Innovative Computing Review (ICR)
Volume 1 Issue 2, Fall 2021
ISSN(P): 2791-0024 ISSN(E): 2791-0032
Journal DOI: https://doi.org/10.32350/icr
Issue DOI: https://doi.org/10.32350/icr/0102
Homepage: https://journals.umt.edu.pk/index.php/icr

Article: **COVID-19 and Cyber Crime: Types of Attacks and an Outline of Related Crimes**

Author(s): Saman Liaqat, Hassan Kaleem

Affiliation: KIT Cloud Solutions Limited, London, United Kingdom

Citation: L. Saman, K. Hassan, "COVID-19 and Cyber Crime: Types of Attacks and an Outline of Related Crimes", *Innova Comput Rev*, vol. 1, no. 2, pp. 71–84, 2021. https://doi.org/10.32350/icr/0102/04

Journal QR

Article QR

Farzana Kausar

A publication of the
School of Systems and Technology
University of Management and Technology, Lahore, Pakistan

COVID-19 and Cyber Crime: Types of Attacks and an Outline of Related Crimes

Saman Liaqat[1]*, Hassan Kaleem[1]

ABSTRACT: The COVID-19 pandemic has unprecedentedly affected life on earth ever since it broke out in 2019. The World Health Organization (WHO) has confirmed 7.5 million COVID-19 positive cases and 430,241 deaths caused by the novel disease, due to which quarantine was imposed on hundreds of thousands of people around the globe . It has not only negatively affected businesses and economies, but it has also shaken the foundation of the technology-driven society because of the rise in cybercrime. For this reason, the techniques and methods used by cyber-criminals and their handiwork is being analyzed, worldwide. Cybercrime has also challenged the information system of healthcare, greatly affecting pharmaceutical firms, hospitals, and various health departments in the US, as well as WHO and many other firms. This paper highlights the range of cybercrimes committed worldwide during the pandemic by presenting an outline of the incidents during the COVID-19 pandemic.

INDEX TERMS: COVID-19, cybercrime, cyber security, healthcare, work from home

I. INTRODUCTION

The pandemic broke out in 2019 and soon became a worldwide crisis. It made people homebound for protection, arising the need to run businesses, educational institutions and other official activities through internet from the hideouts. . This online dependence led to excessive use of internet by people. Among them were cybercriminals who had ample time to negatively use internet for their nefarious designs from the comforts of their homes. It was reported that 3 to 4 unique types of crime were a daily routine. These included scams of imitating public firms (e.g. World Health Organization) and organizations (super-stores and airways) [1], conducting Personal Protective Equipment (PPE) fraud [2], targeting support platforms[3]

[1]KIT Cloud Solutions Limited, London, United Kingdom
*Corresponding Author: Samanliaqat100@yahoo.com

and providing cures for Corona virus. Generally, common people were targeted by these scams. But tons of individuals working from home too were affected. The challenges and concerns of the cybersecurity faced during this pandemic led to new heights of security threat never seen before. Cybercriminals mounted their attacks by taking advantage of the worldwide crisisand turned it into an opportunity. The domestic internet-based working during the pandemic also revealed software vendors' level of un-preparedness for the security of their product which certainly is their main concern. Healthcare firms have also fallen victim to cybercriminals, creating voluminous challenging situations for the health information system. It is found that malware, phishing and Denial of Service (DoS) attacks were common in the healthcare sector. A meeting was held on April 8, 2020 [4] to assess how these criminals were exploiting the ongoing crisis. The issues discussed were malware attacks, phishing and scams, and social media platforms like Microsoft and Zoom [5].

II. SYSTEMATIC LITERATURE REVIEW

Several studies have already been conducted to examine cybercrime committed worldwide during the pandemic. Several of them too have been reviewed for this research. The data and literature regarding this investigation is presented in the following headings:-

1.TYPES OF ATTACKS
2.OUTLINE OF ATTACKS
3.ATTACKS ON HEALTHCARE FIRMS

A. Types of Attacks

1) Cybercrime is Directly Related: to technology. Cybercriminals exploit technology in their favour when the unwary or law abiding people are panicked, desperate or scared. When COVID-19 created these same conditions for people, cybercriminals found it an opportune time to strike globally without any let or hindrance. A Trend Micro research shows nearly 737,000 global malware attacks, 907,000 spam messages, and 48,000 malicious links from the very beginning of April, 2020 [6].

