ISSN 2228-9860 eISSN 1906-9642 CODEN: ITJEA8

International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies

http://TuEngr.com

Cyber Security Threats During Covid-19 Pandemic

Rajesh Yadav[1]

[1] *Department of Computer Science, School of Engineering & Technology, BML Munjal University, INDIA.*
**Corresponding Author (Tel: +919312615797, rycs1980@gmail.com)*

Paper ID: 12A3Q

Volume 12 Issue 3

Received 24 November 2020
Received in revised form 08 January 2021
Accepted 19 January 2021
Available online 22 January 2021

Keywords:
Covid-19 epidemic; Cybersecurity, CT, Security threats, Privacy concerns; Mobile threat; Cyberattack; DDoS attack; Malicious Social Media Messaging.

Abstract

In 2020, Covid-19 was declared as a pandemic, affecting almost every part of societies, because of its impacts economy worldwide faced a big loss which included most of the economic sectors. During that time, technology played a very crucial role worldwide in keeping people connected. Educational institutions adopted online learning, employees started working from home, in addition to that, there has been a high demand for different types of businesses like online healthcare, delivery of food and grocery shopping, etc. Although technology helped in many different ways, we also observed a sudden increase in cyber-attacks. Attackers worldwide took the covid-19 situation as a big opportunity to perform various malicious activities and attacks for financial benefits and to promote their evil demands. This paper identifies major threats in cybersecurity that have taken place worldwide during the situation of covid-19. All these attacks played a big role in bringing harm to different sectors of our society.

Disciplinary: Computer and Network Security (Cyber Security & Threat Intelligence).

Cite This Article:

Yadav, R. (2021). Cyber Security Threats During Covid-19 Pandemic. *International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies, 12*(3), 12A3Q, 1-7. http://TUENGR.COM/V12/12A3Q.pdf DOI: 10.14456/ITJEMAST.2021.59

1 Introduction

World Health Organization declared a public health emergency on January 30th, 2020 with the novel coronavirus outbreak (WHO, 2020). On the next day i.e., January 31st, 2020 public health emergency was also declared in the US by Centre for Disease Control and Prevention (Worldometers, 2020). Corona Virus has spread to every country in the world thereby bringing normal day-to-day activities to a halt and killing many people worldwide (Worldometers, 2020).

Corona disease has been considered (WHO, 2020). To control the spread, almost all countries closed schools, colleges, and universities. Classes are being taken in the online mode by the faculties worldwide on a huge scale. In addition to that, all assessments and evaluations have also been done in the online mode on many different platforms (Bajema et al.,2020; Burgess et al., 2020). Daily life activities started being affected as the physical workplace was being shifted to a virtual workplace, it happened worldwide in many organizations as the reports of pandemic getting worse spread (Accenture, 2020).

One good thing which happened during this time is that communication was at its peak and different tools and technologies have helped people to perform their work and continue to stay in touch with their colleagues, family, and friends. Microsoft team, Google Meet, and ZOOM king of applications saw a very big increase of new and new people signing to their applications (Perez, 2020).

However, this also brought the attention of malicious attackers and they started performing different cybersecurity attacks (Humayun et al., 2020). Along with performing their work during Covi-19 time, organizations also must deal with the security demands which have aroused due to different attacks. Data that is very sensitive as well issues related to privacy have to be considered by the organization (Berman et al.,2020). US FBI gave a strong warning that using the Zoom application might bring serious security concerns as the configurations of zoom were not considered safe, as a result of which Zoom was banned in many countries and many different organizations worldwide (Vigliarolo, 2020). Therefore, it is now the best time to mitigate and avoid cyber threats to ensure that there are no privacy concerns and malicious attackers do not succeed in their evil work (Brohi, 2020).

2 Covid-19 Affected Domains of Society

2.1 Healthcare Systems

Healthcare systems of today's world are based on ICT applications which include nurses, physicians, patients, pharmacists as well as a wide range of healthcare services which we refer to as e-healthcare. During the COVID-19 situation, this sector is badly affected as it has the most vulnerable and targeted systems. We can think it off like a situation that if anything bad happens, it might lead to the loss of a human life which is very precious. A DDoS attack was performed by attackers on the Department of Health and Human Services in the US, its servers were badly affected by the attack (Stein et al., 2020).

