Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic

Navid Ali Khan [1], Sarfraz Nawaz Brohi [1], and Noor Zaman [2]

[1]Affiliation not available
[2]Taylors University

October 30, 2023

Abstract

World Health Organization declared COVID-19 as a pandemic after the breakout in the city of Wuhan, China. The disease has negatively affected the global economy and daily life. Most of the countries around the world have imposed travel restrictions, locked down, and social distancing measures. In the current situation, Information and Communications Technology is playing a significant role in connecting people. Majority of the education organizations have adopted online platforms, students and staff are working from home. Besides, these businesses, e-healthcare systems, food deliveries, and online grocery shopping have witnessed a very high demand. Malicious attackers have considered COVID-19 as an opportunity to launch attacks for financial gains and to promote their evil intents. Healthcare systems are being attacked with ransomware and resources such as patient's records confidentiality, and integrity is being compromised. People are falling prey to phishing attacks through COVID-19 related content. In this research, we have identified the top ten cybersecurity threats that had and could take place during the pandemic. We have also discussed the privacy concerns raised amid COVID-19.

Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic

Navid Ali Khan
School of Computer Science and Engineering
Taylor's University
Selangor, Malaysia
navidalikhan@sd.taylors.edu.my

Sarfraz Nawaz Brohi
School of Computer Science and Engineering
Taylor's University
Selangor, Malaysia
sarfraznawaz.brohi@taylors.edu.my

Noor Zaman
School of Computer Science and Engineering
Taylor's University
Selangor, Malaysia
noorzaman.jhanjhi@taylors.edu.my

***Abstract* — World Health Organization declared COVID-19 as a pandemic after the breakout in the city of Wuhan, China. The disease has negatively affected the global economy and daily life. Most of the countries around the world have imposed travel restrictions, locked down, and social distancing measures. In the current situation, Information and Communications Technology is playing a significant role in connecting people. Majority of the education organizations have adopted online platforms, students and staff are working from home. Besides, these businesses, e-healthcare systems, food deliveries, and online grocery shopping have witnessed a very high demand. Malicious attackers have considered COVID-19 as an opportunity to launch attacks for financial gains and to promote their evil intents. Healthcare systems are being attacked with ransomware and resources such as patient's records confidentiality, and integrity is being compromised. People are falling prey to phishing attacks through COVID-19 related content. In this research, we have identified the top ten cybersecurity threats that had and could take place during the pandemic. We have also discussed the privacy concerns raised amid COVID-19.**

Keywords— COVID-19, Cyber Security, ICT, Security Threats, Privacy Concerns

I. INTRODUCTION

On 30th January 2020, the World Health Organisation (WHO) confirmed a "public health emergency of international significance" with the outbreak of novel coronaviruses (COVID-19) [1]. The Centres for Disease Control and Prevention also declared an emergency for public health in the United States on 31st January 2020 [2]. COVID-19 has now spread to almost every country of the world, and new cases and fatality reports are increasing daily [3].

In addition to being life-threatening, COVID-19 has destabilized businesses, damaged daily lives, and induced stress and anxiety in individuals. It has stunned the global economy. Researchers and scientists have developed collaboration platforms for the discovery of COVID-19 vaccines and drugs. The production of the vaccine will take significant time to be available for the general public due to testing, safety, and quality assurance measures.

As the disease is transferrable from person to person [4].To limit the spread of this novel disease, many countries decided to close educational institutions, including schools, colleges, and universities. Lecturers are teaching online; in fact, this is happening at a very huge untested and unprecedented scale. Students' assessments and exams are also conducted online [5]. One of the most initial impacts of COVID-19 is shifting from the physical workplace to the online virtual workplace. This happened immediately throughout the world in many organizations as soon as the pandemic grew worse and started affecting daily life [6]. COVID-19 has pushed businesses to work quickly and check system durability as never done before. As the businesses are transforming, new system challenges and priorities are increasing, such as real-time decision making, online staff training, continuity risks, and the biggest one is security risks. These issues need to be quickly addressed in the current situation

