



Cyber Threats During COVID-19 Pandemic

Project Thesis

Submitted By

17-33964-1	Afsana Khan
18-36088-1	MD Shoyaib Akhter
18-36131-1	MD Subman Rafid
18-36788-1	MD Raitul Islam Sams

Department of Computer Science

Faculty of Science & IT

American International University Bangladesh

11th August 2022

Declaration

We declare that this thesis is our original work and has not been submitted in any form for another degree or diploma at any university or other institute of tertiary education. Information derived from the published and unpublished work of others has been acknowledged in the text and a list of references is given.



MD Shoyaib Akhter

18-36088-1

CSE



MD Raitul Islam Sams

18-36788-1

CSE



MD Subman Rafid

18-36131-1

CSE



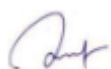
Afsana Khan

17-33964-1

CSE

Approval

The thesis titled “Cyber Threats During COVID-19 Pandemic” has been submitted to the following respected members of the board of examiners of the department of computer science in partial fulfilment of the requirements for the degree of Bachelor of Science in Computer Science on 11-08-2022 and has been accepted as satisfactory.



Mohammad Samawat Ullah

Associate Professor & Supervisor

Department of Computer Science

American International University-Bangladesh



Dr. Kamruddin MD. Nur

Associate Professor & External

Department of Computer Science

American International University-Bangladesh

Dr. Dip Nandi

Asst. Professor & Head (Undergraduate)

Department of Computer Science

American International University-Bangladesh

Professor Dr. Tafazzal Hossain

Dean

Faculty of Science & Information Technology

American International University-Bangladesh

Dr. Carmen Z. Lamagna

Vice Chancellor

American International University-Bangladesh

Acknowledgement

At first, our heartfelt gratitude to Almighty Allah for his terrific bounty, without which we would be unable to complete this thesis satisfactorily. It is an honor to express our gratitude and heartfelt thanks to many different persons for their assistance, supervision, and support in completing this thesis.

Most significantly, our gratitude to our supervisor, Mohammad Samawat Ullah, Associate Professor, Department of Computer Science, AIUB, for his encouragement and support from the beginning to the finish of the thesis. We also thank our external supervisor, Dr. Kamruddin MD. Nur, Associate Professor, Department of Computer Science, for his assistance and presence during our presentation and the advice he has always given us for our presentation progress.

Special thanks to Dr. Carmen Z. Lamagna, Vice-Chancellor, Professor Dr. Tafazzal Hossain, Dean, Faculty of Science & Technology, and Prof. Dr. Mohammed Jashim Uddin, Head, Department of Computer Science, American International University- Bangladesh, for their help, generosity, and encouragement.

Finally, we want to express our appreciation, respect, and warm love to our parents for their unending prayers, assistance, encouragement, and financial support. We are incomplete without them.

Table of Contents

Declaration.....	2
Approval	3
Acknowledgement	4
Tables of Figures.....	6
Abstract	7
Chapter 1: Introduction	8
Chapter 2: Methodology	9
Chapter 3: Industries and Organizations most vulnerable to cyber attacks	11
3.1 E-Health system:	11
3.2 Financial Services	11
3.3 Government and Media Outlets	12
3.4 Educational Institutions.....	13
Chapter 4: Cyber Threats Amidst the Pandemic.....	14
4.1 DDoS Attack	15
4.2 Malicious Domain	15
4.3 Ransomware	16
4.4 Malicious Website.....	17
4.5 Spam Emails.....	17
4.6 Malware.....	18
4.7 Social Media Malware Messaging	19
4.8 Compromising Business Email	20
Chapter 5: Security Breaches	21
Chapter 6: Practical Approach to Reduce Cyber Threats	23
Conclusion	25
References.....	26

Tables of Figures

Figure 1: Flowchart of Research Approach _____	9
Figure 2: Count of Organization Type _____	10
Figure 3: Medical advice for spreading of false information about ibuprofen and COVID-19 _	12
Figure 4: 8 Fatal Cyber Threats During the Pandemic _____	14
Figure 5: Coronavirus Domains Registered Weekly _____	16
Figure 6: Malware and Phishing Sites Visited during Pandemic [20] _____	19

Abstract

Cyber-attack is a common incident nowadays. It is increasing day by day, with the vast use of the internet, modern technology, and the transition from analog to digital. In various organizations and industries, it happens daily. Even on social media, it is a familiar event. There are many types of cyber-attacks. It is an extremely difficult task to identify which cyber-attacks occurred on your system and when it happens. Because providing cyber security is a difficult endeavor that necessitates domain knowledge of assaults as well as the capacity to analyze potential risks. Recently we have passed very tough days because of COVID-19 that time many cyber-attacks take place in different institutions. One of the reasons is that during the covid period every workplace goes online many companies did not have proper knowledge of cyber security. In this report, showed some of the statistical views of different cyber-attacks occurred in different institutions before covid period and during covid period. Our research paper lies in its unique analysis of attacks in the time of covid pandemic. Since using the internet has become necessity for everyone in this pandemic situation, online management will be at risk without an understanding of cyber security. In our research paper, we represent milestone for internet users. We compare two periods of cyber threat during or before. We analyze which types of cyber-attack appear most for the individual institutions. We found which types organization faced the most cyber-attack. We are providing some practical way to reduce the cyber threats while work from home.

