1-1-2023

COVID-19 pandemic and the cyberthreat landscape: Research challenges and opportunities

Heba Saleous
United Arab Emirates University

Muhusina Ismail
United Arab Emirates University

Saleh H. AlDaajeh
United Arab Emirates University

Nisha Madathil
United Arab Emirates University

Saed Alrabaee
United Arab Emirates University

See next page for additional authors

Digital Communications and Networks xxx (xxxx) xxx

Contents lists available at ScienceDirect

Digital Communications and Networks

journal homepage: www.keaipublishing.com/dcan

COVID-19 pandemic and the cyberthreat landscape: Research challenges and opportunities

Heba Saleous [a], Muhusina Ismail [a], Saleh H. AlDaajeh [a], Nisha Madathil [a], Saed Alrabaee [a,1,*], Kim-Kwang Raymond Choo [b], Nabeel Al-Qirim [c]

[a] Information Systems and Security, College of IT, United Arab Emirates University, Al Ain, United Arab Emirates
[b] Department of Information Systems and Cyber Security, The University of Texas at San Antonio, San Antonio, TX, 78249, USA
[c] College of Technological Innovations (CIT), Zayed University, UAE

ARTICLE INFO

Keywords:
COVID-19
Cyberattacks
Security and privacy
Mitigation
Potential solutions

ABSTRACT

Although cyber technologies benefit our society, there are also some related cybersecurity risks. For example, cybercriminals may exploit vulnerabilities in people, processes, and technologies during trying times, such as the ongoing COVID-19 pandemic, to identify opportunities that target vulnerable individuals, organizations (e.g., medical facilities), and systems. In this paper, we examine the various cyberthreats associated with the COVID-19 pandemic. We also determine the attack vectors and surfaces of cyberthreats. Finally, we will discuss and analyze the insights and suggestions generated by different cyberattacks against individuals, organizations, and systems.

1. Introduction

Since the discovery of the Novel Coronavirus (also known as COVID-19 and SARS-CoV-2), more than 12.5 million confirmed infections have been reported worldwide. In a sample of about 6 million patients, an estimated 400,000 died [1]. The statistics are increasing at the time of this research. For example, according to the data provided by the World Health Organization (WHO), more than 4.5 million new cases were reported in the week of April 5, 2021, and the number of new deaths increased for the fourth consecutive week, an increase of 7% with more than 76,000 new deaths reported.[2] In response, governments have introduced measures such as lockdowns, quarantines, remote work, distance learning, social distancing, and travel bans [2]. As a result, individuals spend significantly more time on personal devices because professional, academic, and personal activities are now being conducted virtually [3–7].

Cybercriminals find the uncertainty brought by changing daily habits opportune and the increased virtual existence is converted into available attack vectors [8,9]. According to data from the Federal Bureau of Investigation (FBI), it is reported that during the pandemic, cybercrime increased by 400%.[3] Interpol has also reported that during the COVID-19 pandemic, cybercrimes increased.[4]

This reinforces the importance of user education and training to increase their cybersecurity awareness. Hence, the focus of this paper is to investigate the various cyberthreat vectors associated with the pandemic and explore potential preventive measures. Specifically, when studying COVID-19-related cyberattacks, we will also explain the distribution of the attacks and try to understand the attacker's goals and attack surfaces. This will contribute to the development of mitigation strategies. A summary of the topics covered is also described in Fig. 1.

In the next section, we will briefly review existing cybersecurity research related to COVID-19.

2. Existing research

During the COVID-19 pandemic, the significant increase in online communication also led to a surge in malicious cyber activities. This has aroused the interest of the research community, as evidenced by the number of articles summarized in Table 1.

The ultimate goal of cybersecurity is to protect assets from

* Corresponding author.
E-mail address: salrabaee@uaeu.ac.ae (S. Alrabaee).

[1] The work of Saed Alrabaee was supported by the United Arab Emirates University Start-up Grant G00003261

[2] https://www.who.int/publications/m/item/weekly-epidemiological-update-on-covid-19–13-april-2021.

[3] https://securelogix.com/news/fbi-sees-400-spike-in-cyber-crime-reports-during-coronavirus-pandemic/.

[4] https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19.

https://doi.org/10.1016/j.dcan.2022.06.005
Received 9 November 2020; Received in revised form 2 June 2022; Accepted 12 June 2022
Available online xxxx

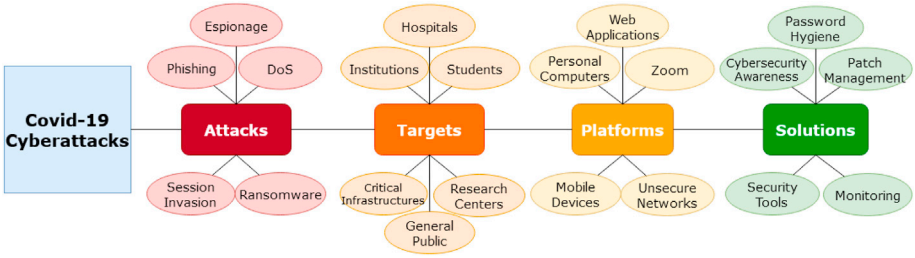


Fig. 1. An overview of the topics related to the cyberattacks during the COVID-19 pandemic.