Furthermore, the February to March 2020 period witnessed a 220-time increase in e-mail spam, and 260% in malicious URLs. The topmost site to detect malware and spam is the United States as most users are accessing them (the ttacks) from there. Fig 1 shows the highest 10 attacks launched during the pandemic.

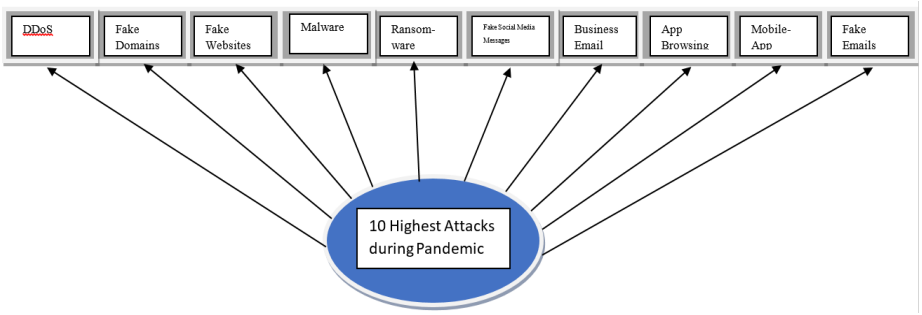

Fig. 1. Ten highest attacks during the pandemic

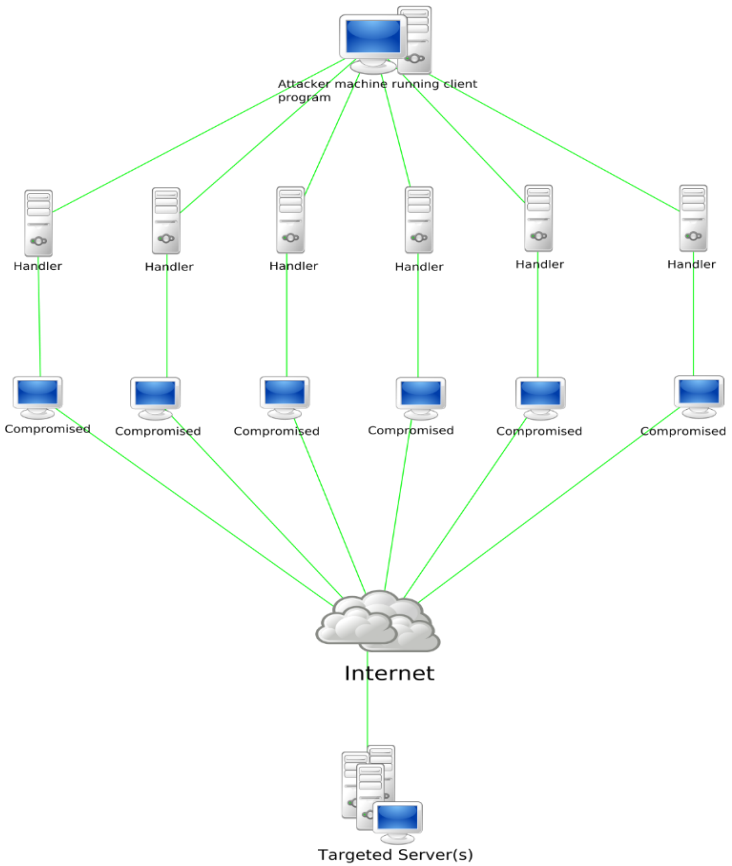

Fig. 2. Distributed denial of service

2) DDoS: The figure shows a significant increase in the distribute denial of service attack during the pandemic. The sector affected by this attack is the government and a healthcare firm

for which the threat continued to grow. To damage the normal working of the system and the communication channel, cybercriminals flood the websites and systems of these firms by fake users. Of late, the website of the Department of Health and Human Service (DHHS), USA, was infected by the denial of service attack by flooding thousands of users on a spot [7].

3) Fake Domains: Cyber Criminals are making various domains by the name of COVID-19 and Corona virus. Some of them are legal sites but some are traps of cyber criminals through which they are spreading malware and phishing to destroy servers. It is reported that over 4,000 domains were registered during the COVID-19. Hackers extract particular data and information and misue them for their nefarious designs [8].