Chapter 1: Introduction

COVID-19 has already spread to practically all of country on earth, with more cases and death reports being reported on a daily basis. The primary consequences of that kind of epidemic include a migration from physical to online workspaces. So many of these businesses and organizations have no preparations in solution to handle with such a significant and rapid shift in a really short amount of time [2].

Due to shifting from physical workplace to online workplace many organizations, industries even the educational sector faced the cyber threats. There is a drastic increase of cyber security during this pandemic as most of the global organization experienced the increase of cyber-attacks. Many financial services even the government and media outlets are also the victim.

The rapid spread continuous incubation of coronavirus provides distinct socioeconomic difficulties. However, one beneficial aspect is that it is occurring at a time when communication through online reaches at its pinnacle. The software and devices used for online communication are widely available. It is now feasible to communicate with colleagues, acquaintances, and family members thanks to advancements in technology. Apps like Zoom, Microsoft Teams, GoToMeeting, Google-Hangouts etc. have faced signing up new individuals on regular basis [3]. It is found that video conferencing app zoom is banned in over 20 countries [5]. Many giant companies such as NASA, SpaceX even google banned their employees from using Zoom app [6]. Therefore, it is very significant to understand that this kind of security is harmful that must be avoided. This paper focuses on cyber security threats in various environment during the global pandemic and the practical approach to reduce them.

Chapter 2: Methodology

This paper uses a qualitative descriptive research approach based on secondary data. We collected data from 2012-2020 all over the world, where year of 2019 was reported as the official outbreak of corona in Wuhan, China. Gathering the information and data, we tried to familiar about in which organizations and industries are most in danger during COVID-19 period. With the help of the graphs and data we get to know the most fatal cyber threats that cause negative effects during COVID-19 period.

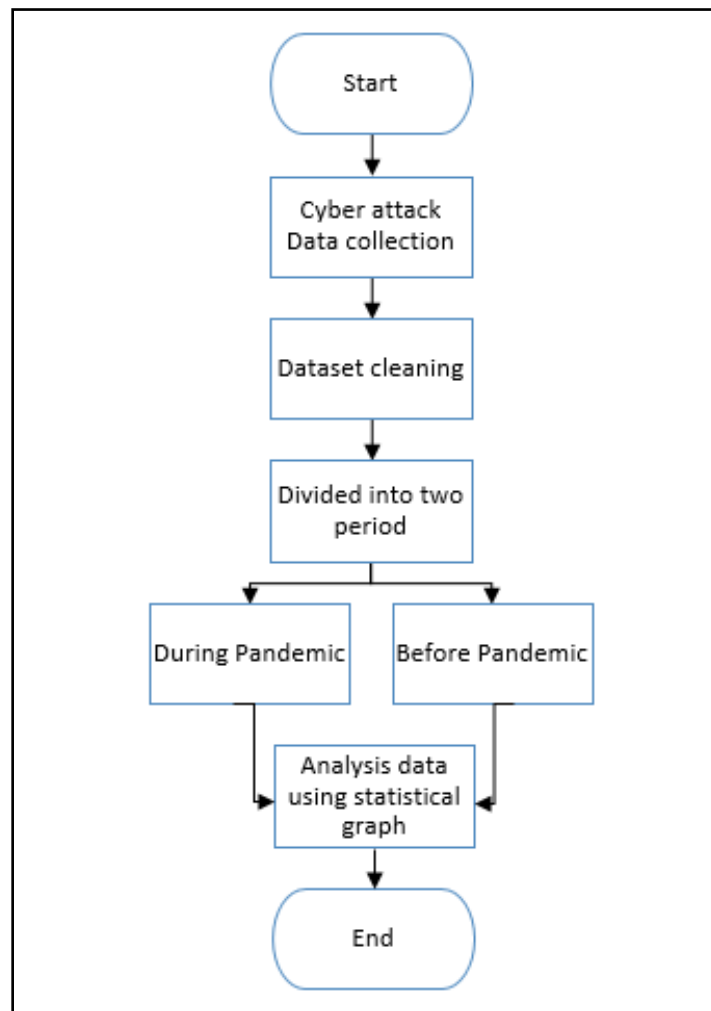


Figure 1: Flowchart of Research Approach

Organization That Are Most Vulnerable to Threats:

