International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 5 May 2022, pp: 1704-1708 www.ijaem.net ISSN: 2395-5252

Cyber Security: Types and Threats –A Study

Preet Kamal
PG Department of Information Technology Goswami Ganesh Dutta Sanatan Dharma College Chandigarh, India.

Submitted: 15-05-2022 Revised: 20-05-2022 Accepted: 25-05-2022

ABSTRACT-This study will put emphasis on most cyber threats that people experience in their daily life. In last two years, people from every field were forced to work online due to outbreak of Covid-19. This outbreak proved to be a good opportunity for the attackers to breach into the sensitive data as whole the world was working online and few of them felt anxious and uncomfortable due to changed platform. Cyber attacks plays a major role in every field such as education, health, banking, reservation, shopping and variety of e-commerce platforms. Online platform have vast exposure as everyone, every time and everywhere working online. This creates a vulnerable environment for every individual, social engineering threats and attacks are unpredictable and can prove to be most dangerous. Last two years were most crucial for everyone in this world as everyone was forced to sit at home and work online. This study will provide the risks involved using online platforms and various attacks that happened in last two years.

Index terms: Cyber attacks, Social engineering, Covid-19, Vulnerable.

I. INTRODUCTION

Corona virus disease 2019 (COVID-19), the extremely communicable transferable disease caused by brutal severe respiratory syndrome corona virus 2 (SARS-CoV-2), has had a terrible consequences on the world's demographics resulted in more than 2.9 million deaths globally, rising as the mainly substantial worldwide health emergency since the era of the influenza pandemic of 1918 [3]. The corona virus outbreak comes out eventually in 2019 resulting in worldwide restrictive measures that were introduced in most countries in 2020. This period provided novel challenges and uncertainties [5].

Transformation in lifestyle associated concerns contiguous corona virus disease 2019 (COVID-19) could possibly impact sleep patterns [10]. The world health organization classified the Covid-19 epidemic as a pandemic in March 2020[14].

With the enlarged Covid-19 infections and deaths, governments forced lockdowns on their citizens, curbing their daily activities. This regulation made organizations discover afresh carrying out their businesses, and most of them had to settle to allow their employees to start working from home. Hence, technology plays a major part in professional as well as in personal life. Despite the rising use of technology, many firms lack a cyber-safe remote environment policy. The transformation in mode of education from traditional to online gave a challenge to the education department and forced schools to shut. Though the transformation of teaching platform was taken to continue the studies of school children, but the negative effects have also taken their place. It worked as an impetus for the educational institutions to grow and opt online platforms using new technologies. This situation forced the educators to shift to online mode overnight and it was difficult for people who were not so efficient using the new technologies. On the other hand, dependency on technology has made everyone vulnerable and exposed to cyber world which created the environment for cyber attacks to steal the data [9][1].

II. LITERATURE REVIEW

According to the World Health Organization (WHO), the count of cyber attacks increased numerously and launched has increased five-fold throughout the period of COVID-19 pandemic [14]. Cybercriminals frequently hamper with information and act as if to be trusted as organizations like the WHO and, as a result, take advantage of individual feelings of vulnerability in the unsure times of a pandemic[15].

A disease was detected in China in December 2019 named COVID-19 afterwards, extended all over the world within a few months of time span and was declared a pandemic by the World Health Organization on 11th March 2020. Educational institutes and universities all over the world enforced to close their campuses and shift all their academic activities online [2].

Authors proposed that outbreak of the corona virus pandemic became a great opportunity for cyber attacks to grow faster as number of users increased online. To get most of this lucrative benefit from this situation, hackers from the field became pro active to threat and attack diverse platforms for their interests and extra benefits [6].

This survey result appears that the college students in Tamil Nadu are having over normal level of awareness on Cyber related risk issues which can offer assistance them to secure themselves from the cyber attacks. Completely fledged cyber mindfulness will make understudies to secure themselves from programmers and hence the mindfulness needs to be made in higher level [8].

Last year proved to be a very hectic and busy year for the attackers, the number of attacks went to 925 per week according to one study [21]. Colonial Pipeline attack conquered media and deliberations on air [22].

Throughout pandemic cyber risks increased as people's usage of technology and handling failures in the development of systems and technology. New technologies inclusive of Telework and IoT-based functioning are most vulnerable to cyber attacks. Attackers breached into Verkada, a cloud-based video security service [22]. Tele health protects patients and other health workers from corona virus infection but at the same time making them vulnerable to cyber and privacy risks. 45 million persons were exaggerated by healthcare attacks [23]. Block chain rescue people form pandemic management and look up the privacy and security of digital health systems. A distributed finance "DeFi" named project PolyNetwork was hacked in August 2021, ensuing in over $600 million loss [24].