The rapid spread and prolonged incubation of the virus present unique societal challenges. Still, one of the positive points, when this pandemic is occurring, is that it's taking place in such times when the remote communication is on its peak. The tools and devices used for this communication are ubiquitous. Due to modern technology, it has been possible to stay in touch with colleagues, friends, and family. The online video conferencing apps such as Zoom, Microsoft Teams, and Google Meet have witnessed an exponential increase in new users signing up daily [7]. However, the use of technology is bringing more issues and threats in terms of cybersecurity [8]. Organizations will have to deal with the growing security demands emerging from the increased risk of cyber-attacks. They must also be mindful of the difficulties created by the need to balance sensitive health information and privacy issues of people who may have been infected with them [9]. For example, with the rapid growth of Zoom's popularity, Zoom is now faced with a massive backlash as security professionals, privacy advocates, lawmakers, and even the FBI warn that Zoom's default settings are not safe. As a result, many companies such as NASA, SpaceX, and countries, including Taiwan, USA, and the Australian Defence force, banned Zoom for communication [10]. Therefore, there is a need to realize these cyber threats and privacy concerns, which can lead to unfavourable situations to mitigate or avoid them [11].

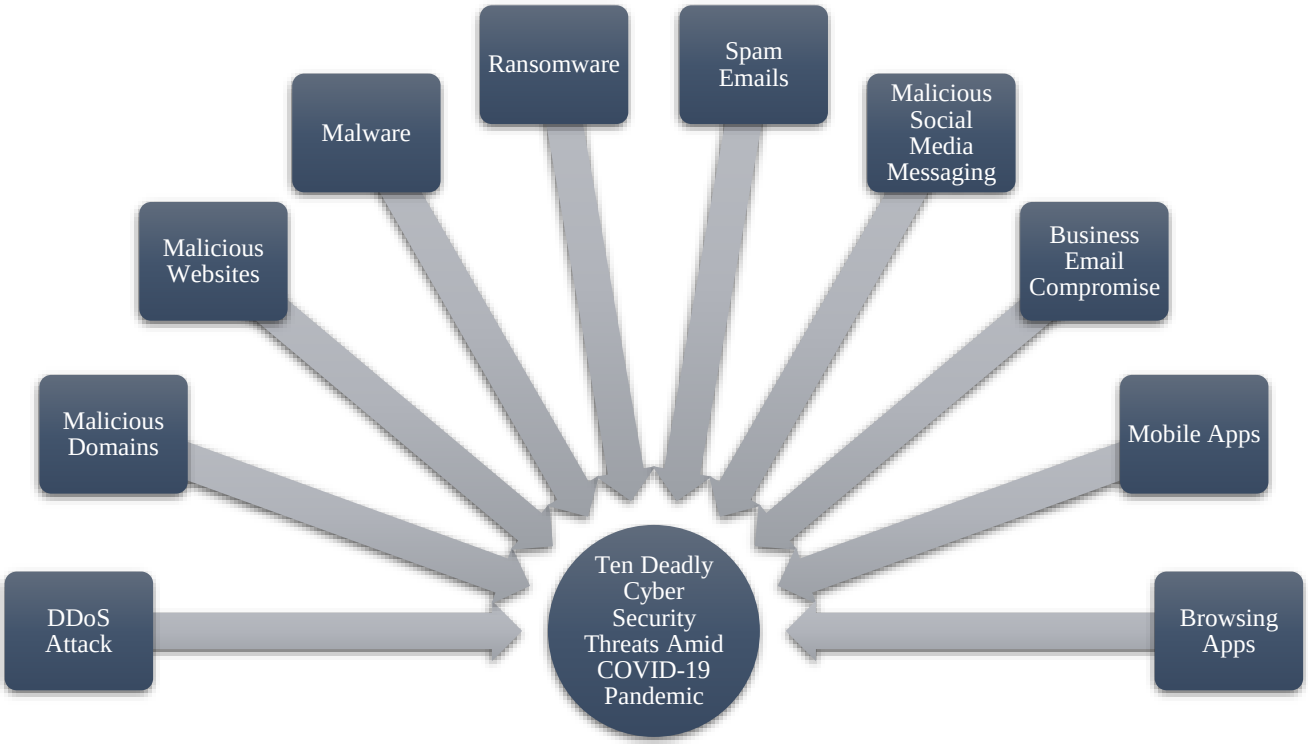

Figure 1: Top 10 Cyber Security Threats Amid COVID-19 Pandemic

II. COVID-19: MOST AT-RISK ORGANIZATIONS AND INDUSTRIES IN TERMS OF CYBER ATTACKS

1) Healthcare Systems

Modern-day healthcare systems are based on ICT applications, which offer its users, including physicians, nurses, pharmacists, and patients, a comprehensive range of medical services known as e-healthcare. In the recent pandemic situation, they are the most vulnerable and targeted systems. If anything goes awry, it can result in an unfavourable condition such as loss to precious human lives. Any malicious cyber-attack will likely escalate the battle currently faced by health institutions with resources and personnel which are already stretched in response to the novel coronavirus. In the USA, the Department of Health and Human Services was reportedly targeted by a DDoS attack as its servers received millions of connection requests over several hours [12]. Although the officials claimed that fortunately, this attack did not interrupt the system and functionality but potentially such kinds of attacks can be disastrous in certain situations.

2) Financial Services

Due to COVID-19, countries and stock markets around the world have fallen to the lowest points in the past 30 years. Crude Oil prices have fallen to the lowest in history since 1991 [13]. This has put the Oil producing countries' economies at stake. As soon as this pandemic outbreak started, a financial recession was already predicted by the experts. At the same time, the financial industries are vulnerable to cyber threats such as phishing and Malware [14] or ransomware [15] attacks. In addition to this, in a normal situation, the fintech users have mostly become the victim of social engineering, where the hackers use certain tricks to pretend to be the legit person and get access to personal information such as password recovery.