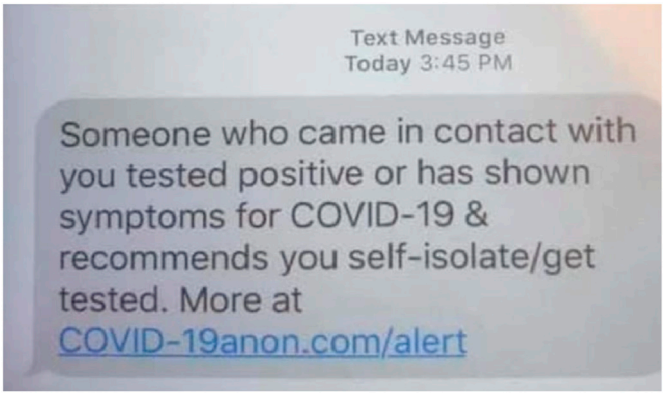
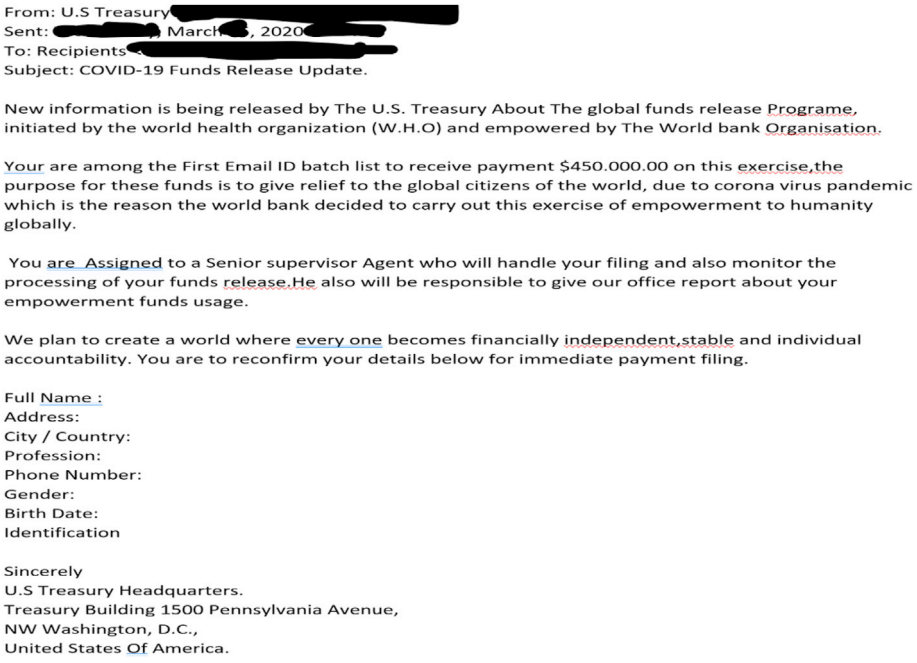


Fig. 2. An example of a fake COVID-19 text message.

unauthorized access or attacks. Due to the continuous evolution of both defenses and attacks, cybersecurity has become one of the most challenging research areas [8]. During the COVID-19 pandemic, researchers and organizations have been attempting to develop various treatments and vaccines for the virus. The scale of this pandemic has made medical research a worldwide effort. In addition to medical research, research in the field of cybersecurity is also increasing to determine if current frameworks are sufficient to protect medical researchers from digital harm and minimize the risks associated with changing work environments [8]. A resource guide for cybersecurity during the COVID-19 pandemic is provided by Ref. [10], which details quick tips to help organizations protect themselves from pandemic-related cyberattacks.

Mouton et al. [11] investigated the cybersecurity threat during the COVID-19 epidemic and discussed the impact of the virus on the world, as well as how to minimize it. Furthermore, the importance of cybersecurity education and the need for people to be vigilant was emphasized. Brian Vail [12] explained the sharp increase in reliance on digital communication methods, the risk of cyberattack, and the need to pay attention to security issues and precautions. The authors in Ref. [13] discussed the COVID-19 cyberwar and how businesses can protect themselves. They identified the main steps that security leaders need to follow to deal with different and influential events that might happen and how to manage such incidents. The authors in Ref. [14] described how COVID-19 changed lives all around the world and affected cybersecurity. The authors also discussed the pandemic and the joint efforts of organizations to reconsider cyber risk management strategies.

Chamola et al. [15] explored the alleviating impact of new technologies, such as Internet-of-Things (IoT), Unmanned Aerial Vehicles (UAV), blockchains, Artificial Intelligence (AI), and 5G, on the COVID-19 outbreak. The survey provides an overall view of the pandemic with regards to its clinical features, identification, treatment and prevention tactics, and any technological solutions being adopted. Mahadevan et al. [14] provided a series of insights on the increase in cybercrimes during the COVID-19 outbreak and described events, such as the ransomware attack on the University Hospital Brno in the Czech Republic. The authors


From: U.S Treasury
Sent: [redacted] March [redacted], 2020
To: Recipients
Subject: COVID-19 Funds Release Update.

New information is being released by The U.S. Treasury About The global funds release Programe, initiated by the world health organization (W.H.O) and empowered by The World bank Organisation.

Your are among the First Email ID batch list to receive payment $450.000.00 on this exercise,the purpose for these funds is to give relief to the global citizens of the world, due to corona virus pandemic which is the reason the world bank decided to carry out this exercise of empowerment to humanity globally.

You are Assigned to a Senior supervisor Agent who will handle your filing and also monitor the processing of your funds release.He also will be responsible to give our office report about your empowerment funds usage.

We plan to create a world where every one becomes financially independent,stable and individual accountability. You are to reconfirm your details below for immediate payment filing.

Full Name :
Address:
City / Country:
Profession:
Phone Number:
Gender:
Birth Date:
Identification

Sincerely
U.S Treasury Headquarters.
Treasury Building 1500 Pennsylvania Avenue,
NW Washington, D.C.,
United States Of America.

Fig. 3. An example of a fake stimulus cheque email.

Table 1
Existing COVID-19 related studies.

Work	Security Objectives		Platform		Sector				
	Privacy	Security	Android	OS	Health	Education	Critical Infrastructure	Individual	Public
[10]		✓		✓				✓	✓
[11]		✓		✓		✓		✓	
[12]		✓		✓				✓	✓
[13]		✓		✓				✓	✓
[14]		✓		✓					✓
[15]		✓		✓		✓	✓	✓	✓
[14]		✓		✓	✓			✓	✓
[16]		✓		✓				✓	✓
[17]		✓		✓	✓			✓	
[18]		✓		✓			✓	✓	
[19]		✓		✓				✓	✓
[20]		✓		✓				✓	✓
This article	✓	✓	✓	✓	✓	✓	✓	✓	✓

of [14] highlighted the extent to which hackers paid attention to medical services during the pandemic and discussed various attacks, such as espionage and phishing, aimed at benefiting from the fear and confusion of people around the world. The authors emphasized the need to protect critical resources from perilous cyberattacks through urgent measures.