4) Fake Websites: Many websites entitled www.antivirus-COVID19.com and www.corono-antivirus.com pop up promising to protect users against virus. However, malware sneaks into the system when people install the app under the wrong impression that this is to protect them against the virus. This malware attack causes devices to run on Botnet. It also helps launch DDoS attacks, download remote files, run fake scripts, extract passwords/ browser cookies [9].

In the United States Department of Justice, a fake website (www.coronavirusmedicalkit.com) appeared that claimed supplying WHO-approved vaccine kits for COVID-19. It happened when validly WHO approved COVID-19 vaccines were still not available in the market [9]. This website demanded US$ 4.95 for one kit, asking users to enter their credit card information to continue with the transaction.

5) Malware: Computer viruses, worms, Trojan horse, spyware and ransom-ware viruses are malware attacks. Cybercriminals and APT groups target vulnerable humans and systems through spreading different kinds of malware via electronic-mail (e-mail) and websites. In fact, 94% of computers damaged through malware were inflamed through an e-mail. It is important for the establishments, mainly affected by cybercrime during the pandemic, to have complete knowledge of the varieties of malware that include ransom-ware [10].

6) Ransom-ware: Cyber criminals have carried out ransom-ware attacks against hospitals, medical centers, educational institutions and public establishments. Criminals believe that these firms are easy targets of such attacks. Ransom-ware infects the system through email attachments, links, exploitation of the system vulnerabilities with corrupted credentials, and employees of the target [6].

A new ransom-ware called Corona-Virus penetrated the website of Fake Wise Cleaner (system optimization software) after it was downloaded. Victims are lured into downloading bogus installation files from the website. Upon installation, this malware steals passwords, encrypts data that cannot be decrypted later, and system information [11].

7) Fake Social Media Massage: Social media is getting popular day by day for being in the reach of every person. Hackers find it suitable for their criminal activity, using sites like Facebook and WhatsApp for their purpose. There are various examples of unleashing scams and phishing spam through Facebook and various apps. Scams often persuade victims to sign up for free like Netflix's free premium account. When the victims click on the link, they are taken to a social media phishing site. In few cases, the victims are prompted to submit their account details. They are tricked into sharing their login information or installing malware on their systems, mobile devices, web browsers to steal information and cookies [12].

8) Business Email Assault: The Agari Cyber Intelligence Division [13] reported that an intruder using COVID-19 attacked a bank via the email intrusion technique. The attack was launched by cybercrime organization known as “Ancient Tortoise” which was also involved in various past BEC incidents. In such attacks the bank account is penetrated to get information of its customers. Then the attacker sends emails to the hacked addresses claiming a change in the banking information and payment methods due to the Corona virus. It is claimed that the attacker represents a legitimate firm or company [14].

In today's environment, business email scams use Corona-virus as a tool. Through phishing, an attacker tricks the targeted people or firms into trading under the guise of alegitimate employee of the same company.

9) Application Browsing: Rapid development of technology has made it easy to access internet. Browsers are being used on a daily basis. There exist software that can be used by anyone having internet access. A new cyber-attack was discovered spreading a fake COVID-19 intelligence app claimed to have been provided by WHO. Hackers access the Domain Name Service (DNS) settings on D-Link or Linksys routers and automatically open a browser to display messages or warnings from malicious applications. The alert will only display a title of "Download COVID-19 Notification Application". When a person clicks the download button, the "Oski Information Stealer" malware is installed in his or her system. This malware extracts browser cookies, saved passwords, browser history, transaction information and other crucial information [15].

10) Mobile Application: Thanks to the technological advancements, the number of mobile phone users is increasing at a mammoth speed. Life without smart phones and devices looks difficult.y. But cybercriminals found it easy to misuse these devices during the pandemic. The app called COVIDLock (ransomware) comes from a malicious android app that tracks COVID-19 cases.The criminals are reported to have demanded $100 in Bitcoin from each use. The users are threatened with deletion of phone data and theft of social media account information in case of non-payment in two days [6].

11) Fake Email: The hackers use spam emails, both in normal and emergency situations, to fulfill their illegal desires. During the current pandemic situation, it has been observed that emails regarding Corona virus containing malicious attachments were sent to users in abundance. Fake domain names were used to trick victims into believing their emails were from WHO, asking them to donate things like Bitcoins. For example, email addresses often end with your organization's website so people can see who you are. And they authenticate that one is communicating with the right person or organization. Intruders use emails like corona-virus fund@who.org. The official WHO website www.who.int finishes with "int" instead of "org". Users who do not check the email can fall victims [13].

