interested in credit card theft? There's an app for that." This statement summed up the ease with which these hackers are accessing all kinds of information online. The new program for infecting users' computers was called Zeus; and the program is so hacker-friendly that even an inexperienced hacker can operate it. Although the hacking program is easy to use, that fact does not diminish the devastating effects that Zeus (or other software like Zeus) can do to a computer and the user. For example, the article stated

that programs like Zeus can steal credit card information, important documents, and even documents necessary for homeland security. If the hacker were to gain this information, it would mean identity theft or even a possible terrorist attack. The ITAC says that about 15 million Americans are having their identity stolen, in 2012.
https://en.wikipedia.org/wiki/Identity_theft