COVID-19 PANDEMIC: A NEW ERA OF CYBER SECURITY THREAT AND HOLISTIC APPROACH TO OVERCOME

Jabber Ahmed
Major, Signal Base Workshop, Bangladesh Army
Dhaka Cantonment, Dhaka, Bangladesh
Email: jas7040@gmail.com

Quddus Tushar
School of Engineering, RMIT University,
GPO Box 2476, Melbourne VIC 3001, Australia
Email: quddus.tushar@rmit.edu.au

2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE) | 978-1-6654-1974-1/20/$31.00 ©2020 IEEE | DOI: 10.1109/CSDE50874.2020.9411533

***Abstract*— In this paper, we present cyber security threat created worldwide has been discussed during the current COVID-19 situation. To stop the spread of Coronavirus, almost all the countries of the world declared lockdown. People are now doing their office, schooling, and business remotely. For that reason, the use of computers and the internet has increased a lot and made cyber criminals more active. Recently the number of cyber-attacks has increased a lot, and everyone has become a target the cyber criminals. Lack of personal safety precautions in using the internet is causing significant damage to everyone. COVID-19 has made it easy for cyber criminals to have easy access to everyone's data. Many banking sectors and government and non-government organizations have faced several cyber-attacks during this time. This paper focuses on some safety precautions to safeguard the personal and organizational data from cyber criminals.**

***Index Terms* — COVID-19, Cyber-attack, Phishing, Malware, DDoS Attack, Ransomware.**

I. INTRODUCTION

COVID-19 has already defined the year 2020 with its rage, and the whole world is suffering from its spread. Almost all the countries are under lockdown, and governments ordered natives to continue their day-to-day work staying at home. A maximum of airports and borders were closed to stop the spread. This COVID-19 pandemic has been forced to implement a 'New Normal' by forcing people to work from home. People from all the sectors, including the students, are doing their office, maintaining the business, and attending the classes remotely. In this situation, information and communication technology is playing a vital role in fulfilling the requirements [1]. Besides this online business, food delivery and day-to-day items' demand through the internet and mobile applications got priority to everyone, making them vulnerable to cyber attackers. Almost all the continents are facing cyber security threats in recent times. Research on the Cyber-attacks in 2020 due to this pandemic is shown in Figure 1.

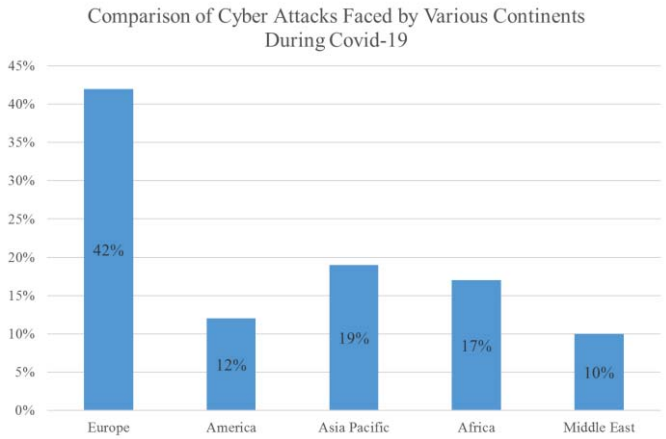

Figure 1 Cyber Attacks faced by Various Continents

Cyber criminals are utilizing this situation to capitalize on their evil motives, and cybercrimes are increasing day by day. Thus, cyber security threats are developing and becoming a more significant concern for the world community [2]. Especially for developing countries, cyber security threat has become a prime concern. Due to a lack of awareness, many sites have been visited by the people without security precautions. These are possible causes to be affected by various cyber security threats. Plausible threats are shown in Figure 2.