B. Outline of Attacks

To help build the outline, we have searched different articles on cyber attacks in various countries during the pandemic. The information is collected and presented in outline (Fig.3).

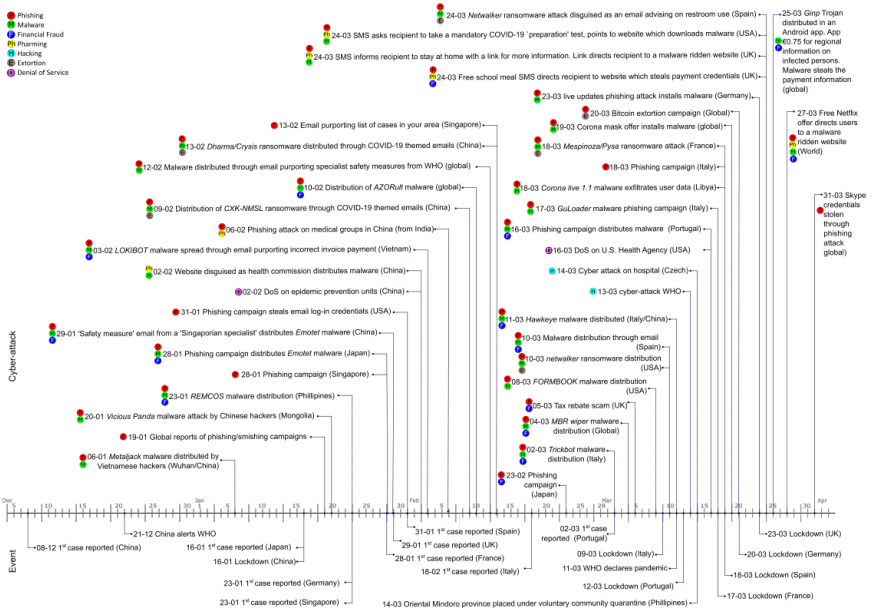

Fig. 3. Outline of attacks amid COVID-19 in various countries

C. Attacks on Healthcare Firms

The healthcare sector faced various attacks in the beginning of the COVID-19 pandemic. This research has chosen famous cyber attacks with detailed information. The findings are discussed as follows:-

- The main COVID-19 testing centre of the central European landlocked Czech Republic, known as "Brno University Hospital," was infected by ransomware attack. It was confirmed early in the morning that the hospital systems have gotten infected by the ransomware. All the computers were failing. And after detecting the virus, the systems were promptly disconnected and closeddown [16].
- In the United States, the Department of Health and Human Services was infected by a Distributed Denial of Service (DDoS) attack which disrupted the department's responses. The servers were found to be overloaded by this

attack [17]. This department was tasked to provide vital healthcare services to general public. The attackers intended to obstruct the department's response to the pandemic. But it declared that the attack was intercepted, disallowing it to penetrate the internal network or extract any data.

- Gilead Sciences, the maker of Corona virus vaccines was infected by the e-mail intrusion attack. Its employees were targeted by a fraudulent e-mail page made to steal passwords. It has been reported that the attackers intended to disrupt e-mail accounts of the employees of the organization through messages pretending to be from journalists [18].
- Romanian hospitals were also targeted by ransomware attack. Cybercriminals used e-mail named COVID-19 to infect the hospitals' systems with ransomware virus. Their target was to create dissent against the COVID-19 isolation by the nation. The criminals used malware like Trojan horse, SQL injection tools, fraudulent websites, and the like to extract information and pull down servers. It is reported that the intention of the hackers was to damage the hospital functionality by infecting computers and encrypt files [19]. This attack failed as the cybercriminals were nabbed by the Romanian law enforcers. Healthcare supply chains have also faced these attacks. In the USA, the Federal Bureau of Investigation (FBI)[20] warned that a supply chain sector will be targeted by malware. A malware known as KWANPIRS, a Trojan, was found t damaging networks of targeted organizations in Asia, the United States, Europe, and the Middle East. The targeted supply chain elements include cyber-physical devices of the healthcare firms. Later, the FBI cautioned against future such attacks on the healthcare firms.