I. Common Attacks And Vulnerabilities

A cyber attack is breach into the sensitive information of any organization or any individual maliciously. The aim of any cyber attack is to destroy the data or financial gain. A skilled attacker launches the attack and it is difficult to differentiate between many identical pages. Based on the goal of the attacker the attacks can differ in two ways: Targeted and untargeted attacks.

Targeted attack: This type of attack can be targeted or funded attack either to gain financial benefits from the organizational data or where the attacker is anxious to steal the information. Researching for such an exploit can take a long time in order to determine the optimal technique to exploit the system. Because they are precisely designed, targeted attacks pose a greater threat than untargeted attacks. Spear phishing, establishing a botnet, and manipulating the supply chain are just a few examples.

Untargeted attack: This type of assault leads the attacker to attacks a large number of devices or users. The attacker could take advantage of the open internet. Phishing, ransom ware, and scanning are just a few examples.

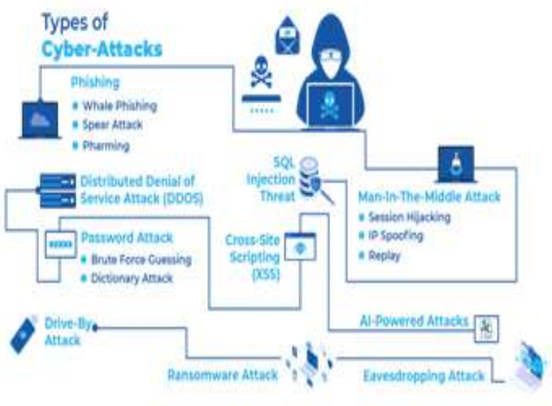
The following stages are involved in majority of cyber-attacks: survey, delivery, breach, and affect.

Survey: Knowledge about the target is evaluated in order to establish the probability of threat.

Delivery- To cope with the aspect of a machine that can be exploited for vulnerability.

Breach– Gaining unauthorized access through the advantage of weaknesses in the system.

Affect- To accomplish the goals attacker perform actions within a device.



III. TYPES OF ATTACKS

A. Denial-of-service (DoS) and distributed denialof-service (DDoS) attacks: A denial-of-service assault overruns the machine sources so that it can't give solution to the provider's request. The host system which might be suffering from malicious software program that are managed with the aid of using an attacker launches DDoS assault. In this kind of cyber-assault, the system or community sources are made unavailable for the supposed person with the aid of using annoying. TCP SYN flood assault, teardrop assault, smurf assault, ping-of-dying assault and botnets are the distinctive sort of DoS and DDoS attacks. It could be very tough to save you DoS assault as it's miles very difficult to distinguish a valid one from a malicious visitors request as they use identical port and protocol. In order to guard the machine from denial-of-provider assault, make certain that the machine comprise IDS, DDoS safety product. It is vital to make certain that there may be surplus of bandwidth net connection on a selected organization [17]. As there may be massive bandwidth for provider visitors requests, it allows to guard in opposition to low-scale DDoS attacks. DDoS attacks that exhaust the main resources of the target system, rendering all services unavailable. Recently reported DDoS attack occurred in Feb 2022 where the attacks happen in Russia and Ukraine where the banks and foreign ministry affairs were the target [24].

B. Man-in-the-middle (MIM) attack: A MIM assault takes location while a 3rd celebration comes in among the verbal exchange of a purchaser and a server. The 0.33 celebration impersonates each the purchaser and the server and benefit get admission to the records among them. This type of assault makes a risk actor to seize, dispatched and acquire the facts which meant for a person else others. A MIM assault misuses the actual time operation of transactions, verbal exchange or trade of different records. The distinct kinds of man-in-the-center assault consists of session hijacking, IP spoofing and reply. An intrusion detection gadget may be installation so that it will keep away from man-in-center assault. It allows to present instantaneously alert if a person attempts to hijack the community flow. Virtual personal community also can be used to save you man-in-center assault. This allows creating extra steady layers while gaining access to a company's personal layer thru Wi-Fi [17][18].