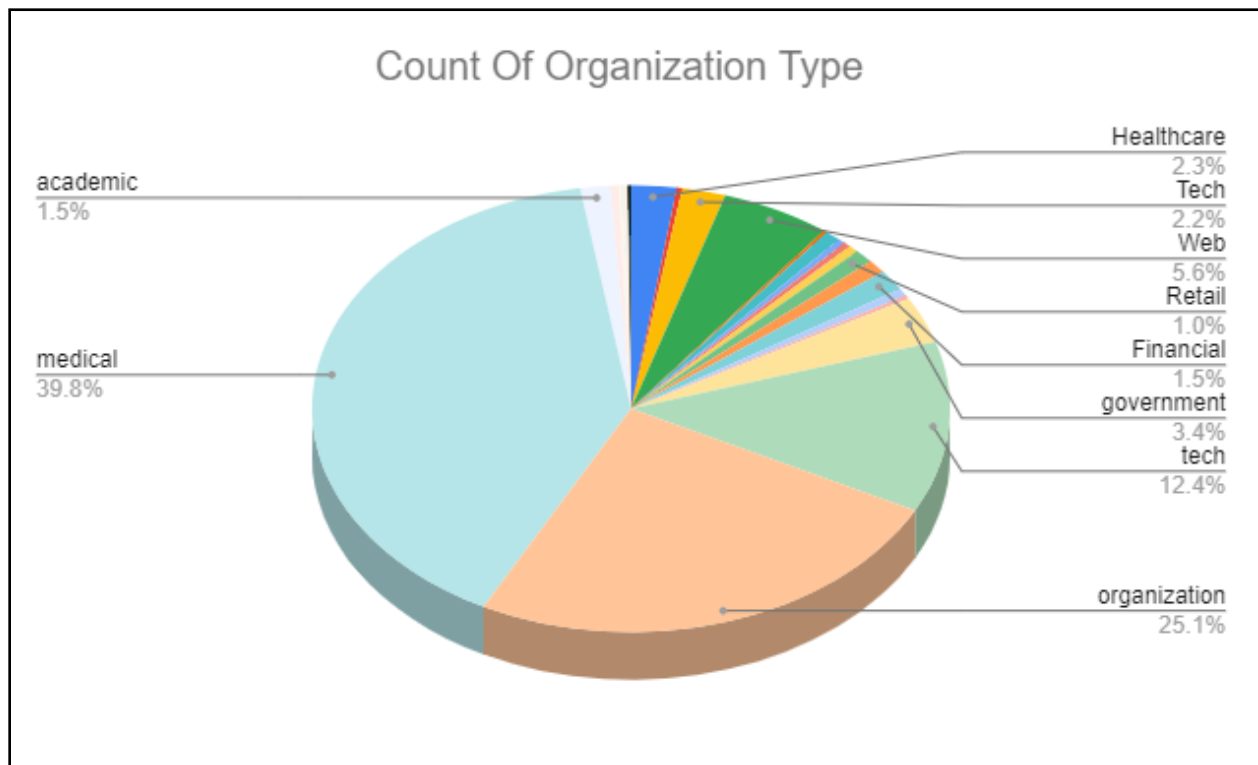


Figure 2: Count of Organization Type

Medical and health-care systems operate on applications that include nurses, patients, physicians, pharmacists, and a variety of e-healthcare services. The graph illustrates that medical sectors have faced more threats than the other organizations. Then we can see that the tech sectors are the next in line that took cyberattacks that many after medical and organizations. The medical and healthcare organizations are the most sensitive and important sectors of a nation. According to the INTERPOL investigation, most of the online attacks include fraud and theft of sensitive information via phishing operations targeting remote personnel. In the time of corona pandemic, malicious actors spread Malware, Trojans and Spyware via linked websites for media, governments and healthcare. They take information after anyone goes to the websites and clicks the link.

Chapter 3: Industries and Organizations most vulnerable to cyber attacks

3.1 E-Health system:

Online Healthcare services are currently built on contemporary technology, which provides its users different medical services which is known as eHealth system. In the time of epidemic, this type of system is the most vulnerable and affected systems. If any hackers attack this system it can result a very adverse situation such as the loss of priceless human life which is unfavorable. Any form of hostile hack will almost certainly aggravate the war that health institutions are now fighting, with staff and resources that have already been taxed in response to the pandemic situation like coronavirus. In United States of America, the health and human service department was presumably targeted by a DDoS attack [7]. Although they stated that the assault did not disrupt the system or operation, but such attacks can be more dangerous in certain instances.

3.2 Financial Services

Since the pandemic has started financial sectors have been hit by cyber-attacks at a higher rate than most other industries. It also had economic impact on the victims and constituted a substantial danger to global economics and financial markets [8]. If we say about the Crude oil price, we can see the prices dropped to lower level ever in 1991 [9]. This affected the economies of oil-producing countries. Simultaneously, financial sectors are affected due to the different kinds of attacks made by cyber hackers. Furthermore, most cases, financial tech users are frequently the victims of social engineering, in which hackers employ various techniques to impersonate a legitimate individual and acquire access to personal data.

3.3 Government and Media Outlets

In terms of delivering precise and up-to-date data to the general public and international organizations, the situation of corona epidemic provides a tremendous challenge for the government and media. Any type of provider of mistake or false data might lead to an unfortunate spot which is unacceptable. Computer security against government and news institutions can be used by attackers and hackers to broadcast misleading data to the public. Even if the activity isn't really online, but instead fake news stories or deliberate misinformation, it could be a matter of concern to the normal citizen of a certain country and also to the country [10].



Figure 3: Medical advice for spreading of false information about ibuprofen and COVID-19

3.4 Educational Institutions

Educational institutions have become more exposed to cyberattacks because of greater use of technology for teaching and learning. Attackers attack for a variety of reasons, but they do not attack an organization for first-grade homework. Many higher education institutions provide research programs with rich data and intellectual property that might be profitable to the right competitor. According to Microsoft Security Intelligence, the education sector accounted for 62 percent of the approximately 5.8 million malware cases reported.

Despite the fact that this sector had a lower percentage of attacks overall, it is still a more vulnerable sector with limited security expenditures and numerous risks. Students and staff provide a huge, decentralized, and difficult-to-control attack surface, making schools and colleges even more vulnerable to cyberattacks.