The presence of the COVID-19 pandemic and the large-scale changes being implemented by organizations for the remote work environment have led to an increase in cybersecurity risks. Bradley J [16]. discussed a few examples of cyberthreats that occurred during the pandemic. The author further provided guidance for handling risks, emphasizing three basic pillars: personnel, process, and technology. Based on [16], an adequate cyber risk insurance strategy is recommended to all organizations.

During the COVID-19 outbreak, doctors have been taking care of patients using personal devices. However, this exposes Electronic Health Records (EHRs) to hackers. Hence, the new remote work orders affect not only ordinary residents and office workers, but also critical medical workers as well. The authors of [17] have provided a series of measures taken by the American Medical and Hospital Associations (AMA and AHA) to ensure protection from cybercrimes. A checklist for cyber-hygiene has been provided for healthcare providers and patients to work and receive healthcare remotely. The checklist also includes techniques and tips for strengthening the personal devices and home networks of both healthcare providers and recipients.

Everyone, including critical sector employees, works remotely during the pandemic, so following the appropriate cybersecurity measures must be taken at home has. The authors of [18] have emphasized the possibility of telecommunications services exploited and the consequences of remote work on the overall infrastructure, data quality and integrity, and security. The report points out that federal agencies usually follow the risk management procedures of the Federal Information Security Modernization Act (FISMA). Cyberattackers have been exploiting the uncertainty, fear, and confusion of users during the pandemic to mislead users with fraudulent websites and emails in an attempt to phish them. It is imperative that the appropriate cybersecurity and risk management measures are employed to protect users from such attacks.

PricewaterhouseCoopers (PwC) [19] also discussed the impact of COVID-19 on cybersecurity, focusing on how to manage and mitigate cyber risks. The teams described three important steps that organizations must take to mitigate emerging risks:

1. Protect remote working environments
2. Ensure the durability of essential security functions
3. Protect systems from potential threats seeking to take advantage of the situation

The authors of [20] explained the existence of a "cybersecurity response package," which includes quick response techniques, the tools used, and services from the European CyberSecurity Organization (ECSO). Due to a positive response to this package, it will be regularly updated as part of the Cyber Solidarity Campaign. The package includes resources for healthcare, the general public and employees that are working from home. These resources can be used to ensure an effective and secure working environment, mitigate cyber risks by following effective guidelines, security assessments, and expert advice for immediate support. Another direction is about the security and privacy of the COVID-19 Apps contact tracking app analysis [21].

3. COVID-19 cyber-pandemic targets

3.1. Health sector

Hospitals have seen a significant increase in the number of cyberattacks detected by their servers [22–26]. These attacks come in different forms, such as espionage attempts, Denial-of-Service (DoS) attacks and ransomware attacks. Any cyberattack that disrupts hospital services can have serious consequences, such as delaying emergency care, cutting off supplies and services, or causing the death of patients. For example, the Brno Hospital in the Czech Republic faced a cyberattack that forced all healthcare staff to shut down their computers and stop IT services [27]. As a result, all surgeries were postponed and patients needed to be transferred to other hospitals. It was noted that the hospital also did COVID-19 testing, but there was no information on whether that section was affected by the cyberattack. On September 17, 2020, a ransomware attack occurred in the University Hospital Dusseldorf in Germany [28, 29]. Similar to the Brno Hospital attack, staff was forced to cancel all surgical procedures while authorities negotiated with the attackers for the decryption key. Although they were successful in retrieving the key, one patient that had been in critical condition passed away while he was transported to another hospital for treatment.

Hospitals are not the only target of cyberattacks. The entire health sector is at risk of being attacked. The Champaign-Urbana Public Health District suffered a ransomware attack, labeled NetWalker, on its website [30]. The district discovered the attack when employees realized that they could not access any files on the system. Although patients were not affected, district employees used their systems and network to exchange information regarding the Coronavirus outbreak. While the attack was being investigated, the health district turned to Facebook to share information among themselves and with the public. However, this solution has its own risks, since anyone can falsify their identity on social media and attempt to breach the organization [30].

The United States Health and Human Services' (HHS) servers were also the target of a cyberattack [31]. The attackers did not manage to breach the network, but they did attempt to disrupt services by trying to overload servers with hits. After the attack failed, the HHS and the federal government began to investigate the attack and suspected that it

originated from a foreign country.

During the pandemic, the WHO has been the focus of attention as they attempt to keep everyone informed, encourage research, and maintain the population. However, in doing so, they have also attracted the attention of malicious hackers and been the target of numerous attacks. In one attack, the hackers created a fake website and pretended to be WHO's internal email system in an attempt to steal employees' passwords [32–34]. Fortunately, Alexander Urbelis, a cybersecurity expert at Blackstone Law Group, noticed the attack in advance since he was already monitoring the hackers suspected of participating in the attack. Unfortunately, Urbelis also mentioned that he and his colleagues had detected similar attacks against ordinary people; hackers have been building fake websites related to the pandemic to lure innocent users and employees to share personal information.

3.2. Education sector

In addition to the health sector, the education sector has also been the target of cyberattacks. During the pandemic, office employees were not the only people that have been ordered to work from home. Primary and secondary schools and university campuses around the world have closed their doors to encourage e-learning. Students and faculty hold classes online through digital multi-party communication platforms such as Zoom or BlackBoard Collaborate. However, rushing to use these systems for classes has its own cyber risks.