3) Government and Media Outlets

The current pandemic due to COVID-19 is a very challenging issue for the government and media outlets itself to provide accurate and timely information to its public and international organizations. Any delay or misleading information may lead to unpleasant situations. The attackers and hackers can launch cyber-attacks on government and media outlets to spread the wrong information in public. For example, even if it's a non-cyber activity but just a piece of false news, it still can create hype and fear among the general public and can raise questions about the governments [16].

III. CYBER THREATS AMID THE PANDEMIC

With the advancement of technology, nowadays, cybersecurity has become very challenging. It's common for hackers, attackers, and scammers to take advantage of emergencies, particularly in times when people are frightened, desperate, and most vulnerable. The outbreak of coronavirus is no different. Bad actors around the world are using the coronavirus as a new tool for their evil deeds in the form of hacking, attacking, or scams. According to Trends micro research [17], in the recent pandemic, there were a total of more than 907K Spam messages, 737 Malware attacks, and 48k hits on malicious links around the world until the start of April 2020.

Moreover, from February to March 2020, there has been a 220 times increase in spam email and 260% in malicious URLs. Furthermore, the United States is the top location for detecting spam and malware, and most of the target users are accessing them from the United States [17]. Figure 1 illustrates the top 10 cybersecurity threats amid COVID-19 and is discussed below.

1) DDOS Attack

Most of the government and healthcare organizations have seen a rapid increase in the Distributed Denial of Services (DDoS) [18] attack in the current pandemic due to COVID-19. The hackers flood the organizations' websites or systems with fake or bot users to crash the normal functioning of the system and thus interrupt the communication channel. A recent example of this happened when a DDoS attack targeted the website of the Department of Health and Human Services (DHoS) in the U.S. by flooding millions of users at a time [12].

2) Malicious Domains

The words "coronavirus," "corona-virus," "covid19," and "COVID-19" have appeared in a wide number of registered domains on the internet recently, and daily more and more increase has been witnessed. Although some are legitimate web sites, cybercriminals build thousands of new sites every day in which spam campaigns, phishing, malware spreading, or servers are compromised.

More than 4,000 domains linked to coronaviruses have been registered worldwide since January 2020 based on the CheckPoint Risk Intelligence report. 3% of these websites are malicious, and a further 5% suspicious. The coronavirus-related areas are 50% higher than those reported in the same period and also higher than recent seasonal events, such as the day of Valentine [19]. These domains are used to carry out different scams, or they are used to act as a honeypot for the target users. Hackers get personal data through this procedure and then use it for their intended purposes.