C. Phishing attack: Phishing: It is a type of attack that make fool out of people so that they get trapped into hackers plan. It makes people disclose their confidential information by clicking on some link received through Email or via SMS. Attacker could pretend to be an organizational official. There are various type of phishing attacks that are mentioned in table they tend to take personal information, make people reveal their passwords and other confidential information [4][18]. Phishing assault is the manner of sending fraudulent emails that appears to return back from relied on sources. The foremost intention of this sort of assault is gaining non-public and credential information. Phishing assault is a shape of social engineering and technical trickery. It is within side the shape of emails which includes embedded links that hundreds malware onto our system. Sometimes this hyperlink additionally ends in an illegitimate internet site that makes us to down load malware or surrender our non-public information. In order to lessen the danger of phishing assault, critical thinking, soaring over the links, studying e mail headers and sandboxing may be used. Moreover, through giving awareness most of the agency personnel in addition to for individuals we will save you phishing assault to a few extent. In April 2022, approximately every week reported with phishing attack. UK government employees receive 'billions' of malicious emails per year, Pegasus mobile spyware used zero-click exploits to snoop on Catalan politicians and Credit card industry standard revised to repel card-skimmer attacks [25].

D. Password attack: The maximum not unusual place approach to authenticate person is to use passwords and acquiring such passwords is an effective assault approach. Password assault is the approach wherein person's password is acquired or decrypted via way of means of illegitimate approach. User password may be acquired via way of means of searching around the person's desk, via way of means of guessing, gaining access to password database, sniffing the community connection to get the plaintext password etc. Password sniffers, dictionary attacks, cracking applications are the specific strategies utilized by the cyber criminals in password assault. By converting the passwords frequently, the use of unrecognizable phrases and minimal length can the specific approach via way of means of which password assault may be defended. Brute pressure and dictionary assault are the 2 main strategies wherein password may be acquired. Brute pressure is a random approach wherein specific passwords are tried looking forward to that one password will phrase while the later approach benefit get entry to a person's pc and community [19][20]. March 2022: Microsoft Breached by Lapsus$ Hacker Group, he most recent known data breach came to light on April 4, 2022 when the company Block acknowledged that Cash App had been breached by an insider threat [26].

E. SQL Injection: SQL (Structured Query Language) is a programming language for storing, manipulating, and retrieving data from databases. Select, for example, is a SQL command. To complete the task, update and remove. SQL can also be used to run searches on the database, and add records to the database database, as well as the ability to create new tables in the database. SQL Injection (SQI) attacks utilise malicious code to gain access to a system. Backend database manipulation is used to gain access to information. Any sensitive organisation could be included in this data. Details, customer/user personal information, and so on. This could lead to the unauthorised access of user data, and the destruction of table data as well as an unauthorised database assault. An attacker who wishes to perform SQL injection will do so modify a common SQL query to find flaws in the system a database that hasn't been checked. Misfiltered characters can also be used by attackers to change SQL statements. There are several of them. If you want to prevent and protect yourself from SQLI attacks, there are a few things you can do. They do happen. It's possible to use input validation to find out what's going on. Illegal user inputs, which is a coding approach that can. This method, however, is not as suitable as the mapping of It is not possible to use all legal and unlawful inputs. This has resulted in

Typically, a web application firewall (WAF) is used to block access to web applications. SQLI is not available. SQL injections can also be identified and blocked with minimal false positives using signature recognition, IP reputation, and other security approaches. Structured Query Language statements are in charge of them (SQL). The interaction is carried out via various SQL statements. SQL injection (SQLI) is a type of attack that exploits SQL statement inputs.To carry out the attacks, SQL queries are usually tainted with special characters or keywords. The attacker tries to change the logic of the statement so that it can read, modify, and delete private database records[7][16]. Internal AWS credentials swiped by researcher via SQL payload, Chief hacking officer and CISO Chris Evans blamed the problem on delays in backend payment systems. [27]

IV. CONCLUSION

In this study main focus of discussion was common attacks and the vulnerabilities that become the cause of attacks. The spotlight was on various attacks that interrupt routine life of a person working and have lots of online data. From exhaustive literature review it has been that majority of attacks are consequences of less awareness of technology or avoidance of little settings that need change in their systems. Cyber attackers are so active online that they try each and every method to use the vulnerabilities left by the user. Common people can become the victim easily and caught up in loosing sensitive data, bank account frauds and ransomware. To avoid such attacks people should avoid clicking on the links and reveling personal information on phone. Leaving vulnerabilities can cause stealing of sensitive information and if system seems to get busy user should not try to access the website, it could be a cyber attack. Choosing password wisely can also help to avoid the attack; password should not be simple so that it can be guessed easily. Avoid using pet name, mother's maiden name, birth place as they are very easy to guess and people around us can use this information to crack the password. Various recent cyber attacks also discussed in the study, future prospective of this study is to bring the various precautions that can save the people from cyber attacks.

REFERENCES

[1]. Aldawood, H., & Skinner, G. (2019). Contemporary cyber security social engineering solutions, measures, policies, tools and applications: A critical appraisal. International Journal of Security (IJS), 10(1), 1.