The survey of the above information shows that the healthcare firms are the main t target of the cybercriminals. The cybercriminals used the COVID-19 pandemic as an opportunity to target people and systems through malware, ransomware, DDoS, and phishing. The healthcare sector was especially attacked. The cyber attacks disrupt healthcare services and e integrity and confidentiality of the healthcare information.

III. OBJECTIVES

The objective of this research is to support ongoing research on how these attacks were launched, to understand their mechanism so that they are tackled if attempted in future. Another objective is to analyze cyber security challenges for various departments/sectors.

IV. METHODOLOGY

This work was completed by searching relevant published papers available on PubMed and Google scholar. These articles were retrieved by placing the term "Cyber Attacks during COVID-19" in the relevant search engine. This resulted in locating 11,800 published papers on Google Scholar while 300 relevant results were shown on PubMed. Only five relevant articles were found on Google Scholar.

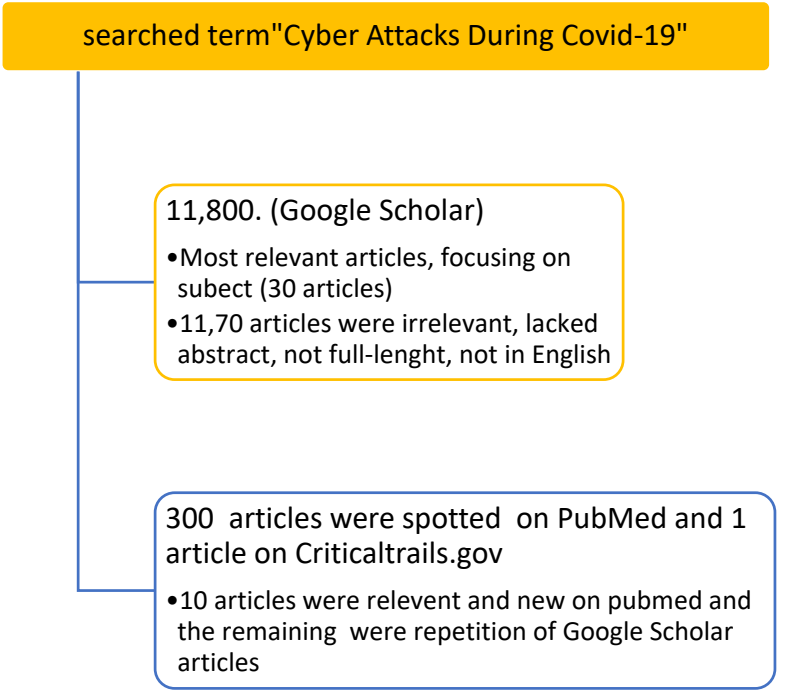

Fig. 4. Shows details of the process

Furthermore, our aim was to peruse the latest research. We excluded the repeated articles and took into account 200 articles. Further segregation was made, picking articles which were

available in toto and written in English. Only research papers and blog articles were picked, whereas data included in books, letters to editor, short communication and patent were excluded. Similarly, articles without any abstract were also not considered.

V. CONLCUSION AND FUTURE WORK

This paper discussed the types of cyber attacks launched during the COVID-19 pandemic and the vulnerabilities of the targets. Cyber criminals have taken advantage of the pandemic to attack vulnerable individuals and systems. Pandemic has enhanced unemployment worldwide. Additionally, it has given cybercriminals the opportunity to plunder others.

For many reasons, healthcare businesses have been the most common target of cyberattacks during the pandemic. As a result, it is important for the healthcare institutions to improve the security of their critical data. Many healthcare firms applied temporary solutions to deter the cyber threats during the pandemic. They should opt for long-term solutions and come up with sufficient cyber security resources to protect against future cyber threats.

Servers and VPNs play an essential role in ensuring future cyber security. Cyber criminals are well aware of the inadequate cyber security systems that individuals have at home. For this reason, people face many challenges when working from home. Such targeted persons, therefore, need to find secure solutions for cyber security.

A. Limitations

On several instances, the current researchers found that the web pages of a referenced article were corrupt and altered their information under the pretext of updating it. In this paper, cyber attack reports are divided into two types, that is, those that mention cyber attacks without giving the date of the attack and those that give the date of the attack. If the date of the attack is not given, the date mentioned in the article is taken as the date of its publication. This is being pointed out to ensure the accuracy of the present information, so that it is understood in its true perspective. Our outline gathered maximum data but it does not mean that we have collected an exhaustive list of attacks. Despite all these shortcomings, we have tried our best to explore the available resources to portray the reality of

cybercrime as accurately as possible.