3) Malicious Websites

There has been an increase in websites that claim to be applications that are supposed to protect users from COVID-19, such as www.antivirus-covid19.site and www.corona-antivirus.com. According to Malwarebytes' blog [20], the website www.antivirus-covid19.site is now inaccessible. The website www.corona-antivirus.com mentions that their application, called "Corona antivirus," has been developed by scientists at Harvard University. But in reality, installing this application infect the system with a malware called BlackNET RAT. This malware makes the infected devices work as a botnet. This can help to launch a DDoS attack, upload some remote files, execute malicious scripts, collect browser cookies and passwords and harvest keystrokes, etc.

In another case, a temporary prohibition order against the coronavirusmedicalkit.com fraudulent website is issued by the United States Department of Justice. It is alleged that the web site provides WHO-approved vaccine kits for COVID-19. However, valid COVID-19 vaccines approved by the WHO are not yet available in the market [17]. The fake website asks for US$ 4.95. In order to proceed with the transaction, users have been requested to enter their credit card details.

4) Malware

Cybercriminals are taking advantage of the current situation by spreading Malware, Spywares, and Trojans through embedded interactive coronavirus maps and websites [21]. One of the main source to lure the user into clicking on the link or downloading the malware are spam emails, for which the user becomes victim through mobile device or computers [22]. To show the information and fatalities about the novel coronavirus, Johns Hopkins University developed a map with an interactive dashboard [23]. Hackers took advantage of it, and they embed a java-based malware to it, the victims not only opened the map, but most of them even shared it.

According to Trend Micro Research, they analyzed a coronavirus-themed Winlocker that can lock users out of affected machines. When this malware is executed, it drops some files and modifies the windows registries. Later it plays a sound and display a message the system has been locked, the system restarts and then requires a password to unlock it [17]. Malware and phishing websites have witnessed the highest increase as compare to other threats and attacks. Figure 2 gives an illustration of the increase in Malware and Phishing websites being visited in the current pandemic from Feb to March 2020.

Figure 2: COVID-19 Malware and Phishing Vesting Sites [24]

5) Ransomware

Cybercriminals are launching ransomware attacks in hospitals, health centers, education, and public institutions. Since they can't afford to be locked out of their systems because of the current situation, criminals are optimistic that these organizations can pay the ransom. The ransomware infects the system via email attachments, links, or through working employees whose credentials are already compromised by exploiting a vulnerability in their systems [22]. Cybercriminals are now even offering ransomware-as-a-service on the dark web.

A new ransomware named CoronaVirus was uploaded and spread through a fake Wise Cleaner (system optimization software) website. The victims were lured to download the fake setup file from the site. Once the victim installs this malware on their computer, this malware can steal a password, encrypts the data which cannot be unencrypted later on, and also steals information from the system as well [17].

6) Spam Emails

Whether it's a normal or an emergency situation, spam emails have always been used on a very large scale by the

scammers and hackers to achieve their intended purposes. In the current epidemic situations, the coronavirus-related emails with malicious attachments have been observed on a very large scale sent to users as early as February 2020. There have been numerous cases in which the intruders pretend to be from legit organizations such as WHO. They use domain spoofing to fool the victim that the email is coming from WHO and ask them to donate in bitcoins etc. For instance, the end of the email address normally ends with the organization's website, and people can know from there whether they are communicating with the right person or organization. The intruders use an email such as coronavirusfund@who.org. The WHO official website www.who.int ends with "int" and not with "org." Any user who did not confirm this email may become a victim [25].

7) Malicious Social Media Messaging

Nowadays, social media is very common and is almost in the reach of every individual. Hackers find it a great opportunity and tend towards the various social media platforms such as Facebook and WhatsApp. There have been numerous cases in which scams and phishing tactics are circulating on Facebook Messenger and many other such applications. The scams typically lure victims into free subscriptions such as Netflix premium free account. When the victim clicks on the link, it redirects them to their social media phishing website. In some cases, it may ask to enter the credentials of their accounts. This way, they either capture their credentials or install malware into their systems, mobile devices, and web browsers to steal information and cookies, and thus, the user becomes a victim [17].

8) Business Email Compromise

Agari Cyber Intelligence Division [26] reported a Business Email Compromise attack as the intruders took advantage of COVID-19. The attack was carried on by the Ancient Tortoise, a cybercrime organization behind several BEC cases in the past. This attack is believed to be a series of the previous attacks the group launched earlier. The attackers first target the bank accounts. Then they use the information of the customers and send them emails to change their bank information and payment methods due to the novel coronavirus. The attackers pretend to be from legit organizations or businesses [27].