[2]. Bao, W. (2020). COVID-19 and online teaching in higher education: A case study of Peking University. Human Behavior and Emerging Technologies, **2**(2), 113– 115

[3]. Cascella, M., Rajnik, M., Aleem, A., Dulebohn, S. C., & Di Napoli, R. (2022). Features, evaluation, and treatment of coronavirus (COVID-19). Statpearls [internet].

[4]. Chetioui, K., Bah, B., Alami, A. O., & Bahnasse, A. (2022). Overview of Social Engineering Attacks on Social Networks. Procedia Computer Science, 198, 656-661.

[5]. Cruz, M. P., Santos, E., Cervantes, M. V., & Juárez, M. L. (2021). COVID-19, a worldwide public health emergency. Revista Clínica Española (English Edition), 221(1), 55-61.

[6]. Khan, Navid Ali, Sarfraz Nawaz Brohi, and Noor Zaman. "Ten deadly cyber security threats amid COVID-19 pandemic." (2020).

[7]. Kowta, A. S. L., Harida, P. K., Venkatraman, S. V., Das, S., & Priya, V. (2022). Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders, and Attacks. In Proceedings of International Conference on Computational Intelligence and Data Engineering (pp. 387-401). Springer, Singapore.

[8]. Lallie, Harjinder Singh, et al. "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic." Computers & Security 105 (2021): 102248.

[9]. M. Humayun, M. Niazi, N. Jhanjhi, M. Alshayeb, and S. Mahmood, "Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study," Arabian Journal for Science and Engineering, vol. 45, Jan. 2020, doi: 10.1007/s13369-019-04319-2.

[10]. Robillard, R., Dion, K., Pennestri, M.-H., Solomonova, E., Lee, E., Saad, M., … Kendzerska, T. (2021). Profiles of sleep changes during the COVID-19 pandemic: Demographic, behavioural and psychological factors. Journal of Sleep Research, **30**(1), e13231. https://doi.org/10.1111/jsr.13231

[11]. Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. Future Internet, 11(4), 89.

[12]. Wang, J., Gong, Y., Chen, Z., Wu, J., Feng, J., Yan, S., … Yin, X. (2020). Sleep disturbances among Chinese residents during the Coronavirus Disease 2019 outbreak and associated factors. Sleep Medicine, **74**, 199–203. https://doi.org/10.1016/j.sleep.2020.08.002

[13]. World Health Organization, "WHO DirectorGeneral's opening remarks at the media briefing on COVID-19 - 11 March

2020,” World Health Organization, Mar. 11, 2020. https://www.who.int/director-general/speeches/detail/ who-director-general-s-opening-remarks-at-the-mediabriefing-on-covid-19---11-march-2020.

[14]. WHO reports fivefold increase in cyber attacks, urges vigilance. World Health Organization. 2020 Apr 23. URL: https:/ /www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance

[15]. Williams, C. M., Chaturvedi, R., & Chakravarthy, K. (2020). Cybersecurity risks in a pandemic. Journal of medical Internet research, 22(9), e23692.

[16]. AL-Maliki, M. H. A., & Jasim, M. N. (2022). Review of SQL injection attacks: Detection, to enhance the security of the website from client-side attacks. International Journal of Nonlinear Analysis and Applications, 13(1), 3773-3782.

[17]. S. Haider et al., "A Deep CNN Ensemble Framework for Efficient DDoS Attack Detection in Software Defined Networks," in IEEE Access, vol. 8, pp. 53972-53983, 2020, doi: 10.1109/ACCESS.2020.2976908.

[18]. Cyber-Attacks-Different types and its prevention methods,https://www.cisco.com/c/en/us/products/sec urity/common-cyberattacks.html

[19]. Antesar M.Shabut,” Cyber Attacks, Countermeasures, and Protection Schemes– AState of the Art Survey”, 2016 10th International Conference on Software, Knowledge, Information Management & Applications.

[20]. Biju, J. M., Gopal, N., & Prakash, A. J. (2019). Cyber attacks and its different types. International Research Journal of Engineering and Technology, 6(3), 4849-4852.

[21]. https://spanning.com/blog/cyberattacks-2021-phishing-ransomware-data-breach-statistics/

[22]. https://technative.io/cyber-attacks-from-2021-which-we-need-to-talk-about/

[23]. https://www.fiercehealthcare.com/health-tech/healthcare-data-breaches-hit-all-time-high-2021-impacting-45m-people

[24]. https://blog.mazebolt.com/list-of-ddos-attacks-february-2022

[25]. https://portswigger.net/daily-swig/phishing

[26]. https://firewalltimes.com/recent-data-breaches/#:~:text=On%20March%2020%2C%202022%2C%20the,been%20compromised%20in%20the%20breach.

[27]. https://portswigger.net/daily-swig/sql-injection