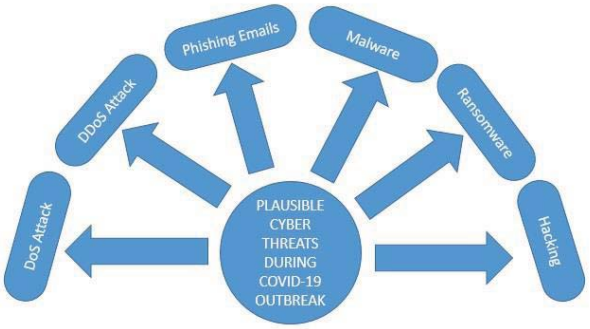

Figure 2 Plausible Cyber Threats during COVID-19 Pandemic

The study has organized the rest of the paper as follows. Past related works are described in Section II, where the works were carried out in the recent past on cyber threats during the pandemic period. Sectors that may face cyber-attack and credible cyber threats that may be encountered during this pandemic are briefly explained in Section III. A holistic approach to overcome the cyber security threat is shown in Section IV. Finally, the conclusion is driven by the authors and delivered in Section V.

II. Related Works

Khan et al. proposed ten deadly cyber threats including ransomware and phishing, and also discussed the privacy concerns [1]. It also recognized very few sectors that seem to be affected by the cyber-attacks during this pandemic. Király et al. described how Information Communication Technology (ICT) helped the general mass reduce psychological stress during this pandemic situation [3]. The paper focused on using ICT to communicate with friends and family and termed ICT as "Savior". But on the other hand, addiction to ICT, like gambling and viewing pornography, was shown as malicious use and may cause a cyber threat to the user. Lallie et al. presented the cyber-attacks analysis during the COVID-19 outbreak era with a case study where it described how the cyber criminals utilized the government announcement to design their cybercrime [4]. Williams et al. described that the cyber security cost will increase fivefold by the year 2021 after the COVID-19 pandemic [5]. It emphasized the healthcare sector, where the cyber threat had a tremendous impact during the epidemic. According to the study, the cyber criminals target the patients' credentials, which may have a long-term effect. Abukari et al. proposed some hygienic protocols for those working from home to ensure proper cyber security [6]. These protocols may guide the users to keep them safe from cyber-attacks during this pandemic.

III. Affected Sectors and Plausible Threats

Presently COVID-19 pandemic has changed the whole world. The usage of the internet on laptops and other mobile devices has increased a lot with the abundance of various mobile applications, which helped raise cyber threats' vulnerability. Recently various government and non-government organizations face cyber-attacks in terms of losing organizational data, including personal data theft. People are using online platforms to buy multiple airline tickets, order foods, and pay numerous utility bills using their credit/debit cards. Cyber criminals are targeting these platforms to collect personal credentials for their monetary benefit [7].

This pandemic has forced people to work from home. Zoom is one of the very famous applications nowadays for attending online conferences and classes. Zoom has become a new target for cyber criminals. They used "Zoom bombing" to collect users' data and may eavesdrop to listen to any conversation of ongoing meetings in Zoom. One cyber security forum is also found that almost 50,000 Zoom accounts are on sale for hackers on the dark web [2]. Likewise, Google Duo, Microsoft Team are all becoming vulnerable to cyber-attacks during this pandemic. The following sectors are mostly affected by cyber-attacks / cyber security threats during this COVID-19 pandemic.

A. Affected Sectors

Almost all the sectors are under continuous cyber security threats during this COVID-19 situation. In this part, the most affected sectors are described.

1) ***Healthcare and Medical Sectors.*** Hackers and intruders know that the healthcare system of the world is a mess during this pandemic. As more people are using the remote care system, thus, for having some financial gain, the hackers are very active in getting access to the healthcare system around the world. According to The UK's National Cyber Security Centre (NCSC) and the US Cybersecurity and Infrastructure Security Agency (CISA), the hackers are trying to get access to a large number of personal data and accounts of the patients and are sending them phishing emails [4]. World Health Organization (WHO) declared that the cyber-attack during this COVID-19 was increased five-fold, which is a concern for the public. During the third week of April 2020, almost 450 active email addresses with a WHO password were leaked [8]. Telemedicine has become the only way to get treatment during this pandemic. The treatment has made the approach more accessible for hackers to collect the individual patient's desired information. In New York, only daily 95 persons used to take the help of telemedicine before the pandemic. During the epidemic, the number of patients has been increased by 4330%, and on average, almost 4209 people took telemedicine support daily. These incredible increasing numbers have caused ransomware attacks [9].

