COVID an disguised opportunity for the Cyber Criminals

Asst. Prof Jyoti Verma[1], Dr. Jaimin Undavia[2]

[1]ROFEL,Shri G.M Bilakia College of Applied Sciences(BCA),Vapi
[2]Smt. ChandabenMohanbhai Patel Institute of Computer Applications (CMPICA)
Faculty of Computer Science and Applications (FCA)
CHAROTAR UNIVERSITY OF SCIENCE & TECHNOLOGY (CHARUSAT)

---***---

Abstract

The world is facing the worst situation today as it has been affected by the by the deadly virus COVID-19 which brought the world to a stand still position. But as its said that nothing can stop humans from making the progress. And even when the lockdown had stopped the people from stepping out from their homes the virus could not stop people from achieving the impossible. Everything which was physical was brought on the online mode be it education or business. Everything was available on the electronic device through the use of the internet. But this online usage gave the opportunity to the cyber criminals to get the information of individual handy. There were cyber criminals around the world who used the email spoofing to generate revenue or used the phishing to get the money transfer to their accounts and the possibility of the DOS and DDOS attack also increased to hamper the normal functioning of various sectors. As the cyber space usage is increasing the more the cyber security issues are being considered.

Keywords

Cyber space, DOS, Phising, Dataset ,Machine learning, multiple regression, mining,COVID, DDOS

INTRODUCTION

The world is moving towards the new era of information technology where everything is being taken online be it the education or banking or medicine. And looking back in 2020 the COVID has brought the world under one roof of the technology. Not even a single person has set back because of the lockdown implemented world wide. Everyone found an alternate way to earn the bread and butter and reach the concerned audience. Also the ISP sector has made tremendous progress as it had to fulfill the requirement of the people to get the internet. But all this lead to the disadvantage which was in fact advantage but people with bad intentions converted this opportunity to disgusting face. All the information which was locked with people is now openly available on the internet due to the usage of internet to take the business ahead and not to stop the regular services. Cyber criminals have just taken the advantage of the situation as people unknowingly the become the victim of the cyber crime either by clicking the link or by opening a email attachment or downloading an extension.

The popular ways to attack people is using the phishing, DOS attack, vishing, randsome ware

LITERATURE REVIEW

(Omodunbi B.A., Volume 11, Issue 9, September 2020) Esan Adebimpe, Adanigbo O.O. have discussed the cyber crimes in various sectors like eduction, health care, social media, ecommerce,and banking. They have analysed all the common types of the cybercrime that took place in pandemics. The authors have considered the crimes which were recorded in Nigeria and they have concluded that more gender senitisation needs to be spread to make the people aware about the crimes which are conducted. The authors have used a questioner to collect the data from the internet users.

(Gondi, 2020)The authors Swathi Sambangi andLakshmeeswari Gond have tried to implement the machine learning algorithm to identify the DDOS attack in the cloud computing environment. The authors have used the popular dataset CICIDS 2017 benchmark dataset for their experiment and have considered only the Friday traffic log file as their day of consideration for the possibility of the attack. A more appropriate finding can be obtained by implementing the multiple regression technique. The model built is 97.86% for the morning logfile. The authors have considered only one day traffic log file which can be extended for all the week days to find the more efficient working model.

(Harjinder Singh Lallie, 2020)The authors Harjinder Singh Lallie, Lynsay A. Shepherd, Jason R. C. Nurse, ArnauErola, Gregory Epiphaniou ,Carsten Maple, and Xavier Bellekens have tried to cover all the possible types of cyber attacks and their intention behind the attack in one paper,by including multiple tables and timeline charts which show how the cyber crimes have affected the people around the world. The attackers have commonly used the phishing techniques in disguise as the government and media announcements to lure people to the attack.

(Tasnuva Mahjabin, 2017)The authors TasnuvaMahjabin, Yang Xiao, Guang Sun and Wangdong Jiang have given the indepth knowledge of the DDOS attack how to detect and prevent the attack, but the authors have also tried to show how the data which is being brought online through the use of IoT. They have tried to make it possible that the people can understand DDOS attack and which mechanism can be used for the prevention also what are the opportunities for the research are mentioned.

