Proceedings of National Conference on "Emerging Trends and Recent Innovations in Engineering and Technologies" held at Nagarjuna College of Engineering and Technology, Bangalore on 22 and 23 April 2022

COVID-19 PANDEMIC: A HOLISTIC APPROACH TO OVERCOME A NEW ERA OFCYBER SECURITY THREAT

Ms. Prathibha B N, Mrs. Bhavya R A, Mrs. Swathi N, Mrs.Vidhyashree B
Dept. of Computer Science & Engineering
Nagarjuna college of Engineering and Technology, Bangalore, India
prathibha.bn@ncetmail.com, bhavya.ra@ncetmail.com, swathi.n@ncetmail.com, vidyashree.b@ncetmail.com

ABSTRACT

We offer a worldwide network safety risk that has been considered during the current COVID-19 circumstance in this article. Pretty much every country in the globe has announced lockdown to forestall the spread of Corona virus. Individuals these days telecommute, go to class, and carry on with work. Thus, the utilization of PCs and the web has risen significantly, expanding the quantity of digital cheats. The recurrence of digital assaults has risen significantly lately, making everybody an objective for digital cheats. Everybody is enduring because of the absence of individual wellbeing strategies while utilizing the web. Cybercriminals currently have basic admittance to everybody's information because of COVID-19. A few digital assaults have been sent off against the monetary business, as well as government and non-government elements, over the course of this time. This paper examines a few safety efforts that can be taken to safeguard individual and authoritative information from digital assailants.

Index Terms — COVID-19, Phishing, Malware, DDoS Attack, and Ransomware are all terms used to describe cyber-attacks.

I. INTRODUCTION

Corona virus anger has previously portrayed the year 2020, and the whole world is enduring because of its multiplication. Pretty much every nation has been put under lockdown, and residents have been told to keep functioning as expected at home. To stop the spread, the greatest number of air terminals and lines were halted. Due to the COVID-19 pandemic, individuals have been constrained to telecommute, making "Another Normal." People from many different backgrounds, including understudies, are telecommuting, maintaining their organizations, and going to classes. In this specific situation, data and correspondence innovation (ICT) is basic to addressing the necessities. Aside from this web-based organization, everybody focuses on food conveyance and everyday things through the web and versatile applications, making them helpless against digital assaults. Lately, practically all landmasses have been exposed to network protection concerns. Figure 1 portrays, in 2020, digital assault exploration will be directed because of the pestilence.

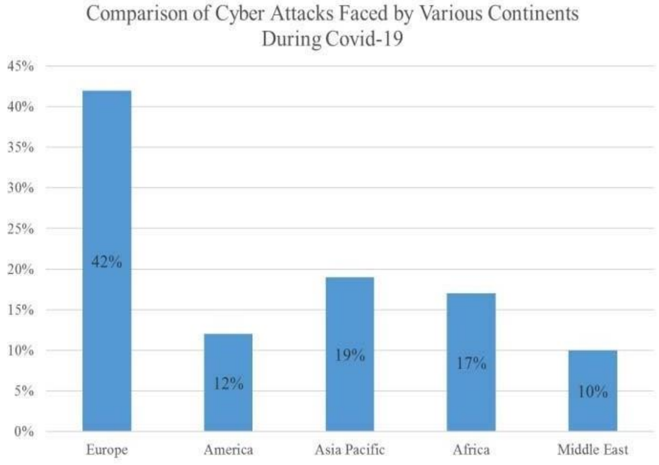

Figure 1 Cyber Attacks on Different Continents

This is being taken advantage of by cyber thieves.

Cyber criminals are taking advantage of the circumstances to further their nefarious goals, and cybercrime is on the rise. As a result, dangers to cyber security are evolving as well as growing as a global issue. Cyber security has become a major worry for underdeveloped countries in particular. Many people have visited sites without taking security precautions because of a lack of information. These are some of the ways that cyber security threats might affect you. Figure 2 depicts possible threats.