Due to the sudden launch of online learning platforms, warnings have been issued regarding the safety risks of increased online activities for students [35–38]. These warnings were prepared with the knowledge of how dangerous cyberattacks on academic institutions have occurred in the past. For instance, a series of attacks occurred in 2017. Cyber-attackers hacked into multiple school district servers across the United States and stole the personal information of faculty, staff and students. The attackers then contacted and abused these students and released their information publicly, which could attract more dangerous entities, such as child predators or other hackers [35]. With the inclusion of a home environment, however, there are multiple factors that affect e-learning safety [36–38]:

1. Using public or home networks to access online learning platforms may not be as secure as a school network. If a student or teacher has an insecure connection, they may put the rest of the class or their families at risk.
2. Exposing young children, who lack computer literacy and knowledge, to the Internet puts them at risk of “over-exploring.”
3. Some web applications used by instructors may not be secure and can may cause the risk of digital hijacking in class.

K-12 schools are not the only institutions attacked by hackers. Universities, especially those involved in COVID-19 research, have also become targets of malicious parties. Several universities in the United States and United Kingdom (UK) have the facilities for Coronavirus and vaccine research. In early May, the National Cyber Security Center (NCSC) in the UK reported several cyber attack attempts against these institutions in an attempt to steal COVID-19 information or disrupt services [26,39–42]. The attacks are suspected to have come from both malicious parties and foreign nations. It is alarming that such attacks were attempted, especially when some research facilities announced that they would start human trials of a possible Coronavirus vaccine [40,42]. The attacks that were attempted were password thefts, ransomware, and espionage.

3.3. Critical infrastructures

The COVID-19 pandemic has forced many organizations to drastically change their business models. The current business model of many organizations has shifted to “working remotely” or “working from home.” This new business model may reduce the number of employees working on site. As a result, cybercriminals may be induced to use any vulnerabilities to carry out cyber attacks with a view to reducing the number of employees and the supervision of the critical infrastructure systems.

Over the past two years, the majority of the attacks against critical infrastructures were the results of system misconfiguration, unauthorized access, reconnaissance, malicious code and phishing. Table 2 depicts some major attacks that have been carried out against critical infrastructures prior to the COVID-19 pandemic. However, given the current circumstances and the drastic change in the business model of many organizations responsible for national critical infrastructures, it is suspected that these attacks may continue.

These systems need to continuously supervise intrusion detection and establish countermeasures related to network security. In order to effectively implement the new business model, utilizing commercial software systems may cause vulnerability risks due to lack of adequate, regular testing. This provides an opportunity for cybercriminals to take advantage of these systems and damage the infrastructures.

3.4. General public

Major organizations around the world have been warning everyone about the increase in the number and frequency of cyberattacks. Dedicated cybercriminals will get what they want by any means. Now that most people are at home and online all day to communicate with loved ones, friends, classmates, and coworkers, they have become easy targets for hackers to wreak havoc.

Major authoritative figures [43,44] have issued many warnings to the public about cybercriminals aiming to take advantage of people in these difficult times. These warnings highlight that criminals are setting up fake Web domains to disguise themselves as the WHO. According to WHO, more than 4000 Coronavirus-related domains have been registered since the beginning of the year, 5% of which are viewed as suspicious and 3% of which are new domains that are considered malicious [45]. The fake websites advertise that they contain information regarding the COVID-19 outbreak and encourage readers to provide personal information to “subscribe for more information” [43,44,46,47]. These scams can be found in the following forms:

- **COVID 19 scam flyers:** COVID-19 provided cybercriminals with the opportunity to take advantage of individuals by creating and circulating flyers that advertise false services, such as charities, online shopping platforms, romantic relationships, and social media applications. They may also impersonate legitimate organizations, such as WHO, CDC, and Interpol, in an attempt to phish personal information from readers.
- **Scam text messages:** Cybercriminals may send text messages that provide false or enticing information followed by a hyperlink to a website or application download. These text messages are a gateway to intrude into an oblivious user's personal devices. Fig. 2 depicts an example of a scam text message sent to a victim in order to lure them to a fake website.
- **Fake stimulus cheque emails:** Many governmental agencies around the world have warned individuals of a new ongoing phishing attack that uses fake government-awarded stimulus cheques or payments as bait to steal personal information. Cybercriminals are using a variety of methods to contact potential victims. Fig. 3 depicts one example of a fake stimulus cheque email.
- **Fake government agency emails:** Cybercriminals are circulating various phishing e-mails or text messages to trick individuals to provide personal information by impersonating government and authoritative bodies.
- **Fake COVID-19 maps:** Fake maps depicting infection, death and recovery rates have been created by cybercriminals in an attempt to lure users into viewing or clicking on them. These maps contain

Table 2
Summary of cybersecurity attacks targeting critical infrastructure.