In the current situation, the business email compromise scams are using coronavirus disease as a tool. The scam works by convincing or tricking the targets into making transactions to an intruder who shows him/herself as a legit employee working in the same company.

9) Mobile Threats

In this modern era of ubiquitous computing, smartphone users are at their peak. Life without smartphones and gadgets has become impossible, and the use is increasing on a daily basis. At the same time, it's a great opportunity for bad actors to take advantage of it. An application named CovidLock (Ransomware) comes from a malicious Android app that is supposedly helping to track COVID-19 cases. The ransomware locks victims' phones, who are given 48 hours to pay USD100 in bitcoin for recovery. Threats include the deletion of the phone data and the leakage of the account information in social media. In another case, an android app which is offering face mask and safety kits to the worried individuals. Once an individual installs the application, this app delivers a SMSTrojan, which collects the contact list of the victim phone directory and sends auto SMS to spread itself [28].

10) Browsing Apps

With fast growth and easy access to the internet around the world, browsers have become a daily used software, and it is used by almost every individual who has access to the internet. A new cyber-attack was found to propagate a fake COVID-19 information app that allegedly came from the WHO. The hacker gets access to the router Domain Name System (DNS) setting in the D-Link or Linksys routers, which open the browsers automatically and display a notification or an alert from the malicious app. The alert only shows a button labelled to download a "COVID-19 Inform app." When the user clicks on the download button, it installs "Oski info stealer" malware on the device. This malware steals the browsers' cookies, stored passwords, browser history and transaction information, and many more [29].

IV. PRIVACY CONCERNS

The data-sharing company by technology is playing their role to help different governments and their officials to overcome the dizzying spread of the novel coronavirus by maintaining the locked downs and social distancing, but at the same time, it's keeping the privacy experts on edge. Tech Giants such as Apple, Google, and Facebook are already collecting masses of data to use it for advertising purposes. Now, some of them are providing personal data such as location and other personal information to public health authorities, government agencies, and even to researchers. This could be helpful to overcome the situation, but at the same time, it is putting public privacy on stake, and there is fear that this data can be used even when this pandemic is over. Recently, many sectors, such as industries, education, have shifted online. Employees around the world are using online communication and conferencing tools and software to continue working from their homes. To sign up for the applications, the consumers have to agree to some terms and conditions, which include their privacy and security data collection. A recent consumer report analyzed the privacy policies of these applications such as Google Meet, Microsoft Team, and Zoom and concluded that they are collecting more data than people realize [30], which is alarming.

The most widely used online conferencing tool Zoom now faces a massive backlash in terms of privacy and safety, as security experts, privacy advocates, lawmakers, and the FBI are warning that Zoom's default settings are not adequately secure [31]. In addition to this, recently, many countries have started monitoring the locations and other details of their citizens and visitors cell phones to locate specific cities and districts where a significant number of the people infected are residing. For instance, the Chinese government is tracking the infected people from the virus to make sure they stay at home so other people may not get infected. If somebody needs to go out of their home, they need to scan a Q.R. code, and they will get a colour code which is based on their COVID-19 test results, i.e., green for clear, red needs to be quarantined and can't go out. In South

Korea, they are using their citizen's smartphones to track them to confirm if someone passes near an infected area and then text them to report for the virus test. They're also using the credit card and security cameras to track the patients of Corona Virus. The same model is also followed in Israel [32]. There are many other examples and applications by different countries and different organization which is collecting and breaching the privacy of the consumers. At the moment, this may not be unsafe or harmful as it seems, but this data can be used for negative purposes in the long run or if any of the data is breached to some bad actors. For instance, the Pakistani government recently come up with a volunteer force called the Corona Relief Tiger Force (CRTF). According to the reports and cybersecurity, analyst tweeted from their official account that the personal data such as National Identity, mobile number, address and other information of the Tiger Force have been shared in PDF files on different unofficial WhatsApp groups [33]. Besides of these top ten deadly cyber security threats resulting from the Covid-19, we have also learned top 7 lessons from the Covid-19 [34] as well.

