International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 05 | May - 2021 ISSN: 2582-3930

IMPACTS OF COVID-19 ON CYBER SECURITY

ARCHANA R
CO-AUTHOR: Dr. SAMITHA KHAIYUM
MASTER OF COMPUTER APPLICATIONS
DAYANANDA SAGAR COLLEGE OF ENGINEERING BENGALURU

.....****.....

Abstract: COVID-19, coronavirus pandemic is an unpredictable worldwide health emergency that not only makes an impact on health and economy but almost on all aspects of our lives, including how we work, meet, communicate, collaborate virtually. To reduce the spread of COVID-19 we supposed to maintain social distancing hence learning and working were transformed to an online mode that is virtual. Which force the organization and individual to connect to the data server, IT assets and work virtually within a short period of time without any proper arrangements. Thus give an advantage for the bad actors in cyberspace. During this pandemic, bad actors in cyberspace have taken advantage of targeting vulnerable people and systems. Hence, this paper studies the issues faced in securing information & Technology assets. This paper gives a clear picture correlation between the pandemic and the increase in cyber-attacks targeting sectors that are vulnerable. This paper also attempts to analyze the impact of COVID-19 on cyber-security. This paper describes measures to be taken to protect from such cyber-attacks.

Key Word: COVID-19, Cyber security, Malware, Phishing, Ransomware, Fuzzy AHP.

1. INTRODUCTION

At corporate level this pandemic cause most serious challenge around the world. COVID-19 pandemic has collaborated peoples around the world to employ the most modern approach from data science to artificial intelligence to connect and communicate with each other. This pandemic has started a new method of work from home to everyone. Most of these companies and institutions have no plans to facilitate this drastic and sudden change within a short period. In this scenario the requirement of employees to use their own personal IT assets and home networks, which are unsecured and lack the required industrial standard security measures. Some organizations and institution provide their employees with business devices, these are typically secured with minimal or no administrative rights. Conversely, where staffs given general setup and temporary rights to installinga required software become an issue. So businesses need to provide more related solutions and employees with more rights which indirectly create a security issue. People relay on the internet for work, shop and stay entertained. People have more and more relied on the internet to work, shop, and stay amused. But, with this exaggerated use of internet services, the internet threats customers area unit exposed more. On-line unhealthy actors have taken advantage of the pandemic and area unit exploiting remote operating setups and new digital services. Finally impacts of covid-19 pandemic on cyber security are not a topic to be neglected in the present era. This paper uses a decision-making problem solving based hybrid approach of fuzzy sets. Theory and analytic hierarchy process for conducting a quantitative evaluation of the impact of thepandemic.

2. LITERATURE REVIEW

Even during the normal situation, online crimes give good returns with the least risk for the cyber attackers. Examining that more people are unemployed now, spend more time at home and using the Internet for work. Furthermore, governments have provided incentives to help people financially and so also other businesses to seek to attract or retain customers. As the world anticipates a potential cure to control the spread of COVID-19, all information related to “COVID-19” will gain the attention of citizens. The scammers are taking advantage of this avenue to send malicious [phi, smi, vi] shing3 attacks to victims disguised as the government, tax authorities, etc. with links to claim assistance in relation to COVID-19.The World Economic Forum (WEF) highlighted that hacking and phishing is the new way of attacking. Even after the viruses have disappeared. These scams are much more effective now during the pandemic as most vulnerable people are more anxious and expecting emails, texts, calls, etc. relating to COVID-19 from the authorities. As cybercriminals become taking more advantage, it is easier for them to create fake emails, messages or websites that replicate the appearance of most similar website, incorporating words use urgency to exploit the globally fear factor is to handle an emergency and needs. Therefore, cybercriminals can increase their phishing attacks. These attacks can occur in various forms such as hiding the executable file in ZIP folder, website links, attachment which consist of malware. So it’s essential to check the sender email and examine the links carefully before opening it.

3. AN EXPLOSION OF CYBER RISKS IN THE PANDEMIC OF COVID-19

Growing the dependency on virtual communication and modification to run the organization online 1has led to increase the risk of cyber-attack. Security of the organization is need to be continuously examined, supervision, and risk assessment for breaches at both physical and digital entry points. Security risk management team has to secure their organization and protect their enterprise web services and digital networks are able to withstand cyber-attacks and hacking. Certain organizations of information technology as to expand remote working capability to include worker who don't have experience in working from home. Most of IT department deploying new kind of collaboration applications for keeping them synchronized which increased the risk of hacking the sensitive data that currently exists in less secure remote based offices.