Chapter 4: Cyber Threats Amidst the Pandemic

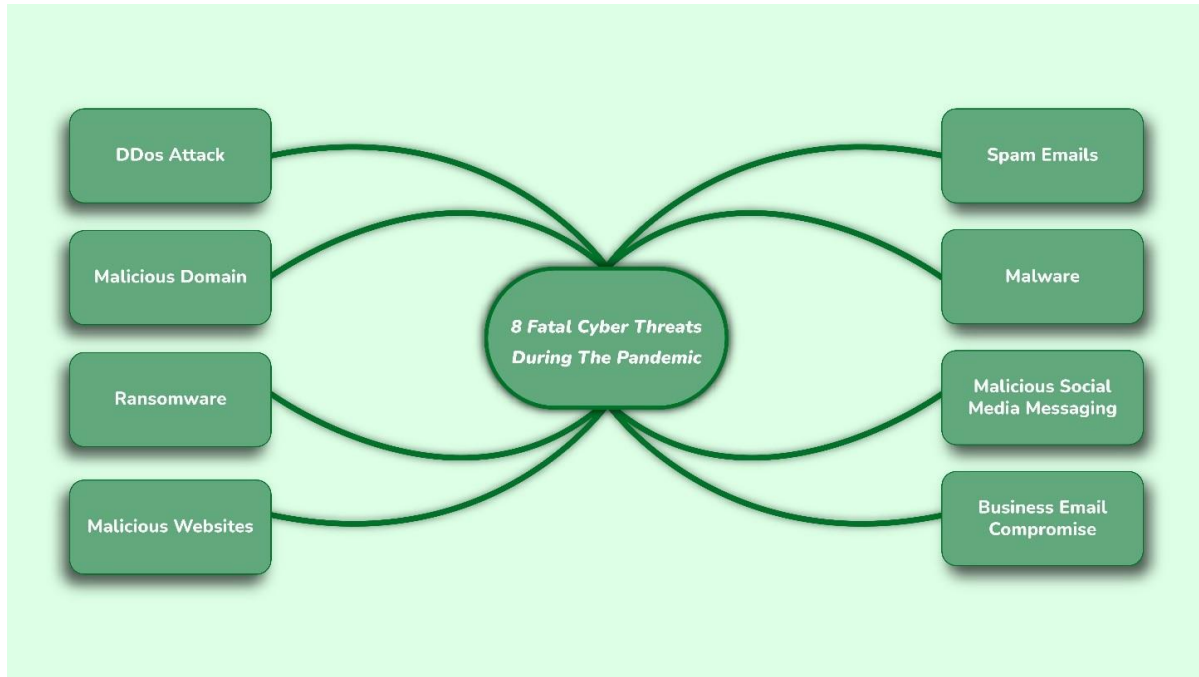


Figure 4: 8 Fatal Cyber Threats During the Pandemic

People nowadays are more inclined to engage with services they would not typically interact with, as well as getting information and resources through emergency service. Threat actors have more chances as demand grows and public concern grows. Despite the enormous impact and devastation caused by this pandemic, the digital behaviour this has enabled isn't really new. With the tremendous advances in technology and the introduction of modern innovation, information safety has now got extremely difficult. Mostly when people or normal individual are at their emergency cyber actors take the advantages of this situation. The coronavirus is being used by bad actors all around the world as a new tool for their wicked activities, such as hacking, attacking, and scamming. According to Trends micro research [11], there were more than 906000 Spam messages, 48000 clicks on malicious URLs, and 736 Malware attacks worldwide during the previous pandemic till the beginning of April 2020.

Furthermore, there was a 220 percent rise in spam email and a 260 percent increase in harmful URLs from February to March 2020 [12]. The top eight-cybersecurity threats during COVID-19 are depicted in Figure 2 and addressed further down.

4.1 DDoS Attack

In the corona epidemic, majority of the organization have faced the significant increase in in Distributed Denial of Service attacks [12]. Bad actors attacks the business organization with phony and bot users to get access to the systems and to destroy system operation and damage the communication interface There was a recent example that occur on the United States Health and Human Services department website has faced attack, which flooded millions of users all at once [13].

4.2 Malicious Domain

Domain names such as “covid19”, “coronavirus”, “COVID-19” and “corona-virus” lately come out that signing up new users in addition the amount of registrations is rising daily. Although some of the sites are legitimate, every day, thousands of new websites are created by fraudsters that are used for spam campaigns, phishing, malware distribution, or server penetration. According to the Checkpoint Risk Intelligence study, globally many domains related to coronavirus have been registered from the January 2020.