(Francois Mouton, march 2020)As the pandemic has affected the world in every aspects of life they authors Francois Mouton1 and Arno de Coning have tried to summarize various forms of the attacks which have been used by the criminals to fulfill their malicious intensions may it be pishing, misleading information, DOS attack, use of malware, email spam and many more. The authors have emphasized that the world needs good cyber security specialist and also the people must be made aware about the type of crimes carried out using the internet as a tool.

(Khurana, 2017)Saloni Khurana has tried to cover various methodology used in the cyber crimes and also tried to make efforts for taking this topic as an elegant topic for the research by explaining the methods of the crimes used in cyber crime and the possible loop holes in the computer management which may lead to the attack.

METHODOLOGY

Various methods used to implement the cyber crime are:

1. Phishing : the criminal uses bulk mail to implement this type of attack. A normal person falls the prey to such crime as he/she considers the mail to be a legal mail and opens the mail which may contain the virus which may get in the system or steal the personal and financial information.

2. Vishing : the criminals make fake call to people demanding their financial details and upon getting the information steal the money from the bank or get the personal information which can be used in some bad way.

3. DOS attack: the attacker tries to bock the services of the provider by attacking the protocols used either at the network layer or application layer.

4. Virus: the hackers and crackers write programs which purposely hamper the normal functioning of the computer and these virus can be the logic bombs which execute at particular time, boot sector virus which affect the boot sector, worms which don't need any host for their replication, adware which are small exe files which when downloaded on the system and harm the computer.

5. Trojans are also malicious programs that doesn't seem to ham the system but these programs steal the personal and financial information without the information of the owner.

How the cyber criminals use various method to perform cyber crime:

Data privacy[1]

Companies, medical providers and government agencies store a large amount of important data, everything from the Social Security numbers of patients to the bank account numbers of customers.[1]

Data privacy refers to a branch of security focused on how to protect this information and keep it away from hackers and cybercriminals.

Breaches in hospitals and medical networks[1]

Hospitals and other medical providers are prime targets for cybercriminals. That's because these medial providers have access to the personal and financial information of so many patients.[1]

Data breaches can expose this information, which hackers can then sell on the dark web.

Increase in phishing attacks: The COVID-19 crisis has seen a spike in phishing attacks that have resulted in many people losing their hard-earned money. Scammers have taken advantage of the ongoing chaos and confusion to launch phishing emails, websites, and other forms of attacks. As more and more people, NGOs, and religious groups are engaged in providing relief to the needy affected by the pandemic, it has become easier for these fraudsters to impersonate them and solicit donations. With the rise in job losses, there is also a possibility of a spurt in job hunting scams through dubious agencies and websites, fraudsters can run scams that offer jobs and may look legitimate but are mostly fake.[8]

KYC/Fake documents for Rs 20 lakh crore benefits: The Government of India has announced many beneficial schemes to help small businesses such as interest/EMI waive-off for MSME, microloan for unorganized vendors, a moratorium of EMI for various loans up to 6-months. But in most cases, common people might find it challenging to avail these schemes owing to the amount of paperwork and the general complexities involved in dealing with banks. There is a high possibility of many bogus agents approaching small business owners with fake offers of support in exchange for money, fraudsters may use fake KYC documents to avail such benefits or could run a racket of fund diversion.[8]

Time line of various attacks which shook the world:

1. COVID-19 test results of Indian patients leaked online (January 2021),User data from Juspay for sale on dark web (January 2021),Police exam database with information on 500,000 candidates goes up for sale (February 2021),BigBasket user data for sale online(October 2020).[13]

2. As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In), a total number of 1,59,761; 2,46,514 and 2,90,445 cyber security incidents pertaining to digital banking were reported during 2018, 2019 and 2020, respectively, Minister of State for Electronics and IT Sanjay Dhotre said in a written reply to the Rajya Sabha.[10]