2) ***Financial Sectors.*** Financial sectors have suffered many cyber security challenges during the ongoing COVID-19 situation. It has forced the financial sectors to continue providing online support to their clients. Again, maximum employees did their office work from home using the unsecured network. When the employees are doing their jobs in office, they are adhered to by some security policies, including cyber security, which was absent during the 'New Normal'. The use of an unsecured network made the employees more vulnerable to cyber threats [10]. Nowadays, clients are also dependent on internet banking, and that makes them vulnerable to hackers. Phishing, Distributed Denial of Service (DDoS), Malware are common attacks made by hackers on the financial sectors.

3) ***Educational Sectors.*** Educational facilities suffered a lot due to the sudden change caused by the COVID-19 pandemic. Students from all levels are now dependent on e-learning, which makes them vulnerable to cybercrimes. For the e-learning process, most of the educational institutions are dependent on applications like Zoom. Some schools in California were forced to shut down their activities for a few weeks for the malware attack [11].

B. *Plausible Threats*

Threats can be of various types. But the most threats faced during this COVID-19 are described as follows:

1) ***DDoS Attack.*** The DDoS attack is one kind of attack that is used to make an online service unavailable for the users by increasing the number of traffic. The DDoS attack has increased three times in the last three months than that of the previous. In the first quarter of the year 2020, the total number of reported DDoS attacks was 242, and in the second quarter, the number was increased to 300 [12] [13].

2) ***Phishing.*** Hackers try to exploit individuals by sending them phishing emails. These emails contain fake webpages and can capture the details of an individual. As most people are now dependent on online platforms during this pandemic; thus, they are becoming vulnerable to these phishing attacks. During March 2020, amongst 4,67,825 phishing emails, a total of 9,116 were related to COVID-19, which is almost 02% of the total phishing emails [14]. There are various types of Phishing attacks like phishing over email, malicious websites, and phishing over the phone (also known as vishing). Types of phishing attack that was conducted during this pandemic, including their percentage, are shown in Figure 3.

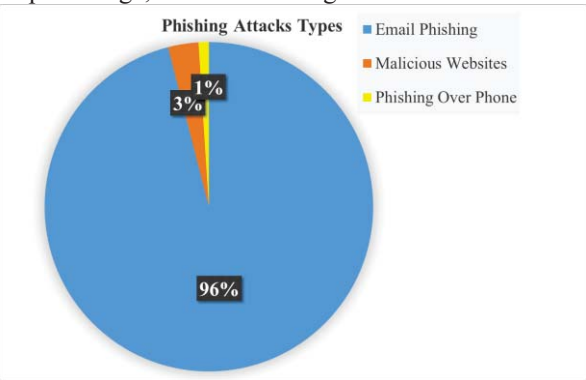

Figure 3 Various Types of Phishing Attacks

3) ***Malware.*** During this pandemic, the cybercriminals are spreading malware in the devices of the users. Malware can create backdoor in user's devices and by which cyber criminals take all the personal credentials / password. Few online Corona tracing maps are spreading this malware [15].

4) ***Ransomware.*** Ransomware attacks increased a lot during the pandemic as remote working has increased. The cyber criminals have chosen this attack for their financial gain. Especially the financial sectors are the main target for ransomware attack. The ransomware attack has a 148% spike during the first half of this pandemic [16].

IV. HOLISTIC APPROACH TO OVERCOME CYBER THREATS

Our life is now at a stack due to the COVID-19 pandemic. People are mental stressed to follow the stay at home rule and are trying to reduce their stress through online activities. On the other hand, the cyber criminals are also more active than ever and utilize this stressed situation to achieve their financial goals. The reluctance on the Cyber security knowledge on the user end creates more chances for the cyber criminals to gain access to the users. Cyber-attacks are creating the situation more tense and becoming a concern for all.