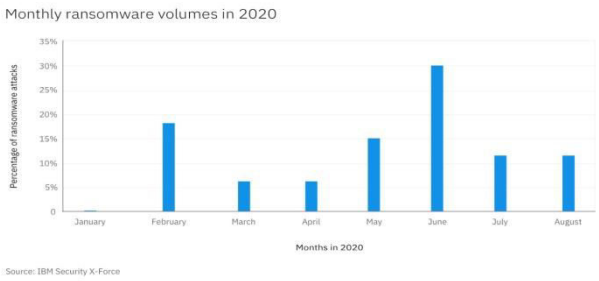
It is difficult task to implements organizational security policy and controls on team members remotely. Most of the security controls have limited ability and take considerable time to deploy. Cybercriminals knows that numerous of business and their team worker have open their door to hacking. The increased digital traffic and footprints are used by hackers to find vulnerability. In the form of phishing emails with malicious attachments, COVID-19 theme based attacks that drop malware to network steal the data and credentials. In order host malicious code attackers use the compromised website or build temporary. They attract the people to this website and inject the malicious code to the device.

COVID-19 patient's computational application status as Viruses and malware. Virtual working platforms have been hacked with video conferencing. The cyber security team has to make the virtual working of their organizations aware of scams, teach them about how to protect them from becoming prey.

4. SEVERAL CYBER-ATTACKS INCREASED DURING THE COVID-19.

1. Ransomware:

Ransomware used malware code which encrypts the MS windows machine data and this attack mainly uses affected or corrupted email attachments and malicious websites. Where the hacker threats the user to publish the data and demands money to the user to decrypt the file. This pandemic provides advantage to this kind of group and they use specific tactics such as data exfiltration/removal is performed along with malicious encrypts and when the user fails to pay or compromise the demanded money and then the hacker may leak stolen data. Below graph shows the ransomware attacks in the year 2020 it clearly shows the number of attacks more at the peak time of COVID-19 in 2020.



2. Phishing Attack:

Phishing attack refers when the hacker threats the victim by sending mails. Where the victim gets the mail and when victim follows the link provided in the mail. Where following this link connects the user computer to command center which gives access to the hacker to get any information required from the users system. Hence in this pandemic of COVID-19 people from all corners of the word panicked and therefore id they see any news or information that seams useful to prevent the disease. This gives an opportunity to the hackers to use mails which resembles organizations like WHO and when user follows link this makes success in cyber-attack.

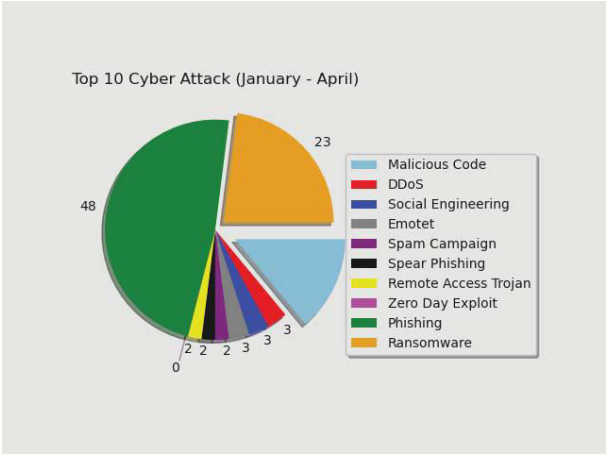
3. Pharma Spam Splashes:

When the user follows the link which referred to the preventive drugs for the COVID-19. This tempts the user to buy and this leads to harmful attack . This type of attack leads to the massive bio war when this kind of links flow through one society and they believe it's real and tempt to buy harmful needs. Hence, we can say that the COVID-19 had given a ground stage for the hackers and caused more cyber-attack which had threatened various organizations along the worldwide.