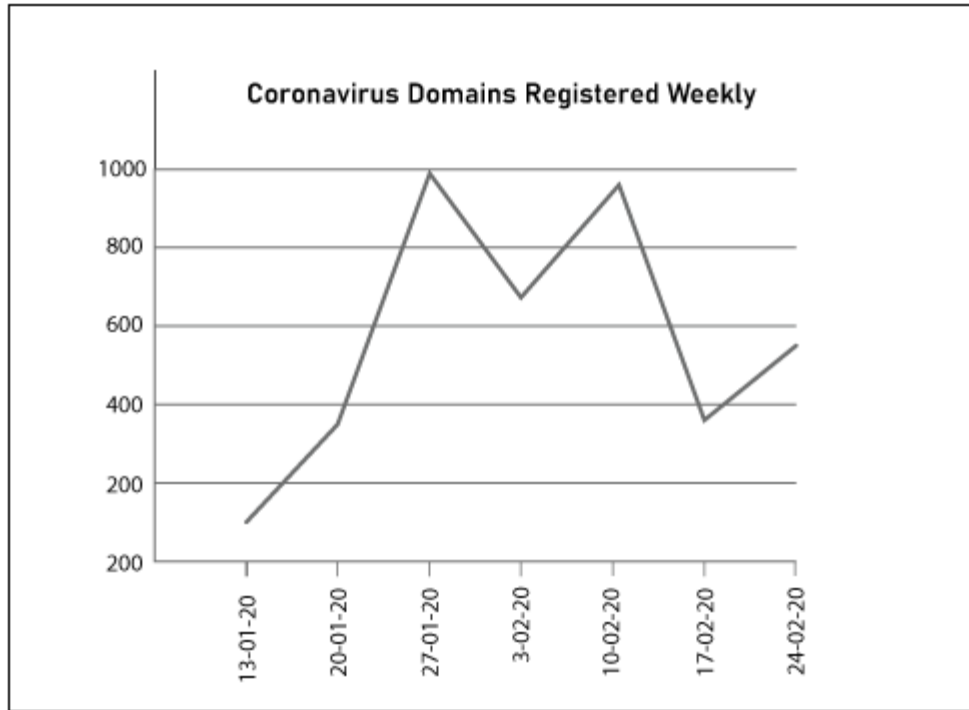


Figure 5: Coronavirus Domains Registered Weekly

This type of domains commonly used to perform various frauds or to function as a botnet for the potential customers. This approach allows hackers to obtain personal information, which they subsequently utilize for their intended purposes.

4.3 Ransomware

Ransomware attacks are being launched against hospitals, health services, universities, as well as other governmental authorities. Criminal thinks that the organization or site they attack, owners will pay ransom as they cannot bear to shut down the system. Ransomware access a program or device through fake email links, URLs, users who has been been hacked due to a system weakness [22]. On the dark web, cybercriminals are increasingly selling ransomware as a service. A ransomware named coronavirus was published in spreading using fake websites which seems like real websites. The users were forced to download file. And at the time the users download the files or after downloading open the file, the file has the ability to open their

computer, access any file in the system, can steal the personal files or data, and could encrypt the data which cannot be decrypted later. [11].

4.4 Malicious Website

There are some websites on the internet that published in the pandemic time. Websites like `www(.)antivirus-covid19(.)site` or `www(.)coronaantivirus(.)com` and pretending to be corona protection but not. Some websites among them are now unavailable, according to Malwarebytes' blog [20]. Some websites, and their application, branded as “Corona Antivirus” was programmed by Harvard University engineers. However, by installing this program, PC infected by a virus named as Black NET RAT. This spyware turns affected devices into botnets. This further could be used to perform a DDoS attack, uploading files from a remote site, execute malicious programs, gather data like passwords, emails, cookies, and capture inputs. As an example we have seen, Department of Justice un USA has declared a short-term injunction to fake websites.

4.5 Spam Emails

Different scammers use spam emails technique to accomplish their goals. And they do this kind of activity in the regular or crisis situations. In the time of epidemic situation, emails related to coronavirus with dangerous files observed a massive scale being delivered to customers as beginning in February 2020. Sometimes it can be seen that the criminals pretend that they are the representative of authorized organization like WHO. They use such type of domain to trick the users in such way that the user will think the email possibly from the authorized organization and then the criminals ask for online payment and bitcoins. Normal users can identify if they interact through real person's mail or official mail's of organization or not. They can identify by glancing the email addresses mostly the last part of the email

name. But the criminals normally used the email address `coronavirusfund@who.org`. Therefore, user must be careful about dealing with this kind of situation.

4.6 Malware

Criminals normally take the advantages in critical situation. In the epidemic situation they also do the same, they take the benefits by transmitting Malware, Trojans, and Spyware via linked the coronavirus maps and various sites [17]. Sending spam emails to the users' emails is a way to hack the user system by entering on a link or installing programs furthermore the user could become the victim [18]. A map developed by Johns Hopkins University with a responsive dashboard that shows different ideas and information in the pandemic and deaths related to coronavirus [19]. Cyber criminals inject malware that is java application based. And users not only use or access the map but also shared the map to the different users. A coronavirus-themed win locker was uncovered that could shut down the clients out from afflicted machines. when this malware is executed, it got access to the systems and change the registry key of the windows. Then it produces sounds and shows some message that contains warning about the system is shut down or closed, before restarting and requiring a pin to access [11].