V. Conclusion

As the world is advancing and the use of ubiquitous computing is increasing daily, with the same ratio, there's an increase in cybersecurity threats and privacy issues as well. With the recent outbreak of the coronavirus pandemic, there has been a huge increase in the number of users interacting with each other working online. Taking advantage of the situation, the bad actors became more active to hack and attack different platforms for some financial gains and other interests. There has been a considerable increase in the registration of malicious domains, websites, and spam emails. The intruders are targeting individuals, government officials, and even medical and health care systems. This paper presented the threats that are vital to avoid in this pandemic situation. These Cyber Security threats have led to some serious privacy issues and concerns. Future work will focus on new threats and the privacy issues that have been emerged due to the COIVD-19 pandemic.

References

[1] WHO (World Health Organization), "Statement on the second meeting of the International Health Regulations (2005) Emergency Committee regarding the outbreak of novel coronavirus (2019-nCoV)," 2020. [Online]. Available: https://www.who.int/news-room/detail/30-01-2020-statement-on-the-second-meeting-of-the-international-health-regulations-(2005)-emergency-committee-regarding-the-outbreak-of-novel-coronavirus-(2019-ncov). [Accessed: 04-May-2020].

[2] K. L. Bajema *et al.*, "Persons evaluated for 2019 novel coronavirus—United States, January 2020," *Morb. Mortal. Wkly. Rep.*, vol. 69, no. 6, p. 166, 2020.

[3] Worldometers, "Reported Cases and Deaths by Country, Territory, or Conveyance." [Online]. Available: https://www.worldometers.info/coronavirus/#countries. [Accessed: 04-May-2020].

[4] WHO, "Modes of transmission of virus causing COVID-19: implications for IPC precaution recommendations," 2020. [Online]. Available: https://www.who.int/news-room/commentaries/detail/modes-of-transmission-of-virus-causing-covid-19-implications-for-ipc-precaution-recommendations. [Accessed: 04-May-2020].

[5] S. Burgess and H. H. Sievertsen, "Schools, skills, and learning: The impact of COVID-19 on education," *VoxEu. org*, vol. 1, 2020.

[6] Accenture, "COVID-19: Managing the human and business impact of coronavirus," 2020. [Online]. Available: https://www.accenture.com/my-en/about/company/coronavirus-business-economic-impact. [Accessed: 04-May-2020].

[7] 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-apps-saw-a-record-62m-downloads-during-one-week-in-march/. [Accessed: 05-May-2020].

[8] M. Humayun, M. Niazi, N. Z. Jhanjhi, M. Alshayeb, and S. Mahmood, "Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study," *Arab. J. Sci. Eng.*, pp. 1–19, 2020.

[9] S. P. Berman and J. W. Gately, "COVID-19 and Its Impact on Data Privacy and Security," 2020. [Online]. Available: https://www.lexology.com/library/detail.aspx?g=dec8ccab-d74a-4bc1-9e4a-9b1e5626e936. [Accessed: 04-May-2020].

[10] B. Vigliarolo, "Who has banned Zoom? Google, NASA, and more," 2020. [Online]. Available: https://www.techrepublic.com/article/who-has-banned-zoom-google-nasa-and-more/. [Accessed: 04-May-2020].

[11] 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.

[12] S. Stein and J. Jacobs, "Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak," 2020. [Online]. Available: https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response. [Accessed: 04-May-2020].

[13] P. Stevens, "Oil plunges 24% for worst day since 1991, hits multi-year low after OPEC deal failure sparks price war," 2020. [Online]. Available: https://www.cnbc.com/2020/03/08/oil-plummets-30percent-as-opec-deal-failure-sparks-price-war-fears.html. [Accessed: 05-May-2020].

[14] Y. Dion and S. N. Brohi, "An Experimental Study to Evaluate the Performance of Machine Learning Alogrithms in Ransomware Detection," *J. Eng. Sci. Technol.*, vol. 15, no. 2, pp. 967–981, 2020.

[15] A. Ren, C. Liang, I. Hyug, S. Broh, and N. Z. Jhanjhi, "A Three-Level Ransomware Detection and Prevention Mechanism," *EAI Endorsed Trans. Energy Web*, vol. 7, no. 26, 2020.