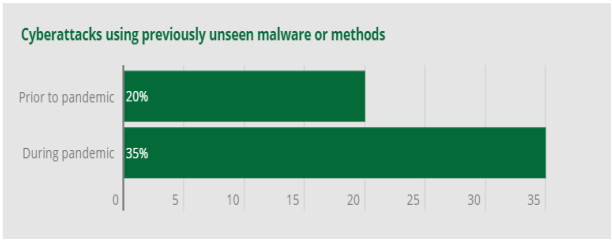
Rate of different types of cyber-attack during pandemic:

Type of cyber attack	percentage
Phishing	48
Ransomware	23
Malicious code	24
DDoS	3
Social engineering	3
Spam Campaign	2
Remote access Trojan	2

Zero day exploit	2



1. IMPACTS OF COVID-19 ON CYBERSECURITY



1. Increased Security Risk from Remote Working/Learning:
As the many companies adopted the new way of working that is working from home and even the education institutions are adapted to virtual learning for students. This made many companies and schools adopted the VPN (virtual private networking) servers which had become a life line which helped with their security and made to move forward inspite of COVID. As a result, the unpreparedness and with less knowledge of virtual platform which lead to misconfiguration of security in VPN by which the sensitive information of the organizations is exposed to internet and to further exposing the user device to the DoS (denial of Service) cyber-attacks. In addition to this some of the students and employees will be using their own personal deceives to attend their official works which in turn poses grater amount of risk to the organization and the user.

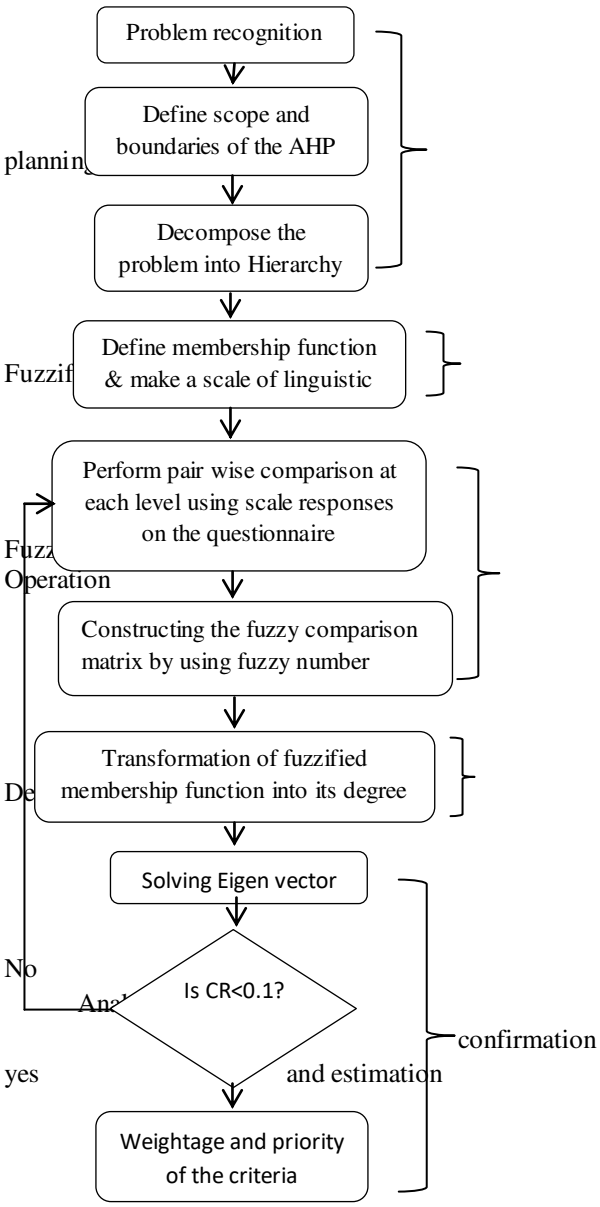
2. Impact Related Phishing &Ransomwarecyber attacks:
The hackers used the COVID-19 as the temptation to mask up and resemble the brands and attack the employees and other users. This type of attacks more porn to the devices like computers and phones which are more contaminated. Other than the organization other end users are also targeted who may download the application related to the preventing COVID-19 which often fools installing ransomware disguise as the legitimate application. Hence the organizations should instruct the employees to not to get attracted to the dominating mails which are COVID related links, emails or downloads. There by company should insure that their identity and warning capabilities are in hold and should keep an eye on impacts of remote working employees.

3. Potential Delays in Cyber-Attack Detection and Response:
Because of the COVID-19 the several functioning security terms are likely to be compromised which makes difficult to identify the various harm causing activities and also more difficulty in responding to that activities. This also leads to problem in updating the patch if terms of security are not operational. The organization should be in place of defending the security breach with the help of co sourcing from external consultants should be explored.