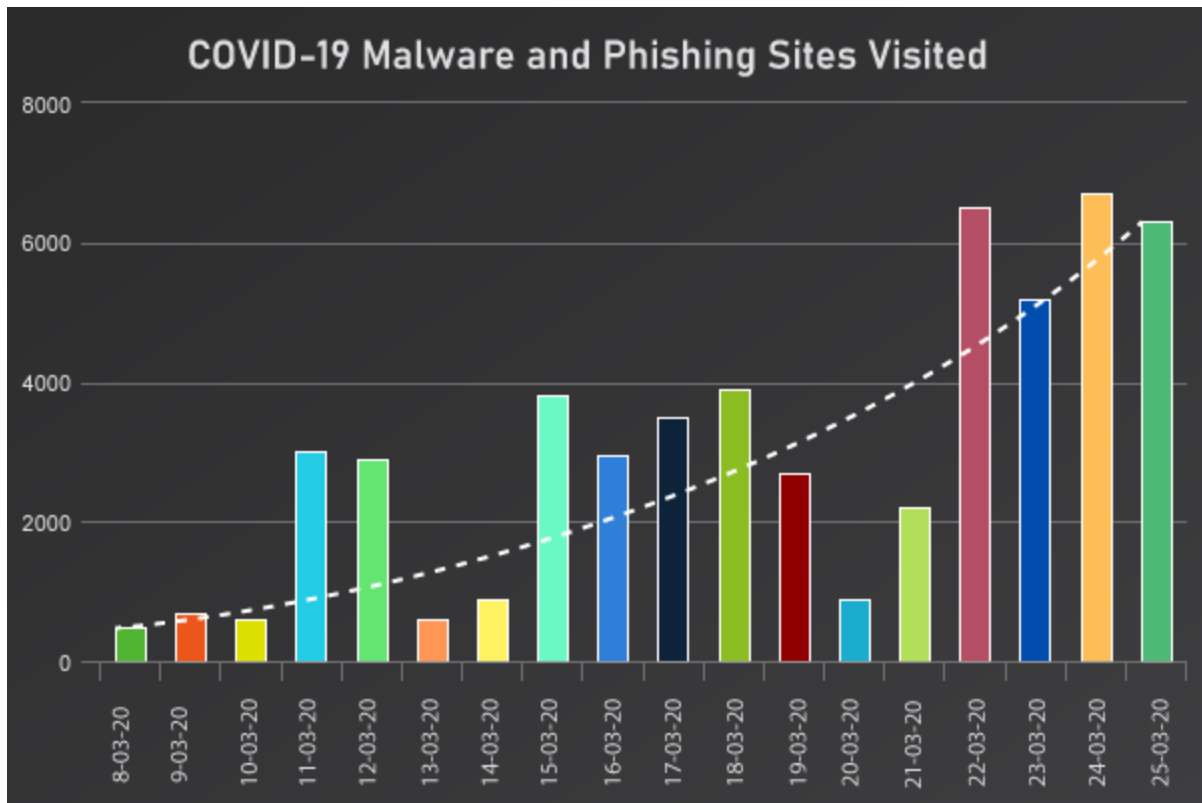


Figure 6: Malware and Phishing Sites Visited during Pandemic [20]

In comparison to other threats and attacks, Different kinds of malware pretend to government or non-government sites expanded to the greatest. Figure 4 depicts the rise of Malware and Phishing website visits during the current epidemic, from February to March 2020.

4.7 Social Media Malware Messaging

Using of social media is increasingly regular these days and almost everybody has connection to that though. Attackers steal platforms from social media account since they perceive this to be a great chance. Numerous instances of thefts and cyber attempts have already been documented on Fb and some other social networking sites. The scammers typically use freebie subscriptions, like a Netflix paid version, to lure their users to become targets. Whenever the user clicks, users are sent to the online social phishing domain. In certain cases, they might need to provide their login information. This kind of activity make possible for them to enter

a system and can hack password or could install the malware in the system to steal data or cookies.

4.8 Compromising Business Email

Intruders used COVID-19 to launch a Business Email Compromise attack, according to Agari Cyber Intelligence Division [21]. The Ancient Tortoise, a group with cybercrime activity actually linked to several BEC incidents, executed the attack. This incident is likely to be part of an attack that occurred before. The attackers go after the bank accounts first. Then, because to the unique coronavirus, they normally collect the data and use this data to send various emails urging them to update their personal information and the information in bank details and correct or change their payment option. The bad actors impersonate reputable companies or organizations. [21].

Chapter 5: Security Breaches

To fight against the corona pandemic, various Organization through technology has a significant function in supporting various countries and associated in controlling lockdowns, however, it is causing concern among privacy experts. Apple, Google, and Facebook, among other tech giants, are already gathering massive amounts of data for the aim of using it for commercial reasons. A number of people are now willing to share their information which contains personal data with various health officials, government agencies and even to academicians. This includes their very personal information like location, passwords, mails and access drive. This might be beneficial in overcoming the problem, but that also puts the public's privacy at risk, and there is concern that the data collected may be exploited long after the epidemic has ended. Many industries, including manufacturing and education, have recently made the transition to the internet. Employees all around the globe are using digital communication and meeting software and tools to stay working from the comfort of their own homes or other remote locations. Prior to using the apps, users must agree to a set of terms and conditions that involve the gathering of personal data and information about their online activities. An investigation of the privacy policies of various programs, was conducted recently, and the results revealed that companies significantly collect much information than people believe [22], which is a matter of concern. Zoom default settings are not safe enough that's why various privacy groups and FBI are warning the zoom authority [23], the most frequently used web conferencing program, Zoom, is facing a significant privacy and safety issue. In addition to this, several governments have lately begun monitoring the whereabouts and other data of their residents and tourists' mobile phones in order to identify particular towns and districts where a considerable percentage of the infected individuals reside. Therefore, for example, the Chinese government is keeping watch on the virus-infected individuals to ensure that they remain