2.2 Financial Services

Financial markets around the world got fallen to the lowest points during the corona pandemic, oil prices also got fallen due to the non-collapse of the economy and no demand for crude oil (Stevens, 2020). As a result, different oil-producing countries saw their economy coming to a very low level. Many experts predicted that a recession will be faced by the economy worldwide during the pandemic time and financial companies are highly vulnerable to cyber threats like malware, phishing, DDoS. (Stevens, 2020; Dion et al., 2020).

2.3 Media and Government Platforms

Both governments as well as media outlets- faced a difficult time during the COVID-19 pandemic as they are responsible for bringing the real news to a public platform and timely information must be given. Any misleading information and delay might lead to a dangerous situation and a serious panic can rise so a proper check as well as the distribution of information by both government and media agencies had to be ensured. Malicious attackers can explore the vulnerabilities in the platforms used by agencies and then they can perform attacks thereby heavily affecting and manipulation the information which if get spread will cause a bug problem in society. Misleading information can turn the people against the government and serious problems may arise during that time (Ren et al., 2020).

3 Cyber Threats During the Pandemic

We have seen that cyber security has now become a very challenging aspect with the technological advancements nowadays. Attackers and hackers are commonly seen targeting the vulnerabilities and take benefit from any emergency in many domains of society like healthcare, financial, etc. specifically in a situation where people worldwide are worried by the ongoing situation. where many different assets are highly vulnerable and are being continuously targeted by the malicious attackers worldwide. The Corona pandemic situation is the same situation Evil deeds are satisfied by the malicious attackers worldwide by taking this coronavirus pandemic as a god opportunity and this pandemic is being used as a tool to perform different attacks and scams worldwide. From the report of an agency, it has been reported that during this corona pandemic, around 600 malware atatcks, 800k spam messages and 50k hits on malicious websites have been observed since May 2020 (Cook,2020). Also, starting from February to March 2020, spam emails numbers have increased 300 times and 300% increase in malicious URLs. US is the top country for spam detection as well as malware and the majority of target users are using them from the US (Cook,2020). Figure 1 shows the major cybersecurity threats during the COVID-19 pandemic.

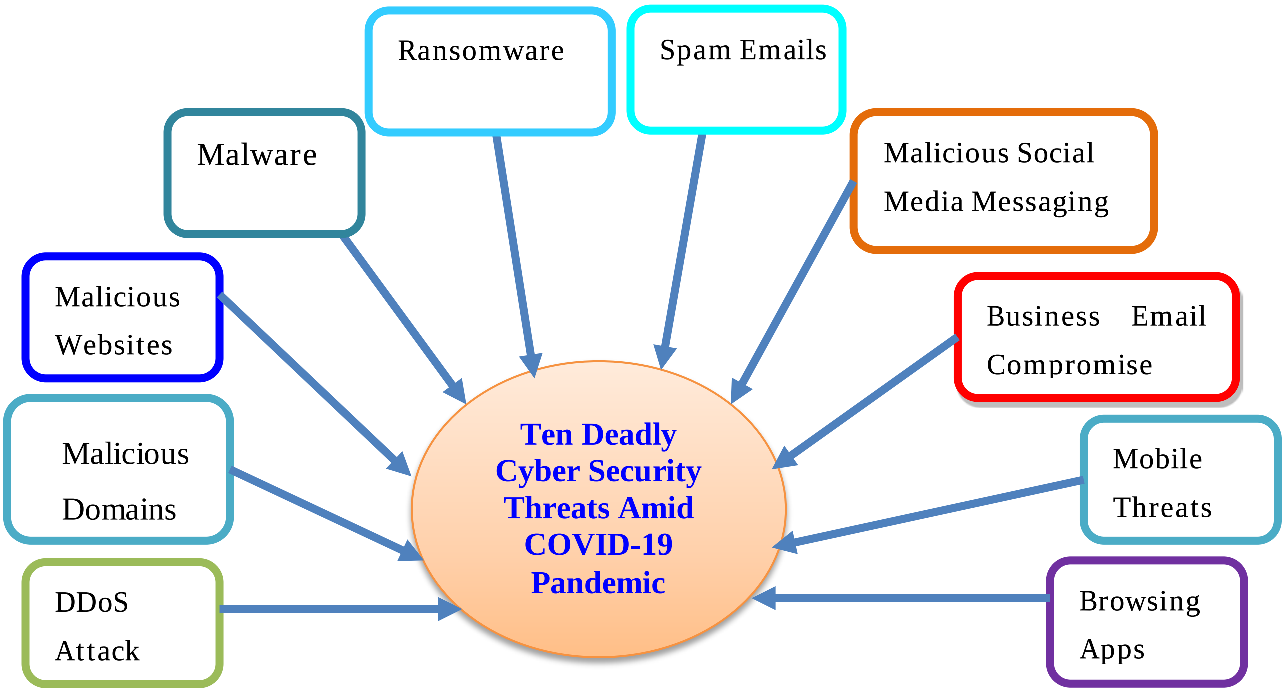
Ransomware
Spam Emails
Malware
Malicious Social Media Messaging
Malicious Websites
Business Email Compromise
Malicious Domains
Mobile Threats
DDoS Attack
Browsing Apps
Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic

Figure 1: Cyber Security Threats during COVID-19 Pandemic (Khan, 2020)

3.1 DDOS Attack

DDoS (Distributed Denial of Services) has been observed as a rapidly increasing attack in many governments and healthcare companies. During the recent corona pandemic (TM,2020). In this DDoS attack, the company websites are flooded with fake and bot users by the attackers thereby resulting in the crashing of those websites and heavily affecting their normal operations. For example, during this pandemic US Department of Health and Human Services has been the target where the attackers flooded the severs of that organization with millions of users at one time.

3.2 Malicious Domains

Recently on the Internet, a large number of registered domains have seen the corona virus word appearing on them, and day by day more increase in the same has been observed those and many other registered domains. Cyber attackers create new websites and launch spam campaigns as well as other attacks like phishing, malware injection, and perform DOS kind of attacks affecting the servers of many organizations (Khan et al.,2020).

3.3 Malicious Websites

There has been a big expansion in the number of websites that claim to be applications that are supposed to protect users from COVID-19 (Malwarebytes, 2020).

3.4 Malware

Malwares are continuously being spread by cyber-criminals worldwide in this present corona pandemic situation. Through many different websites and links, if the user opens the websites or clicks on a link, a trojan is being injected into the victim machine which later starts creating many different cyber issues (Malwarebytes, 2020; Han et al., 2020). John Hopkins University designed an interactive dashboard that reports the information and fatalities of the novel corona virus (Interpol, 2020). Unfortunately, hackers took befit from it and injected a trojan into it leading to problems with the victims who downloaded that dashboard on their machines.

3.5 Ransomware

Many ransomware attacks are being launched by malicious attackers where the victims were from different domains of society like hospitals, educational organizations as well as government agencies. The ransomware once starts its operation locks the sensitive files on the server of the victim and then asks for financial benefit to provide back access to the sensitive data on those servers (Han et al., 2020). In fact, attackers are now offering ransomware as a service.

3.6 Spam Emails

Spammers and hackers have always used spam emails on a very big scale for getting their purpose satisfied. During the corona pandemic, spam emails containing corona-related content have been shared with many users worldwide thereby affecting their normal operations (JHU, 2020). The end of the email address basically ends with the company 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 (M.Security, 2020).

3.7 Malicious Social Media Messaging

Social media in the present times is in very easy reach of every person. Attackers use it as a good opportunity to use these platforms for performing their malicious activities like injecting a trojan on the victim machine etc. Also, it has been observed that the hackers have used the opportunity of offering free Netflix account for example to the users and by giving them attractive offers, they hack the machines of those users and make them victims later on.

3.8 Business Email Compromise

It has been recently observed that business emails have been compromised by hackers (Peterson, 2020). These types of attacks have been performed by some specific organization like the ancient tortoise. The hackers first start by targeting th4e bank accounts and then they use this information to convincing customers to change their account details and send them emails for changing their bank account intimation (Peterson, 2020). Corona virus disease has been used heavily as-business email compromise tool and it has affected many users worldwide.

3.9 Mobile Threats

We live in a world with so many smartphone users and it is right to be said that life is impossible without phones and gadgets. This turns out to be a good opportunity for attackers who are always looking for hacking the mobile machines of people worldwide. Most of our operations are being done through our smartphone and our credentials are also being stored on the phone which makes it easy for the attackers to hack our account information after accessing our smartphones. Trojans are being continuously injected into the victims' smartphones thereby controlling the phone remotely from any location worldwide.

3.10 Browsing Apps

Web browsers have become a daily using software nowadays and every person uses it who has Internet access. 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.

4 Conclusion

With the use of different technologies, people are always connected to each other. It is good for sharing information as well as performing other activities like using social media, working from home, etc., but sometimes this turns out to be bad and it results in some harmful effect on the life of people. Worldwide cyber-attacks are growing rapidly and we have seen a high rise in the number of attacks during the situation of the covid-19 pandemic. Our life becomes easy with the help of technologies, but on the other side, it also brings the attention of attackers who can explore vulnerabilities and then perform an attack. There have been very serious concerns about our privacy and security with the recent corona outbreak. In this paper, I have shown how cyber-attacks have affected different categories of people in many different ways and we need to look seriously into the mitigation and preventive measures of all these threats so that our need of staying connected through technologies in the future does not bring any more danger to us.