3. On October 16, US-based cybersecurity firm Cyble reported a data breach on PM Modi's website narendramodi.in, believed to have impacted 5 lakh users which shows the poor cybersecurity infrastructure in the country.[10]

4. Haldiram's also witnessed a ransomware attack on its servers by unidentified hackers who have allegedly stolen crucial data and demanded a ransom of $7,50,000.[10]

5. Zoom also made a cybersecurity acquisition this year. The video conferencing company acquired Keybase, a startup that provides end-to-end encryption to protect calls from intruders and clandestine monitoring.[11]

6. Several Indian platforms in the past have seen data breaches. Earlier in May, it was reported that data of 4.75 crore Truecaller Indian users was found to be up for sale on the dark web. The development which was denied by the Swedish mobile application platform Truecaller India, was a result from its data leak.[10]

CONCLUSION

Cyber space has increased as the users have increased. And because of the large amount of information available on internet which has paved new opportunities for the criminals. May it be the health care sector, banking sector, small/big business, social media and even the personal. Whatever might be the situation around the world the people don't understand the problems of others instead they are ready to take the advantage of the situation. People with the greed to earn money and fame are the ones who are mostly engaged in such activities. Year 2019 was the golden era of the cyber crime as per the statistics a total number of 44.5 thousand cyber crimes came into the target of the cyber cell and were actually reported[14]. Most of the attacks were carried using the DDOS attack and randome ware, phishing vishing and spam emails. Also the study shows that the people are now aware of the crimes committed using the cyber space and because of that the people have started reporting the crimes.

REFERENCES

1. Francois Mouton, A. d. (march 2020). COVID-19: Impact on the Cyber Security Threat Landscape .Researchgate.
2. Gondi, S. S. (2020). A Machine Learning Approach for DDoS (Distributed Denial of Service) Attack Detection Using Multiple Linear Regression. 14th International Conference INTER-ENG 2020 Interdisciplinarity in Engineering, Mures. Romania: INTER-ENG 2020.
3. Harjinder Singh Lallie, L. S. (2020). Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic.
4. Khurana, S. (2017). A Review Paper on Cyber Security. International Journal of Engineering Research & Technology (IJERT).
5. Omodunbi B.A., O. O. (Volume 11, Issue 9, September 2020). CYBER SECURITY THREATS IN THE ERA OF COVID -19 PANDEMIC: A CASE STUDY OF NIGERIA SYSTEM. International Journal of Advanced Research in Engineering and Technology (IJARET), 387-396.
6. TasnuvaMahjabin, Y. X. (2017). A survey of distributed denial-of-service attack,prevention, and mitigation techniques. International Journal of Distributed Sensor Network.

WEBOGRAPHY

1. https://us.norton.com/internetsecurity-emerging-threats-cyberthreat-trends-cybersecurity-threat-review.html
2. https://www.wipro.com/blogs/amit-kothari/cybersecurity-strategies-for-adjusting-to-covid-19/
3. https://www.pwc.com/jg/en/topics/covid-19/managing-impact-of-covid-19-on-cyber-security.html
4. https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance
5. https://www.helpnetsecurity.com/2020/12/21/covid-19-cybersecurity/
6. https://www.cisecurity.org/blog/resource-guide-for-cybersecurity-during-the-covid-19-pandemic/
7. https://www.geektek.com/6-emerging-cyber-security-risks-to-look-out-for/
8. https://www.cnbctv18.com/information-technology/cyber-crime-in-times-of-covid-19-6-types-of-frauds-you-should-watch-out-for-in-coming-months-6287931.htm
9. https://www.indiatvnews.com/technology/news-top-5-cyber-attack-trends-likely-to-continue-in-2021-679814
10. https://www.business-standard.com/article/finance/over-290-000-cyber-security-incidents-related-to-banking-reported-in-2020-121020401220_1.html
11. https://inc42.com/buzz/india-hit-by-375-cyberattacks-daily-in-2020-says-pant/
12. https://analyticsindiamag.com/top-cybersecurity-stories-that-made-headlines-in-2020/
13. https://www.csoonline.com/article/3541148/the-biggest-data-breaches-in-india.html