at home and do not spread the illness to other individuals. If they want to go outside the first thing, they need to do is scanning the QR code then a code is issued which is based on colour depending on the report of corona reports. If it shows green, then the individual is good to go outside but if it shows red then it means the individual is restricted to go outside. It is being used to monitor citizens' cell phones in South Korea in order to check if anyone is passing through the infected region and afterwards, they are texted to give the report of the test. To track down Corona Virus sufferers, they are now using credit card technology as well as security cameras. There are several such instances and applications by various governments and organizations that acquire information about customers while also violating their right to personal information. While this may not seem to be risky or damaging at this time, this information might be utilized for adverse causes for the long time, or if any of the data is compromised and made available to malicious actors. For example, the Pakistani government has established a volunteer organization known as the Corona Relief Tiger Force to assist victims of natural disasters (CRTF). A cybersecurity specialist said in the twitter that that private data of the Tiger Force members, including their National Identity card number and address, as well as other information, was published in PDF format on several unauthorized groups, according to reports [24]. Besides learning about the top ten lethal cyber security dangers as a consequence of the Covid-19 [25], we have also learnt about the top seven lessons learned from the Covid-19 [25].

Chapter 6: Practical Approach to Reduce Cyber Threats

Reducing and preventing cyber-attacks is not really a simple task to accomplish. When it comes to Work from Home, there still are practical ways that can be used to lessen the danger of cyber-attacks.

- 1. Training the users:** Approximately 11 percent of organizations have offered training program to non-cybersecurity personnel in the last year, according to recent research [26]. The strength of a security system is just as strong as its weak point. There are many security systems which consider user to be the weakest link in their chain of protection. Developing security awareness among users via on-going training is thus critical to reducing the dangers of cyber-attacks over an organization's systems and infrastructure.
- 2. Using Virtual Private Network:** A network that connects the two computers with a secure connection over the Internet is known as Virtual Private Network (VPN), encrypting all data traveling between them. Virtual private networks (VPN) have become the norm for browsing the Internet. It is possible to increase security policies to remote workers via a virtual private network (VPN), which provides both confidentiality and integrity.
- 3. Using Multi Factor Authentication Feature:** Multi Factor Authentication increases security by requesting a username and password, as well as temporary one time code sent to a device through an authentication app or SMS, in addition to a username and password. Multi Factor Authentication is a critical component of protecting against password cracking and theft, such as those perpetrated by brute force cyber-attacks. In order to, access the network of a certain company from home, an employee should provide her username and password first, as well as the code that sent to her mobile phone in order to verify her identity.

- 4. Strict Company Policy:** There has been very little or maybe no time for organizations to ready for the World from Home (WFH) scenario. An effective and complete WFH strategy is necessary to safeguard data and decrease cyber-attacks. Strict WFH standards, for example, prohibit employees from having crucial professional talks in public areas and require them to utilize only organization-approved audio and video conferencing lines. In addition, policies should contain a thorough and tested disaster recovery plan as well as a backup strategy.
- 5. Updating devices firmware:** Make sure that all the software and operating systems on all of your devices and equipment's are updated with the most recent security patches. This will protect them from any significant problems. It may be less likely for a zero-day attack to happen if you get regular and update patches.
- 6. Updating anti-malware software's:** Check on that anti-malware program is enabled on any internet devices, including cyber thieves use a variety of viruses to prey on the most susceptible members of the population. Because millions and millions malware and its strains are created each year, keeping anti-malware software up to date on a regular basis may help to lessen the threat of cyber forms of malware.

Conclusion

In the pandemic situation we had to stay home and the uses of internet and using social media is increasing drastically. Cyber bad actors took the scope and intensified their crime activities throughout the pandemic days. Worldwide cyber-attacks are increased rapidly during the pandemic of COVID-19. From the collected data that shows 2019 is the official outbreak of COVID-19 and it also the year that cybercrimes were increased more than the previous years. During the pandemic the most important organizations or major sectors like governments, medicals, media and tech companies are the most to be attacked by the hackers. Medical organizations are one of the most that are affected by the cyberattacks. During the attacks, hackers used different types of methods but the most they used is the hacking method. DDoS becomes more important as its assaults on businesses, medical services, and even on academics escalate. Additionally, by the end of 2020, the globe has experienced the greatest cyber assaults including malware activities. In the pandemic situation, it can be seen that cyber-crimes have increased in many sectors due to lack of security the sector or organization are providing and a lack of knowledge of using internet. By providing some practical way to reduce the cyber-threats while work from home or spreading awareness about how readily cyber threats can affect the organization, institutions or any individuals. We can at least hope to control the cyber-attacks.