Threat Actor	Targeted Countries	Affected Infrastructure	Motivation	Malicious Tools
MuddyWater	UAE, Saudi Arabia, Oman, Lebanon, Pakistan, India, Iraq, Georgia, Turkey, Tajikistan, Israel, USA	Oil and Gas Industry and ICT	Cyberespoinage	Powerstates
Static Kitten	UAE, Saudi Arabia, Oman, Lebanon, Pakistan, India, Iraq, Georgia, Turkey, Tajikistan, Israel, USA	Oil and Gas Industry and ICT	Cyberespoinage	Power states
Molerates	UAE, Saudi Arabia, Egypt, Jordan, Libya, Iran, Iraq, Israel, USA, UK	Oil and Gas, Government Diplomat and Media	Cyberespionage	Xtreme RAT, njRAT
Gaza Cybergang	UAE, Saudi Arabia, Egypt, Jordan, Libya, Iran, Iraq, Israel, USA, UK	Oil and Gas, Government Diplomat and Media	Cyberespionage	Xtreme RAT, njRAT
Gaza Hackers Team	UAE, Saudi Arabia, Egypt, Jordan, Libya, Iran, Iraq, Israel, USA, UK	Oil and Gas, Government Diplomat and Media	Cyberespionage	Xtreme RAT, njRAT
Moonlight	UAE, Saudi Arabia, Egypt, Jordan, Libya, Iran, Iraq, Israel, USA, UK	Oil and Gas, Government Diplomat and Media	Cyberespionage	Xtreme RAT, njRAT
Extreme Jackal	UAE, Saudi Arabia, Egypt, Jordan, Libya, Iran, Iraq, Israel, USA, UK	Oil and Gas, Government Diplomat and Media	Cyberespionage	Xtreme RAT, njRAT
DarkHydrus	UAE, Saudi Arabia, and Turkey	Transportation (Aviation), Government and Education	Cyberespionage	RogueRobin, Phishery
LazyMeerkat	UAE, Saudi Arabia, and Turkey	Transportation (Aviation), Government and Education	Cyberespionage	RogueRobin, Phishery
RogueRobin	UAE, Saudi Arabia, and Turkey	Transportation (Aviation), Government and Education	Cyberespionage	RogueRobin, Phishery
Shamoon 3	UAE, Saudi Arabia, India, Scotland, and Italy	Oil and Gas, Transportation, Government	Sabotage	Disttrack, Filerase
OilRig	UAE, Saudi Arabia, Qatar, Kuwait, Turkey, Lebanon, Israel, USA	Transportation (Aviation), Financial, Government, Energy, Chemical, Telecommunications	Cyberespionage	Bondupdater
APT34	UAE, Saudi Arabia, Qatar, Kuwait, Turkey, Lebanon, Israel, USA	Transportation (Aviation), Financial, Government, Energy, Chemical, Telecommunications	Cyberespionage	Bondupdater
Helix Kitten	UAE, Saudi Arabia, Qatar, Kuwait, Turkey, Lebanon, Israel, USA	Transporation (Aviation), Financial, Government, Energy, Chemical, Telecommunications	Cyberespionage	Bondupdater
Helminth	UAE, Saudi Arabia, Qatar, Kuwait, Turkey, Lebanon, Israel, USA	Transporation (Aviation), Financial, Government, Energy, Chemical, Telecommunications	Cyberespionage	Bondupdater
Clayslide	UAE, Saudi Arabia, Qatar, Kuwait, Turkey, Lebanon, Israel, USA	Transporation (Aviation), Financial, Government, Energy, Chemical, Telecommunications	Cyberespionage	Bondupdater
IRN2	UAE, Saudi Arabia, Qatar, Kuwait, Turkey, Lebanon, Israel, USA	Transportation (Aviation), Financial, Government, Energy, Chemical, Telecommunications	Cyberespionage	Bondupdater
DNSpionage	UAE, Saudi Arabia, Qatar, Kuwait, Lebanon, Turkey, Israel, Iran, USA	Transportation (Aviation), Financial (Banks), Government, Energy, Telecommunication	Cyberespionage	DNSpionage
ColdRiver	UAE, Saudi Arabia, Qatar, Kuwait, Lebanon, Turkey, Israel, Iran, USA	Transportation (Aviation), Financial (Banks), Government, Energy, Telecommunication	Cyberespionage	DNSpionage

malicious malware to infect the victim's device once the user interacts with it.

- **Scam supply offers:** With governments around the world calling for curfews and quarantines, many consumer-based businesses have started using online platforms to allow people to safely shop and avoid physical contact. The increased demands of hygienic supplies, medications, and food have provided cybercriminals with an opportunity to take advantage of shoppers. Offers can be fabricated to entice shoppers to click on or respond to fake advertisements and provide personal information.

3.5. COVID-19 cyber-pandemic attack methods

Ever since worldwide attention began to turn to the Coronavirus, various cyberattacks have occurred. Cybercriminals sought to take advantage of people's panic all around the world for various reasons, such as data or identity theft, harassment, or denial of services. A spike in types of attacks occurred over the first three months of 2020, which can be observed in Table 3.

3.6. Personal data theft

Cybercriminals tend to use social engineering strategies combined with email messages to attempt to gather personal data from individuals. These messages attract users by disseminating COVID-19 information or alerting them with messages. They typically contain links that will open a form for the user to complete. Malicious websites include links to other online facilities. The damaged webpages include keywords related to the Coronavirus to attract potential victims. For example, the URL may include phrases such as "COVID-info-status," "increase_covid_fundrelease," or "2019_cov_gov_status". These corrupted websites are designed to imitate authentic ones. However, careful users can differentiate between legitimate and false websites by inspecting the webpage URL.

Some users have found that they were being specifically targeted, receiving personalized messages that led to webpages that they might open. However, careless users can access these links and drop personal information or credentials, which cybercriminals can use for their own purposes. An example of this can be seen in Fig. 4.

In other cases, messages containing malicious attachments encourage

Table 3
COVID-19-related threats in Q1 2020.

	Spam messages			Malware			Malicious URL			Contact tracing Apps		
	Jan	Feb	Mar	Jan	Feb	Mar	Jan	Feb	Mar	Jan	Feb	Mar
United State	80,900	180,000	355,000	150	230	300	10,000	18,000	33,000	800	1200	4000
Europe	77,000	169,000	240,000	79	123	265	6500	13,700	27,500	900	1500	6900
Asia	82,500	190,200	275,000	50	105	245	8000	14,000	30,000	1050	2900	9000
Africa	60,500	130,000	205,000	44	98	169	7000	12,000	21,500	650	1000	2750