To prevent cyber-attacks, at first, we need to detect and identify them. Before connecting to any network, the following steps can be taken to keep the device safe from the intruders to take control over it.

A. *Initial Steps to Prevent Cyber-Attacks.*

1) Step1: Devices must have updated anti-virus software.
2) Step2: Keep the firewall on your device.
3) Step3: Do not use any pirated software.
4) Step4: Stop visiting unknown websites that may contain phishing content.
5) Step5: Never keep your username and password saved in the browser.
6) Step6: Do not open any email links till you are sure.
7) Step7: Try to site those security certified (Websites starting with 'https://' is safe).
8) Step8: Never save your credit/debit card number to your browser.
9) Step9: Go through the website address and be sure about the address (Is it a phishing site?) before complete payment using the credit/debit cards.
10) Step10: Never use the same password to all your accounts.
11) Step11: Passwords must be strong enough and should not match special dates or numbers (Like your birthday, personal numbers).
12) Step12: Use a paid operating system (OS).
13) Step13: Keep your OS updated.

B. *Prevention of Cyber Attacks.*

1) ***Prevention from DDoS Attack.*** To prevent DDoS attacks, the organization must keep the firewall on. Ingress/Egress filtering can help to detect the source IP address range to control the overflow [17].

2) ***Prevention from Phishing.*** Phishing attack has become a new threat to internet users. Cyber criminals send phishing email with a fake website to capture the personal data and uses it to be financially benefited. Phishing can be prevented by the following means

- Adequate knowledge of Phishing emails.
- Do not click on phishing links.
- Do not provide your credentials to unsecured websites.

3) ***Prevention from Malware.*** The use of updated anti-virus devices can reduce the chance of malware attacks. The firmware must be updated according

to the new patch, and the firewall should remain switched on [18].

4) ***Prevention from Ransomware.*** Ransomware is on kind of malware which is hijacking the data from the device only for financial benefit. Updated anti-virus software is the option for the end-users. Updated OS can provide an updated patch file for the prevention of ransomware.

5) ***Prevention from Hacking.*** To prevent hacking following measures can be taken

- Do not share the username and password to anyone.
- Passwords should be strong enough so that it cannot be guessed easily.
- Account details are not to be shared.

C. *Imparting Adequate knowledge on Cyber Threat.*

In present scenario, everyone must have adequate knowledge on cyber security threat. But unfortunately, maximum people are unaware of this topic and many of them are not even familiar with the plausible cyber threats. This is creating a vacuum in preventing the cyber-attacks and cyber criminals are taking this as an easy way to fulfill their ill motives. A survey was carried out to judge the knowledge of mass people on cyber threats on a hundred people. The result is shown in Table 1.

Table 1 Survey Report Based on Few Questionaries'

Question	*Correct Answer*	*Incorrect Answer*
What is Phishing?	27%	73%
What is DoS and DDoS attack?	21%	79%
What is Malware?	18%	82%
What is Ransomware?	22%	78%
What is Hacking?	36%	64%

Considering the above survey result, it is clear that mass people are not aware of these topics and imparting knowledge to them on cyber security has become must. Different organizations (both Government and Non-Government) should plan to educate their employees on cyber security threats by arranging training or workshop to ensure the security of the organization. Mass people should also try to gather minimum knowledge on cyber security threats to keep themselves safe from losing their personal information.

V. CONCLUSION

The study has tried to focus on the present cyber threats amid the COVID-19 pandemic. This pandemic has seen the maximum use of the internet ever. People from all parts of the world continued their communication, jobs, and education through this internet. This pandemic has also tested the stress level of everyone. The Internet has also helped people to minimize their stress levels. This pandemic has proved that people can work, continue classes and all other activities even staying at home. Cyber criminals have taken this chance to exploit this extensive use of internet by the mass people to capitalize on his benefit. Cyber security threats had increased a lot during this pandemic due to the ignorance of cyber security knowledge.