References

1. Ducharme, J. (2020, March 11). World Health Organization Declares COVID-19 a 'Pandemic.' Here's What That Means. Time. <https://time.com/5791661/who-coronavirus-pandemic-declaration/>
2. Furnell, S. (2020, August 18). Home working and cyber security – an outbreak of unpreparedness? National Library of Medicine. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7434364/>
3. Perez, S. (2020, March 30). Videoconferencing apps saw a record 62M downloads during one week in March. Techcrunch. <https://techcrunch.com/2020/03/30/video-conferencing-apps-saw-a-record-62m-downloads-during-one-week-in-march/>
4. Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. Arabian Journal for Science and Engineering, 45(4), 3171-3189. doi:10.1007/s13369-019-04319-2
5. Patange, T. (2020, May 26). Zoom already banned in over 20 countries; India to join the list?. News. <https://news.thewindowsclub.com/zoom-already-banned-in-other-countries-100168/>
6. (2020, April 12). Google bans employees from using Zoom app - Times of India. Timesofindia. <https://timesofindia.indiatimes.com/gadgets-news/google-bans-employees-from-using-zoom-app/articleshow/75058247.cms>
7. Stein, S. & Jacobs, J. (2020, March 16). Cyberattack hits HHS amid COVID-19 outbreak | BenefitsPRO. Benefits Pro. <https://www.benefitspro.com/2020/03/16/cyberattack-hits-hhs-amid-covid-19-outbreak/?slreturn=20220629124908>
8. Jabeen, S., Farhan, M., Zaka, M., Fiaz, M. & Farasat, M. (2022). COVID and World Stock Markets: A Comprehensive Discussion. Frontiers in Psychology, 12. <https://doi.org/10.3389/fpsyg.2021.763346>
9. Stevens, P. (2020, March 8). Oil plunges 24% for worst day since 1991 after OPEC deal failure sparks price war. Cnbc. <https://www.cnbc.com/2020/03/08/oil-plummets-30percent-as-opec-deal-failure-sparks-price-war-fears.html>
10. Cook, A. (2020, March 26). COVID-19: Companies and Verticals At Risk For Cyber Attacks | Digital Shadows. Digital Shadows. <https://www.digitalsadows.com/blog-and-research/covid-19-companies-and-verticals-at-risk-for-cyber-attacks/>

11. (2020, November 11). Developing Story: COVID-19 Used in Malicious Campaigns - Security News. Trend Micro.
<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains#:~:text=COVID%2D19%20is%20being%20used,as%20a%20lure%20likewise%20increase>
12. (2021, February 11). DDoS attacks intensify — Driven in part by COVID-19 and 5G | 2021-02-11 | Security Magazine. Security Magazine.
<https://www.securitymagazine.com/articles/94570-ddos-attacks-intensify-driven-in-part-by-covid-19-and-5g>
13. Salvi, V., Ananth, V. & Bari, Y. (2020, July 14). Infosys Knowledge Institute | Being Resilient: Overcoming Healthcare's Cybersecurity Challenge. Infosys.
<https://www.infosys.com/iki/perspectives/overcoming-healthcares-cybersecurity.html>
14. Khan, N. A., Brohi, S. N., & Jhanjhi, N. Z. (2020, 2020//). UAV's Applications, Architecture, Security Issues and Attack Scenarios: A Survey. Paper presented at the Intelligent Computing and Innovation on Data Science, Singapore.
15. Marchetti, Dr. Penelope. (2020, March 5). Update: Coronavirus-themed domains 50% more likely to be malicious than other domains. Check Point.
<https://blog.checkpoint.com/2020/03/05/update-coronavirus-themed-domains-50-more-likely-to-be-malicious-than-other-domains/>
16. W. Han, J., J. Hoe, O., S. Wing, J. & N. Brohi, S. (2017). A Conceptual Security Approach with Awareness Strategy and Implementation Policy to Eliminate Ransomware. 2017 International Conference, 222-226. 10.1145/3168390.3168398
17. (2022, July 11). Cyberthreats are constantly evolving in order to take advantage of online behaviour and trends. The COVID-19 outbreak is no exception.. Interpol.
<https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats>
18. (2022, July 29). COVID-19 Map - Johns Hopkins Coronavirus Resource Center. Johns Hopkins Coronavirus Resource Center. <https://coronavirus.jhu.edu/map.html>
19. (2020, April 4). Sophisticated COVID-19–Based phishing attacks leverage PDF attachments and SaaS to bypass defences. Menlo Security.
<https://www.menlosecurity.com/blog/sophisticated-covid-19-based-phishing-attacks-leverage-pdf-attachments-and-saas-to-bypass-defenses/>

20. Peterson, P. (2020, March 19). Business Email Compromise (BEC): Coronavirus a Costly New Strain of Email Attack | Agari. Agari. <https://www.agari.com/email-security-blog/business-email-compromise-bec-coronavirus-covid-19/>
21. St. John, A. (2020, April 30). Google-Meet-Microsoft-Teams-Webex-Privacy-Issues-Consumer-Reports.pdf. Hawaii. <https://www.hawaii.edu/its/wp-content/uploads/sites/2/2020/05/Google-Meet-Microsoft-Teams-Webex-Privacy-Issues-Consumer-Reports.pdf>
22. Warren, T. (2020, April 1). Zoom faces a privacy and security backlash as it surges in popularity - The Verge. Theverge. <https://www.theverge.com/2020/4/1/21202584/zoom-security-privacy-issues-video-conferencing-software-coronavirus-demand-response>
23. Saeed, H. (2020, May 4). Personal Data of Thousands of Tiger Force Members Leaks. Propakistani. <https://propakistani.pk/2020/05/04/personal-data-of-thousands-of-tiger-force-members-leaks/>
24. Jayakumar, Priyanka; Brohi, Sarfraz Nawaz; Zaman, Noor (2020): Top 7 Lessons Learned from COVID-19 Pandemic. TechRxiv. Preprint. <https://doi.org/10.36227/techrxiv.12264722.v1>
25. N. A. Khan, S. N. Brohi, and Jhanjhi. NZ, "UAV's Applications Architecture Security issues and Attack Scenarios: A Survey," in 1st International Conference on Technology Innovation and Data Sciences (ICTIDS) 2019, 2019.
26. Bhuyan, S., Kabir, U., M. Escareno, J. & Ector, K. (2019). Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations. Journal of Medical Systems, 44. 10.1007/s10916-019-1507-y