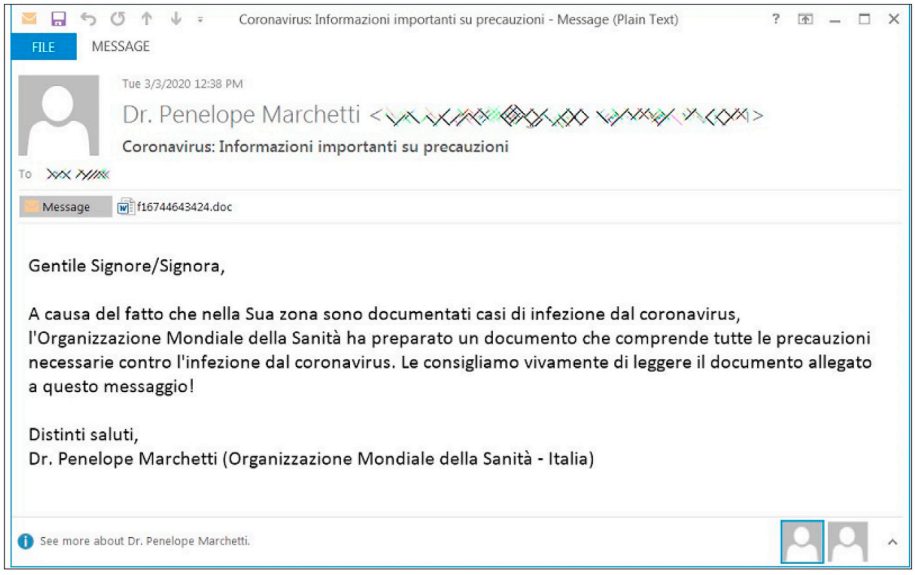


Fig. 4. Email containing malicious macro targeting Italian users.

users to open them, and once the message is read, the malicious software is executed. This software will grant hackers access to the victim's device.

3.7. Malware

While the Coronavirus is spreading fear worldwide, cybercriminals are taking advantage of this to spread malware and virtually wreak havoc. Fear and paranoia have become a hacker's enabler; people will do anything to learn about how they can prepare for the pandemic and protect themselves and loved ones from COVID-19. As previously explained in this work, hackers have been using fake, malicious domains and spam messages to attempt to steal personal information from users. If they fail to do this the first time, these messages and websites may contain malware that downloads onto the target's device. Analysts have identified a variety of malware that hackers use to infect devices. Most of these malware are Trojans, Ransomware, and Backdoors.

Trojans are a type of malware that appear legitimate or innocent to users, but are actually inconspicuously running malicious background processes on the infected device. Trojans appear when a user has downloaded an application or email attachment. During the COVID-19 pandemic, propagation for Trojans appears in the form of documents containing information regarding the virus outbreak or applications that offer services, such as face mask supply [47–50]. Trojans may also be remotely downloaded by hijacking router DNS [51].

Some well-known Trojans detected are Hawkeye, Oski, Lokibot, and Redline Stealer. These Trojans are used for purposes such as stealing device information, recording keystrokes, and stealing personal information and credentials [47–49,52]. Some of these Trojans, such as Hawkeye and Lokibot, take advantage of the CVE-2017-11882 exploit, which abuses the equation editor in Microsoft Office tools. Redline Stealer was found in a fake, trojanized version of the Folding@Home application, where users can sacrifice their computational resources to help researchers analyze the Coronavirus. Other notable Trojans that have appeared are the Cerberus, Anubis, and Danabot banking Trojans [47,48]. These are Trojans that take the form of banking or payment systems to bait users into providing their private credentials.

Ransomware has increased worldwide since the pandemic began. SDXCentral, for example, has reported a 148% increase in ransomware attacks in March [53]. BitDefender has also commented on the increase in ransomware attacks, mentioning that hospitals appear to be the prime target for this type of malware [54]. They shared the number of ransomware attempts that were blocked in hospitals, which is illustrated in Fig. 5.

A particularly popular type of ransomware targeting hospitals is Ryuk

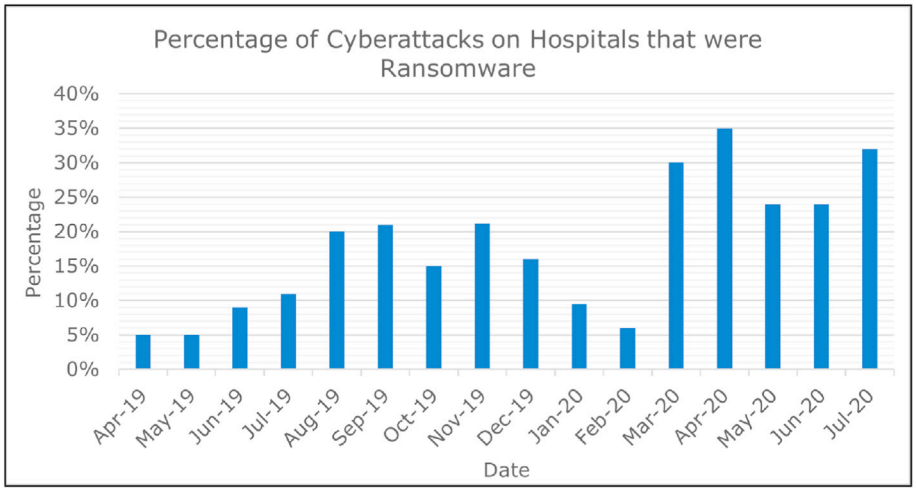


Fig. 5. The percentage of cyberattacks attempted that were ransomware blocked by hospitals.

[55]. Other detected ransomware include NetWalker, HiddenTear, Corona Winlocker, CoronaVirus, and Ransomware-GVZ [47–49]. Some of these malware work by deleting any shadow files detected on the machine and encrypting the remaining files. Once the files have been encrypted, their file formats are changed to an unrecognizable form. Payment will then be demanded to decrypt the files. Another feature that some ransomware have is the ability to write itself into the device's Master Boot Record (MBR). Once the user restarts their device, they will instead boot into the ransomware lock screen, which would then demand direct payment or communication with another party, as seen in Fig. 6.

The final type of malware that analysts have detected during the time of the pandemic are Backdoors. This malware can provide attackers with remote access to the infected machine. Backdoors can be dangerous due to the attacker's ability to steal information, sniff networks, or use the infected device to pull off more attacks. Some of the Backdoors that have been detected recently are Remcos, AgentTesla, BlackNET, NetSupport and Nanocore [47–49].

A summary of the malware that was used for COVID-19-related cyberattacks can be seen in Table 4.