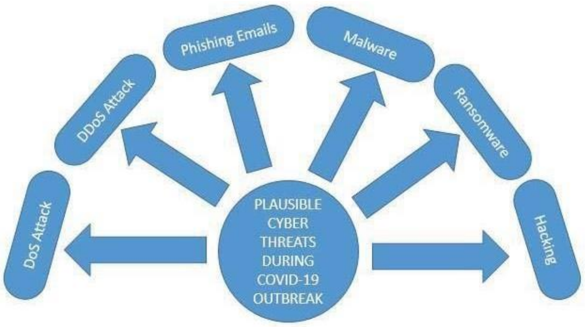

Figure 2 Cyber Threats in the Event of a COVID-19 Pandemic

II. DAMAGED ZONES AND POSSIBLE RISKS

The present Corona virus pandemic has thrown the whole planet into disarray. With the wide range of mobile applications available. The utilization of the web on workstations and other cell phones has expanded immensely. Expanding the weakness of digital dangers, A few government and private associations have as of late been casualties of digital assaults that brought about the robbery of classified data. including the burglary of individual data. People use online platforms to purchase several plane tickets., They use their credit/debit cards to place restaurant orders and pay various utility bills. Cyber criminals are attacking these networks in order to obtain personal information in exchange for money.

As a result of the pandemic, some have needed to telecommute.. Nowadays, Zoom is a well known instrument for going to online gatherings and workshops.. Zoom has turned into another objective for digital crooks. They utilized "Zoom besieging" to gather client information and might be tuning in on continuous Zoom meetings. On one network protection gathering, around 50,000 Zooms were distinguished. On the dim web, programmers can trade accounts. Likewise, during the pandemic, Both Google Duo and Microsoft Team are powerless against hacking. The accompanying businesses are the most defenseless against digital assaults and network safety worries during the COVID-19 pandemic. Impacted Sectors, Almost all areas are continually under network safety dangers in the current COVID-19 circumstance. This segment examines the ventures that have been the most impacted.

The medical and healthcare industries. Programmers and trespassers are completely mindful that the episode has tossed the overall medical care framework into bedlam. Programmers are turning out to be more dynamic in accessing medical services networks all around the world as more people utilize the remote consideration framework monetary advantage. As indicated by the UK's National Cyber Security Center (NCSC) and the US Cyber security and Infrastructure Security Agency (CISA), programmers are endeavoring to acquire admittance to an enormous number of individual information and patient records. Digital assaults expanded five-crease during COVID-19, as per the World Health Organization (WHO), comprising a general wellbeing concern. Almost 450 dynamic email accounts with a WHO secret key were uncovered during the third seven day stretch of April 2020. During this pandemic, telemedicine is the main means to get treatment. The treatment has made it more straightforward for programmers to acquire the required data from every individual patient. Prior to the pandemic, telemedicine was just utilized by 95 individuals every day in New York. During the flare-up, the quantity of patients expanded by 4330%, and all things considered, almost 4209 individuals utilized telemedicine consistently. Because of these shocking numbers, ransomware assaults have expanded.

Financial Industries. A few network protection weaknesses have emerged in the monetary business because of the continuous COVID-19 circumstance. Monetary firms have been compelled to keep giving web-based client assistance subsequently. Most of representatives telecommuted on an unprotected organization. Representatives are held to specific working environment security principles, including digital protection, which didn't exist during the 'New Normal.' When workers utilized an uncertain organization, they were more helpless against digital assaults. Clients' dependence on web banking is developing, setting them at risk of being hacked. Phishing, dispersed disavowal of administration (DDoS), and malware are well known assaults on the monetary area. monetary enterprises.

Categories of Education The COVID-19 pandemic caused ruin on instructive establishments with its abrupt change. E-learning is turning out to be more famous among understudies at all levels, putting them at risk of cybercrime. To make the e-learning process simpler, most instructive foundations use programs like Zoom. A few California schools had to close for half a month because of the infection flare-up.

Threats that are Real

1) Threats happen in various sorts and sizes. Nonetheless, coming up next are the main risks during COVID-19:

2) A DDoS (Distributed Denial-of-Service) assault. DDoS assaults are one kind of attack that makes an internet based assistance inaccessible to clients by expanding traffic. DDoS assaults are expanding threefold over the most recent three months contrasted with the past 90 days. In the primary quarter of 2020, there were 242 DDoS attacks and 300 in the second.

3) Phishing emails are used by hackers to take advantage of people. These emails contain bogus websites that can be used to steal personal information. Because the majority of people are increasingly reliant on online channels to cope with the pandemic, they are exposed to phishing attempts. COVID-19 was linked to a total of 9,116 phishing emails in March 2020, accounting for nearly 2% of all phishing emails. Phishing assaults come in a variety of forms, including email phishing, rogue websites, and phone phishing (also known as vishing).

Threats that are Real

1) ***Malicious Software:*** Cybercriminals are spreading malware through users' devices during this outbreak. Malware can install a backdoor on a user's device, allowing cyber thieves to steal all of the user's personal information. This malware is propagated using a few online Corona tracing maps.