4. Cyber-attacks on healthcare organization:
Due to the pandemic one of the main target is the health sector. This attacks mainly on healthcare organizations, pharmaceutical organizations and research industries. Health care organizations are more vulnerable to ransomware cyber-attacks due to the limited budget on their IT security system. Which lead them to use the outdated software which will be having high risk of cyber-attacks? The rules from United Kingdom's National Cyber Security Centre (NCSC) and also the u. s. Department of Homeland Security (DHS) Cyber Security and Infrastructure Security Agency (CISA) provides the difficulty on phishing, malware, the tools employed in WFH like zoom. Cyber-attack on hospital and healthcare organization as top hacker trend in 2020, as monthly cyber-attack per healthcare organization jumped to 37% in the last 12 months.

2. METHODLOGY

Flow chart of fuzzy AHP method



Protecting the system in advance from the attack with advanced techniques is the best way to secure our system from attackers. This estimated security would come from prioritizing the security issues during the pandemic. Multi-criteria community decision-making (MCDM) problems are widely in practice in order to satisfy customer needs. AHP is the better method for analyzing the attributes of variables than any other MCDA method. AHP along with fuzzy is a powerful method of evaluating difficult decision-making context and gives a specific graded target rate that determines the complicated problem. AHP method uses only the pair-wise review matrix to resolve the inaccuracy of multicriteria decision labeling challenges. The model projected here makes it possible to use triangular fuzzy figures to define linguistic parameters and integrate fuzzy procedures with AHP. There are 6 steps in to get decision result.

Step 1: Recognize the problem and identify the attributes. Fuzzy-AHP method to test the pandemic's most prioritized impacts. Here impacts of COVID-19 pandemic are analyzed. 50 domain expert discussed and rank the impacts among them finally gathered the data according to their perspective.

The next stage is to build the Triangular Fuzzy Number (TFN) from the Tree Hierarchy. With the support of one factor's impact on the other factor, a pair-wise evaluation of each category of specified goal plays a key role. TFN, which ranges from 0 to 1. Accurate statistics are graded as 1,2, …… 9. As per the scale given to the variables that affect the scores in a numerical way, the experts awarded the points.

Step 2: The next step is to create the fuzzy comparison matrix according to the flow chart.

Step 3: The next step is the transformation of the fuzzified values into their degrees and the resolution of their own values.

Step 4: The next move is to check if the CR is below 1 or not. The values are defuzzified if CR concludes less than 1, and the final results are determined, otherwise the pair-wise matrices are reconstructed and calculations are performed again if the CR is less than 1.

Step 5: Final results of the weights of all the attributes help to determine the attribute with the highest priority, and the attribute with the least priority. Here, the attributes are COVID-19 results, hence the highest and the lowest impact is determined at the end. Finally displays the complete weights and priorities of the models.Prioritization of the models in the descending orderof covid-19 impacts: I4>I3>I2>I1.

3. RECENT CYBER-ATTACKS AT THE TIME OF COVID-19

2020 is considered as the worst year with increase in total number of records of cyber-attack. 1st three months the number is added with count of 8.3 billion bringing the total number to 36 billion at the end of the September. In the first three quarter of 2020, 21% are reported breaches which involve ransomware. Some of the recent worldwide attacks at the time of corona virus are briefed below.

As per the record of Kaspersky,93 number of malware related to COVID-19 are recorder in Bangladesh, 40 recorded in China, 53 number of attacks in Philippines, 22 in India, 23 in Vietnam, 20 in

Malaysia in the 1st quarter of 2020. Many email scams are recorded at the time of COVID-19 impersonating with the same of WHO. According to the report from WHO on 23rd of April 2020 there was about 450 active email IDs along with the passwords of access have been exposed in coronavirus pandemic. Zoom meeting app have become the most popular application at the time of April and about 500,000 mail and the passwords have been exposed are up to sail on dark web. This was not only in zoom, goggle, Microsoft video conference applications are most porn for the cyber-attack by sending fake URL phishing like "You have added to a Google meeting" over 192,000 breaches are recorded. The well-known hacking of twitter accounts of reputed persons on July 15 which referred as $2000 for $1000 from unknown Bit coin address which lead about $121,000 was transferred. When COVID-19 was peaked on April 2020 the ransomware attack which made to stuck in Magellan Health and over 365,000 patients were affected in the sophisticated cyber-attack.