3.8. Possible cyberwarfare

While the world has its attention turned towards resolving the COVID-19 outbreak and treating those that have been infected, some nations have decided that this is the opportune moment to perform cyberattacks against another. On top of performing cyberattacks that may cause damage, nations have reportedly been attempting cyber-espionage during the pandemic. In addition to the Coronavirus data theft attempts mentioned in 3.2, Gilead Sciences in the US has reported a cyberattack that attempted to steal research. Gilead Sciences is one of the drug-manufacturing firms in the race to develop a vaccine for the virus [56, 57]. Reports stated that there were multiple attempts to compromise Gilead's staff.

4. Cyber-pandemic platforms

4.1. Zoom

Ever since outbreak of the epidemic, the number of cyber attacks around the world has been increasing. Now that everyone is encouraged to stay at home to avoid contracting and spreading the virus, hackers are taking advantage of the increased use of mobile phones, tablets, personal computers and the Internet. As the government orders their residents to work and study from home, there has been an increased use of online platforms such as Microsoft Teams, Zoom, and Discord. Zoom creator Eric Yuan has reported a surge in users; initially serving 10 million users worldwide, as of March 2020, approximately 200 million users have been using the app [58–61].

Although companies typically strive to get so much attention, the surge in Zoom usage has exposed its security vulnerabilities. Malicious users have begun partaking in “Zoombombing,” where they join a random Zoom call and begin posting malicious content [58–62]. This brought to light other security and privacy flaws with the application. In addition to calling hosts to post their lobby links, malicious users can also hijack calls through illegal means. Yuan has admitted that the application shares data with third parties, raising concerns about the level of privacy the application really has. This has encouraged his teams to halt feature development and focus purely on security and privacy enhancements for the application.

Fig. 6. An example of ransomware that has written itself into the MBR and left a Discord server link for communication.

Table 4
A summary of the malware detected during the COVID-19 pandemic.

Name	Type	Purpose
Lokibot	Trojan	Infostealer
Hawkeye	Trojan	Keylogger
Oski	Trojan	Infostealer
Redline Stealer	Trojan	Infostealer
Cerberus	Trojan	Banking
Anubis	Trojan	Banking
Danabot	Trojan	Banking
Clipbanker	Trojan	Banking
Ursnif	Trojan	Banking
SMSTrojan	Trojan	Mobile SMS Spam
Azorult	Trojan	Infostealer
KPot	Trojan	Infostealer
CovidLock	Ransomware	Mobile Ransom
Corona Winlocker	Ransomware	Ransom
NetWalker	Ransomware	Ransome
HiddenTear	Ransomware	Ransom
Ryuk	Ransomeware	Ransom
Remcos	Backdoor	Remote Access Trojan
BlackNET	Backdoor	Remote Access Trojan
Tesla	Backdoor	Spyware
Nanocore	Backdoor	Infostealer
NetSupport	Backdoor	Remote Access Trojan

4.2. Contact tracing apps

In an effort to help contain COVID-19 and track how its spread, countries all around the world have introduced the concept of “Contact Tracing.” Through Contact Tracing, people install an application on their mobile smartphones that uses their Bluetooth and GPS to help detect who was around them just before they tested positive for the Coronavirus [63–66]. However, the urgency to release this application and have residents download it, concerns over the level of privacy the app provides have risen.

The first concern is the reliance of some versions of the application on GPS locations. Although the applications are useful and help maintain the virus to prevent it from further spread and recording possible locations with high infection rates, malicious actors can interfere with the app's signals [65]. The second concern is the application of Bluetooth, which has its own vulnerabilities [63,64,66]. These two features may attract hackers due to the large databases containing the identities and locations of those who decide to install the application. The UK's Contact Tracing application had even failed cybersecurity tests, making users vulnerable to attack [64]. Some of these applications have been found to provide backdoors for users' mobile devices, allowing developers and associated parties to collect more information about the user than they claim [63, 66].

An early concept of the application even proposed timing how long individuals stayed out of their home and informed them if they stood too close to others using the same application [66,67]. This had its own security concerns, which clearly go against what are considered ethical practices while developing and receiving an application. Experts in the field have denounced these features, claiming that government-backed applications used to keep track of user locations to this extent “risks the most insidious mission creep” [67]. Tracking such features will also likely reduce the amount of trust the people have in their government and they will be more inclined to go behind their backs by keeping their mobile devices at home, for example.

4.3. Folding@Home abuse

When the Coronavirus pandemic began to rise, researchers began to encourage an activity called "Folding@Home." This project, is "dedicated to understanding protein folding, and the diseases that result from protein misfolding and aggregation, and novel computational ways to develop new drugs in general" [68]. The project uses distributed computing to run numerous calculations to understand and simulate protein folding, which can be used for studies and treatment. Users that are willing to participate in Folding@Home can visit the main website to download the application, which utilizes spare CPU and GPU resources. This project is greatly supported by major organizations, such as NVidia, AMD, Microsoft, Oracle, and Intel.

Once the calls for participation in COVID-19 Folding@Home came out, cybercriminals saw this as an opportunity to take advantage of users' volunteering their processors. Amid the Folding@Home announcements and excitement, hackers created false Folding@Home applications and phishing emails, hoping users would download the malicious app. Once downloaded and installed, the fake application would begin running RedLine, which is an information-stealing malware. It collects passwords to any account found on the infected device, and newer versions of the malware have the ability to even steal crypto-currency wallets [69,70]. Representatives of the official, legitimate Folding@Home project, as well as WHO, Interpol, and HHS, have since published warnings against these phishing attempts and urged users to visit the official Folding@Home webpage to learn more about the project and download the official application.

4.4. Web applications

In the early stages of the pandemic, organizations such as Google, WHO, and Johns Hopkins created online maps containing infection and death rates, statistics, and visual spread demonstrations for people to follow. However, cyberattackers saw this as an opportunity to take advantage of the tension that people all around the world were feeling and created their own maps to send out for spreading malware or tracking users [71–75]. These maps were made to look realistic, with some being designed to look like maps from legitimate organizations. One example of the latter case was a map created to look like and claim to have been created by Johns Hopkins, depicted in Fig. 7.