2) ***Ransomware.*** As the number of people working remotely rose during the pandemic, ransomware attacks increased dramatically. The cyber thieves have selected this attack as a means of making money. The financial sector, in particular, is a prime target for ransomware attacks. During the first half of the pandemic, ransomware attacks increased by 148 percent.

II. A HOLISTIC APPROACH TO DEFEATING CYBERTHREATS

The COVID-19 pandemic has thrown our lives into chaos. People are mentally agitated by the requirement to keep themselves at home and are attempting to relieve their anxiety by participating in internet activities. Cyber crooks, on the other hand, are busier than ever, and they're taking advantage of the pressure to attain their financial objectives. Because people are hesitant to learn about cyber security, cyber thieves have more opportunities to obtain users' permission information. Attacks on the internet are on the rise escalating the issue and causing everyone to be concerned.

First, we must detect and identify cyber-attacks in order to avoid them. The following procedures can be followed before connecting to any network to protect the gadget from attackers who could try to take control of it.

A. First Steps in Preventing Cyber-Attacks

1) All gadgets should have modern antivirus programming.
2) Keep your gadget's firewall dynamic.
3) Don't use any product that has been pilfered.
4) Avoid getting to new sites that might incorporate phishing material.
5) Your login and secret word ought not be saved in your program.
6) Make sure you're certain prior to clicking any email joins.
7) Look for security-affirmed sites (those that start with the letters "https://" are protected).
8) Your credit or charge card number ought not be saved in your program.
9) Before making a credit/charge card installment, twofold check the site address (is it a phishing site?)..
10) Never utilize similar secret phrase for a considerable length of time.
11) Passwords ought to be long and contain no abnormal dates or digits (Like your birthday, individual numbers).
12) Purchase a working framework (OS).
13) Make sure your working framework is cutting-edge

B. Defending Against Cyber-Attacks

1) DDoS Attack Protection. The organization's firewall must be turned on to avoid DDoS attacks. Ingress/Egress filtering can assist control the overflow by detecting the source IP address range.

2) Prevention from Phishing. Phishing attacks have emerged as a new online hazard. Cyber thieves send phishing emails containing a false website in order to collect personal information and profit from it. The following methods can be used to avoid phishing:

- Familiarity with phishing emails is required.
- Don't click on phishing links, and don't give up your passwords to unprotected websites.

3) Prevention from Malware. Malware assaults can be diminished by utilizing around date against infection programming. The firewall should be empowered and the firmware should be refreshed to mirror the current fix .

4) Ransomware protection. Ransomware is a type of virus that takes control of a device's data only for the purpose of making money. End-users might choose to install updated anti-virus software. A patch file for ransomware prevention can be downloaded from an updated OS.

5) Prevention from Hacking. The steps below can be followed to prevent hacking.

- Don't tell anyone else your login and logon.

- Logon should be difficult to guess.

- No information about your account should be shared with anyone else.

C. Providing sufficient information on Cyber attacks.

In today's world, everyone needs to be well-versed in the threat of cybercrime. However, the vast majority of people are uninformed of this issue, and many are oblivious of the potential cyber hazards. This is generating a void in terms of preventing cyber-attacks, and cyber criminals are using it to further their nefarious goals. On a hundred persons, a survey was conducted to assess their level of knowledge about cyber dangers.

To safeguard the security of the association, various organizations (both government and private) ought to plan to instruct their staff on digital protection risks by holding preparing or studios. To try not to lose their own data, the overall population should try to advance however much as could reasonably be expected about digital protection concerns.

CONCLUSION

The research was carried out during the COVID-19 epidemic attempted to focus on current cyber risks. The usage of the internet has never been higher than during this outbreak. The internet allowed people from all around the world to keep in touch, work, and learn. Everyone's stress levels have been put to the test by the pandemic. People have also been able to reduce their stress levels thanks to the Internet. This epidemic has shown that people can still work, go to school, and do other things even while they are sick.

Cyber thieves have seized the opportunity to profit from the general public's widespread use of the internet. Due to a lack of cyber security understanding, cyber security threats surged dramatically during this epidemic.

Cyber security dangers and credible cyber-attacks must be understood at all levels. Cyber-attacks damage different government and private institutions. As a result, it has become a top priority to provide every employee with a basic understanding of cyber security in order to avoid losing sensitive data to hackers.

Future Enhancements

Corona virus is only the start up. Later on, the globe might be presented to a rising number of infections like this. So this is the ideal opportunity to begin pondering what's to come. We should all gain from the COVID-19 flare-up and prepare for the impending circumstances so Cyber Safety harm the globe.

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 Psychiatry