REREFENCES

[1] Threat Intelligence Team, (2021). "*Cybercriminals impersonate World Health Organization to distribute fake coronavirus e-book*", Malwarebytes Labs. https://blog.malwarebytes.com/social-engineering/2020/03/cybercriminals-impersonate-world-health-organization-to-distribute-fake-coronavirus-e-book/ (accessed Jun. 15, 2021).

[2] "Pandemic profiteering: how criminals exploit the COVID-19 crisis," Europol. https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-COVID-19-crisis (accessed Jun. 15, 2021).

[3] "Live Coronavirus Map Used to Spread Malware – Krebs on Security," Prof Point. https://krebsonsecurity.com/2020/03/live-coronavirus-map-used-to-spread-malware/ (accessed Jun. 15, 2021).

[4] "Advisory: COVID-19 exploited by malicious cyber actors." https://www.ncsc.gov.uk/news/COVID-19-exploited-by-cyber-actors-advisory (accessed Jun. 15, 2021).

[5] H. S. Lallie *et al.*, "*Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic*," Comput. Secur., vol. 105, p. 102248, Jun. 2021, https://doi.org/10.1016/j.cose.2021.102248

[6] "*Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic*." https://www.techrxiv.org/articles/preprint/Ten_Deadly_Cyber_Security_Threats_Amid_COVID-19_Pandemic/12278792 (accessed Jun. 03, 2021).

[7] "*Cyber-Attack Hits U.S. Health Agency Amid COVID-19 Outbreak - Google Search.*" (accessed Jun. 03, 2021).

[8] "*Update: Coronavirus-themed domains 50% more likely to be malicious than other domains - Check Point Software*." https://blog.checkpoint.com/2020/03/05/update-coronavirus-themed-domains-50-more-likely-to-be-malicious-than-other-domains/ (accessed Jun. 16, 2021).

[9] "*Error Page - Trend Micro Inc*." Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names- (accessed Jun. 03, 2021).

[10] B. Pranggono and A. Arabo, "COVID-19 pandemic cybersecurity issues," *Internet Technol. Lett.*, vol. 4, no. 2, p. e247, 2021, https://doi.org/10.1002/itl2.247

[11] "COVID-19 cyberthreats." https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats (accessed Jun. 16, 2021).

[12] "Error Page - Trend Micro Inc." https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names- (accessed Jun. 16, 2021).

[13] "Cybersecurity." https://www.who.int/about/communications/cyber-security (accessed Jun. 03, 2021).

[14] "Business Email Compromise (BEC): Coronavirus a Costly New Strain of Email Attack," *Agari*, Mar. 19, 2020. https://www.agari.com/email-security-blog/business-email-compromise-bec-coronavirus-COVID-19/ (accessed Jun. 03, 2021).

[15] "*Oski Stealer Removal Report*." https://www.enigmasoftware.com/oskistealer-removal/ (accessed Jun. 03, 2021).

[16] "*Cyberattack on Czech hospital forces tech shutdown during coronavirus outbreak*," Healthcare IT News. https://www.healthcareitnews.com/news/emea/cyberattack-czech-hospital-forces-tech-shutdown-during-coronavirus-outbreak (accessed Jun. 22, 2021).

[17] "*Cyberattack Hits HHS During Coronavirus Response - Bloomberg*." https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-COVID-19-response (accessed Jun. 22, 2021).

[18] J. S. Bing Christopher, "*Exclusive: Iran-linked hackers recently targeted coronavirus drugmaker Gilead - sources*," Reuters, May 08, 2020. Accessed: Jun. 22, 2021. [Online].

Available: https://www.reuters.com/article/us-healthcare-coronavirus-gilead-iran-ex-idUSKBN22K2EV

[19] "*Hackers preparing to launch ransomware attacks against hospitals arrested in Romania*, ZDNet." https://www.zdnet.com/article/hackers-preparing-to-launch-ransomware-attacks-against-hospitals-arrested-in-romania/ (accessed Jun. 22, 2021).

[20] C. Cimpanu, "*FBI re-sends alert about supply chain attacks for the third time in three months*," ZDNet. https://www.zdnet.com/article/fbi-re-sends-alert-about-supply-chain-attacks-for-the-third-time-in-three-months/ (accessed Jun. 22, 2021).