At all levels, we must have minimum knowledge of cyber security threats and plausible cyber-attacks. Different government and non-government organizations are affected by cyber-attacks. Therefore, it has become a foremost requirement to impart minimum knowledge on cyber security for every employee to safeguard from losing important information to cyber criminals.

COVID-19 is just the beginning. The world may face more and more viruses like this in the future. So, it is time to start planning for the future. We all should take the lessons from the COVID-19 pandemic and may prepare ourselves for the future so that Cyber Security may not bring any more trouble for the world.

REFERENCES

[1] N.A. Khan, S.N. Brohi, N. Zaman, Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic, (2020).

[2] I.C. Eian, L.K. Yong, M.Y.X. Li, Y.H. Qi, Z. Fatima, Cyber Attacks in the Era of COVID-19 and Possible Solution Domains, (2020).

[3] O. Király, M.N. Potenza, D.J. Stein, D.L. King, D.C. Hodgins, J.B. Saunders, M.D. Griffiths, B. Gjoneska, J. Billieux, M. Brand, Preventing problematic internet use during the COVID-19 pandemic: Consensus guidance, Comprehensive Psychiatry (2020) 152180.

[4] H.S. Lallie, L.A. Shepherd, J.R. Nurse, A. Erola, G. Epiphaniou, C. Maple, X. Bellekens, Cyber security in the age of COVID-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic, arXiv preprint arXiv:2006.11929 (2020).

[5] C.M. Williams, R. Chaturvedi, K. Chakravarthy, Cybersecurity Risks in a Pandemic, Journal of Medical Internet Research 22(9) (2020) e23692.

[6] A.M. Abukari, E.K. Bankas, Some cyber security hygienic protocols for teleworkers in COVID-19 pandemic period and beyond, International Journal of Scientific & Engineering Research 11(4) (2020) 1401-1407.

[7] J. Wakefield, Zoom boss apologises for security issues and promises fixes, BBC,[online] Available at:< https://www. bbc. com/news/technology-52133349>[Accessed 15 May 2020] (2020).

[8] W.H. Organization, WHO reports fivefold increase in cyber attacks, urges vigilance, April, 2020.

[9] M. Jalali, A. Landman, W. Gordon, Telemedicine, privacy, and information security in the age of COVID-19, Available at SSRN 3646320 (2020).

[10] E. Babulak, J. Hyatt, K.K. Seok, J.S. Ju, COVID-19 & Cyber Security Challenges US, Canada & Korea.

[11] A. Harris, M. Jones, COVID 19–school leadership in disruptive times, Taylor & Francis, 2020.

[12] S. Wu, Y. Chen, M. Li, X. Luo, Z. Liu, L. Liu, Survive and

Thrive: A Stochastic Game for DDoS Attacks in Bitcoin Mining Pools, IEEE/ACM Transactions on Networking 28(2) (2020) 874-887.
[13] S. Mansfield-Devine, The growth and evolution of DDoS, Network Security 2015(10) (2015) 13-20.
[14] R. Naidoo, A multi-level influence model of COVID-19 themed cybercrime, European Journal of Information Systems (2020) 1-16.
[15] S. Hakak, W.Z. Khan, M. Imran, K.-K.R. Choo, M. Shoaib, Have you been a victim of COVID-19-related cyber incidents? Survey, taxonomy, and mitigation strategies, IEEE Access 8 (2020) 124134-124144.
[16] J.P. UPATHAM, J. Treinen, Amid covid-19, global orgs see a 148% spike in ransomware attacks; finance industry heavily targeted, 2020.
[17] V.E. Balas, R. Kumar, R. Srivastava, Recent Trends and Advances in Artificial Intelligence and Internet of Things, Springer2020.
[18] M.P. Gounder, M. Farik, New Ways To Fight Malware.