4. SOME OF THE PREVENTIVE MEASURES TO PREVENT CYBER-ATTACKS.

Different measures can be taken by the organization to prevent the successful cyber-attack. One of the most outstanding solutions to maintain the security during COVID-19 is to implement secure infrastructure. The main reason to attack start-ups and small-scale business is lack of necessary security infrastructure. To control this attack and data breach company need to implement strong security policy. Some security measures must be followed to protect the organization data are:

- **Provide limited employee access to the company data:** Main reason of successful attack is due to employee carelessness or intentionally exposing the data. Therefore in order to secure the data organization as to restrict the data access to limited employees. Data has can be assessed by the employees depending on priorities of duty. Only top management of the organization access sensitive informationin order to secure the data. Reducing data access leads to avoid successful attack.

- **Regular updating patching of the system with the updated software:** Manufacturer of the organization gives regular operating system and software updates to enhance security. Because as time passes available security measure are not enough to secure data. Hence organization updates the operating system and software to enhance the security.

- **Backing up the all the data to the hard disk before sharing to the other cloud networks:** Backup of data is one of secure way of protecting the sensitive information or data that is being stolen or encrypted by the attacker. If any disaster or ransomwareattacks occur we don't need to pay ransom to the attacker to decrypt it because we have back-up of data.

- **New cyber risk occurring during covid-19 pandemic must be understood:**Security management team must determine their security policy and techniques can able to prevent the current cyber-attack where everyone shifted to work from home environment.

- **Advanced technologies must be deployed:** Advanced technology must be deployed with advanced technique of bigdata, Al, and machine learning which involves threat detection and prevention technique. This technique does not involve human intervention to detect and prevent.

5. CONCLUSION

New age in cyber-security has been created during the COVID-19 pandemic. Bad actors in cyber space have taken an advantage in targeting the vulnerable peoples and IT assets. Health care organizations became a major target for most of the cyber-criminals during the pandemic. Hence it is very important for the health care organization to protect the important data by improving the security for their data and assets. During this condition employees of many organizations started to work from home. Employees can easily become a pray for the attacker due to lack of security measure at home. This report analyses the impact and prioritize the impacts using MCDM procedures. The outcomes of the final result can be used by any practitioner to establish guidelines for fraudsters to secure apps and mobile applications in this pandemic. In the list of 4 impacts, the most prioritized impact is cyber-attack on health care organization. Automated instruments, decision analysis, Fuzzy-AHP for computation and dynamic analysis, which play an important role in pandemic management, are also included in the proposed prioritization model. To monitor the distribution of COVID-19 impacts, the Fuzzy-AHP tool is used to prioritize based on the available results. Hence every organization has to implement and adopt security policy to analyze andprotect themselves from cyber-attack.

6. REFERENCES

- McKinsey & Company, "COVID-19 Crisis Shifts Cybersecurity Priorities and Budgets." 2020. [Online].Available: https://www.mckinsey.com/business-functions/risk/our-insights/covid-19-crisis-shifts-cybersecuritypriorities-and-budgets#.
- TCS Worldwide, "How COVID-19 is Dramatically Changing Cybersecurity." 2020. [Online]. Available:

https://www.tcs.com/perspectives/articles/how-covid-19-is-dramatically-changing-cybersecurity.

- OrangeCyberDefense, "A Biological Hazard Goes Digital." 2020. [Online]. Available: https://orangecyberdefense.com/global/white-papers/covid-19-a-biological-hazard-goes-digital/.
- Deloitte, "COVID-19's Impact on Cybersecurity," 2020. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/ng/Documents/risk/ng-COVID-19-Impact-on-Cybersecurity-24032020.pdf.
- S. N. Brohi, N. Z. Jhanjhi, N. N. Brohi, and M. N. Brohi, "Key Applications of State-of-the-Art Technologies to Mitigate and Eliminate COVID-19," 2020.
- S. Perez, "Videoconferencing apps saw a record 62M downloads during one week in March," 2020. [Online]. Available: https://techcrunch.com/2020/03/30/video-conferencing-appssaw- arecord-62m-downloads-during-one-week-in-march/. [Accessed: 05- Sept.-2020].
- Managing the impact of COVID-19 on cyber security. https://www.pwc.com/jg/en/topics/covid-19/managing-impact-of-covid-19-on-cyber-security.html .
- B.Vigliarolo, "Who has banned Zoom? Google, NASA, and more," 2020. [Online]. Available: https://www.techrepublic.com/article/who-has-bannedzoomgoogle-nasa-and-more/. [Accessed: 04-Sept.-2020].