[16] A. Cook, "COVID-19: Companies and Verticals at Risk for Cyber-Attacks," 2020. [Online]. Available: https://www.digitalshadows.com/blog-and-research/covid-19-companies-and-verticals-at-risk-for-cyber-attacks/. [Accessed: 04-May-2020].

[17] TM, "Developing Story: COVID-19 Used in Malicious Campaigns," 2020. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-

and-malicious-domains. [Accessed: 04-May-2020].

[18] 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.

[19] CP, "Update: Coronavirus-themed domains 50% more likely to be malicious than other domains," 2020. [Online]. Available: https://blog.checkpoint.com/2020/03/05/update-coronavirus-themed-domains-50-more-likely-to-be-malicious-than-other-domains/. [Accessed: 04-May-2020].

[20] MalwareBytes, "Fake 'Corona Antivirus' distributes BlackNET remote administration tool." [Online]. Available: https://blog.malwarebytes.com/threat-analysis/2020/03/fake-corona-antivirus-distributes-blacknet-remote-administration-tool/. [Accessed: 04-May-2020].

[21] J. W. Han, O. J. Hoe, J. S. Wing, and S. N. Brohi, "A conceptual security approach with awareness strategy and implementation policy to eliminate ransomware," in *Proceedings of the 2017 International Conference on Computer Science and Artificial Intelligence*, 2017, pp. 222–226.

[22] Interpol, "COVID-19 cyberthreats," 2020. [Online]. Available: https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats. [Accessed: 04-May-2020].

[23] JHU, "Coronavirus COVID-19 Global Cases by the Center for Systems Science and Engineering (CSSE) at Johns Hopkins University (JHU)"," 2020. [Online]. Available: https://coronavirus.jhu.edu/map.html. [Accessed: 04-May-2020].

[24] M. Security, "Sophisticated COVID-19–Based Phishing Attacks Leverage PDF Attachments and SaaS to Bypass Defenses," *2020*. [Online]. Available: https://www.menlosecurity.com/blog/sophisticated-covid-19-based-phishing-attacks-leverage-pdf-attachments-and-saas-to-bypass-defenses. [Accessed: 05-May-2020].

[25] WHO, "Beware of criminals pretending to be WHO," 2020. [Online]. Available: https://www.who.int/about/communications/cyber-security. [Accessed: 04-May-2020].

[26] "Agari Cyber Intelligence Division (ACID)," 2020. [Online]. Available: https://acid.agari.com/. [Accessed: 04-May-2020].

[27] P. Peterson, "Business Email Compromise (BEC): Coronavirus a Costly New Strain of Email Attack," 2020. [Online]. Available: https://www.agari.com/email-security-blog/business-email-compromise-bec-coronavirus-covid-19/. [Accessed: 04-May-2020].

[28] MalwareBytes, "SMS Trojan," 2016. [Online]. Available: https://blog.malwarebytes.com/threats/sms-trojan/. [Accessed: 05-May-2020].

[29] GoldSparrow, "Oski Stealer," 2020. [Online]. Available: https://www.enigmasoftware.com/oskistealer-removal/. [Accessed: 05-May-2020].

[30] A. St. John, "It's Not Just Zoom. Google Meet, Microsoft Teams, and Webex Have Privacy Issues, Too.," 2020. [Online]. Available: https://www.consumerreports.org/video-conferencing-services/videoconferencing-privacy-issues-google-microsoft-webex/. [Accessed: 04-May-2020].

[31] T. Warren, "Zoom faces a privacy and security backlash as it surges in popularity," 2020. [Online]. Available: https://www.theverge.com/2020/4/1/21202584/zoom-security-privacy-issues-video-conferencing-software-coronavirus-demand-response. [Accessed: 04-May-2020].

[32] P. Boyden, "COVID-19 and privacy. Do we still have our privacy?," 2020. [Online]. Available: https://fraudwatchinternational.com/all/covid-19-and-privacy-do-we-still-have-it/. [Accessed: 04-May-2020].

[33] H. Saeed, "Personal Data of Thousands of Tiger Force Members Leaks," 2020. [Online]. Available: https://propakistani.pk/2020/05/04/personal-data-of-thousands-of-tiger-force-members-leaks/. [Accessed: 04-May-2020].

[34] 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