5 Availability of Data and Material

Data can be made available by contacting the corresponding author.

6 Acknowledgment

I would like to express my sincere appreciation to BML Munjal University for the support towards the research paper.

7 References

Accenture. (2020). COVID-19:Managing the human and business impact of coronavirus.:https://www.accenture.com/my-en/about/company/coronavirus-business-economic-impact (Accessed May 2020).

Bajema, K. L., et al. (2020). Persons evaluated for 2019 novel coronavirus— United States, January 2020, Morb. Mortal. Wkly. Rep., 69(6), 166.

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

Brohi, S. N., N. Z. Jhanjhi, N. N. Brohi, and M. N. Brohi. (2020). Key Applications of State-of-the-Art Technologies to Mitigate and Eliminate COVID-19.

Burgess, S. and H. H. Sievertsen. (2020). Schools, skills, and learning: The impact of COVID-19 on education, VoxEu. org, vol.1.

Cook, A. (2020). COVID-19: Companies and Verticals at Risk for Cyber- Attacks. https://www.digitalshadows.com/blog-and-research/covid-19-companies-and-verticals-at-risk-for-cyber-attacks (Accessed May 2020).

CP. (2020). Update: Coronavirus-themed domains 50% more likely to be malicious than other domains. https://blog.checkpoint.com/2020/03/05/update-coronavirus-themed-domains-50-more-likely-to-be-malicious-than-other-domains (Accessed May 2020).

Dion, Y., and S. N. Brohi. (2020). An Experimental Study to Evaluate the Performance of Machine Learning Algorithms in Ransomware Detection. J. Eng. Sci. Technol., 15(2), pp.967-981.

Han, J. W., O. J. Hoe, J. S. Wing, and S. N. Brohi. (2017). 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, pp. 222–226.

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

Interpol. (2020). COVID-19 cyberthreats. https://www.interpol.int/en/Crimes/Cybercrime /COVID-19-cyberthreats (Accessed May 2020).

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

Khan, N. A., S. N. Brohi, and Jhanjhi. NZ. (2019). UAV's Applications Architecture Security issues and Attack Scenarios: A Survey, in 1st International Conference on Technology Innovation and Data Sciences (ICTIDS).

Khan, N., S.N. Brohi and N.Zaman. (2020).. Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic. http://www.researchgate.net/publication/341324576_Ten_Deadly_Cyber_Security_Threats_Amid_COVID 19_Pandemic (Accessed July 2020).

Malwarebytes. (2020). Fake Corona Antivirus distributes Black NET remote administration tool. https://blog.malwarebytes.com/threat-analysis/2020/03/fake-corona-antivirus-distributes-blacknet-remote-administration-tool (Accessed: May 2020).

M-Security. (2020). Sophisticated COVID-19-Based Phishing Attacks Leverage PDF Attachm- ents and Saas to Bypass Defenses. https://www.menlosecurity.com/blog/sophisticated-covid-19-based-phishing-attacks-leverage-pdf-attachments-and-saas-to-bypass-defenses (Accessed May 2020).

Perez, S. (2020). Videoconferencing apps saw a record 62M downloads during one week in March. https://techcrunch.com/2020/03/30/video-conferencing-apps-saw-a-record-62m-downloads-during-one-week-in-march (Accessed May 2020).

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

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

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

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

TM. (2020). Developing Story: COVID-19 Used in Malicious Campaigns. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains (Accessed May 2020).

Vigliarolo. (2020). Who has banned Zoom? Google, NASA, and more, available: https://www.techrepublic.com/article/who-has-banned-zoom-google-nasa-and-more (Accessed May 2020).

WHO. (2020). Statement on the second meeting of the International Health Regulations (2005) Emergency Committee regarding the outbreak of novel coronavirus (2019-nCoV). World Health Organization http://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 May 2020).

Worldometers. (2020). Reported Cases and Deaths by Country, Territory, or Conveyance. https://www.worldometers.info/coronavirus/#countries (Accessed May 2020).

Dr. Rajesh Yadav is an Assistant Professor in the Department of Computer Science at BML Munjal University, India. His current interests involve Cyber Security and Computer Networks.