Although this map looks almost exactly like the Coronavirus tracking map created by Johns Hopkins, it was also loaded with the AZORult trojan, which is used for stealing sensitive information [71,74,75]. The link to this map was circulated on the web or sent through phishing emails by cybercriminals to promote the website, installing the trojan on anyone's device that visited the link. Warnings of such maps have since been issued by major organizations, such as the HHS, Interpol, and WHO, urging users to be cautious of any links they click on.

4.5. Personal devices

The COVID-19 pandemic has seen an increase in more than just computer- and critical infrastructure-related malware and cyberattacks. Smaller-scale personal devices, such as mobile phones, tablets, and IoT devices, have also been targeted by cybercriminals. This is due to the increase in remote work, monitoring, or study and the installation of contact tracing applications.

It is reported that in the first quarter of 2020, the total number of malware attacks against mobile devices increased by at least 12% [74,76]. McAfee reports that 71% of mobile malware is new [74]. Fig. 8 shows the increase in new mobile malware provided by McAfee.

In addition to the fake SMS and email messages as part of phishing attempts, attacks on mobile devices included attempts to convince users to download malicious applications. These applications may be found in

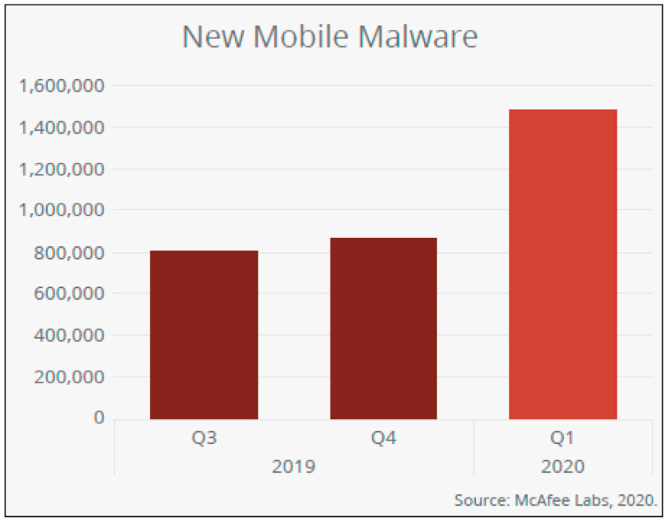


Fig. 8. The number of new mobile malware.

Fig. 7. The fake, malicious version of Johns Hopkin's COVID-19 tracking map.

the device's app store, or advertised as a downloadable application package from fake messages or websites. These applications are used to install malicious content on the user's mobile device, such as spyware, ransomware, or trojans. An example of such an application can be seen in Fig. 9 [74]. This application advertises that it allows the user to order face masks from a fake malicious domain (*coronasafetymask[dot]tk*) and requires several suspicious permissions to run, such as:

1. Full internet access: used to create network sockets on the device
2. Read contact data: to collect data about which contacts the user has on their device
3. Send SMS messages: abuses the contact list permission to send scam SMS messages to the contacts found

In addition to the increase in mobile device cyberattacks, the number of attacks on IoT devices has also increased. This category includes gaming devices, such as consoles, controllers, headsets, and virtual reality or sensory devices, smart household appliances, such as refrigerators or stove ovens, smart household devices, such as doorbells or security systems, and remote health monitoring devices. There was reportedly at least a 50% increase in cyberattacks on these devices [74,77]. Attackers target these devices due to the way they are manufactured; IoT devices do not have the same manufacturing and security standards as computers and mobile devices. If an IoT device has been compromised, it can be used as backdoors into a network, allowing cybercriminals to deploy other attacks or eavesdrop with little to no detection.

5. Solutions

Given the events of the past year, it is imperative to integrate state-of-the-art solutions into the lives of users worldwide. We want to encourage users, casual and professional alike, to consider these solutions to not only prevent cyberattacks, but to also be prepared in the event of an incident. The incidents discussed in this paper are summarized in Fig. 10. The potential solutions to these cyberattacks can be categorized as countermeasures to cyberthreats or privacy enhancements. These solutions will not only help users prevent and mitigate attacks, but will also inform them of the risks at hand and allow preemptive preparation for any incidents, both at home and in the workplace.

5.1. Countermeasures

According to Dark Matter's cybersecurity report [78] and the warnings published by WHO [43], Interpol [44,79], and Kaspersky [80], the following are general recommendations for countermeasures against cyberattacks based on the analysis of cybersecurity vulnerabilities of key infrastructures previously attacked. The recommendations are divided into two main groups:

Fig. 9. The name and APK link of a fake COVID-19-related app.

- Organizational
  - **Awareness training:** The human factor is known to be one of the weakest links in any system, and there is no exception in the context of this paper. Therefore, we emphasize the importance of designing security awareness programs for different audiences (e.g., age groups, culture, and backgrounds) in order to maximize the impact.
  - **Multi-factor authentication:** Theft and stolen access credentials are key targets for cyberthreats. Multi-factor authentication is necessary to assure reliable access to vital systems.
  - **Configuration management:** Misconfiguration may also occur during security change processes, especially when the organization's cybersecurity or operational technology team is shrunk or the budget is reduced. There are a number of possible solutions, including technical solutions (e.g., configuration management solutions) and industry best practices.
  - **Password hygiene:** Adopt industry best practices, such as those outlined in NIST Special Publication 800-63B (Digital Identity Guidelines – Authentication and Lifecycle Management Change).[5]
- Technical:
  - **Network and device:** Implement industry best practices, such as those published by government agencies (e.g., Australian Cyber-Security Centre). For example, the Australian CyberSecurity Centre has

> "developed prioritized mitigation strategies to help cybersecurity professionals in all organizations mitigate cybersecurity incidents caused by various cyberthreats. This guidance addresses targeted cyber intrusions (i.e., those executed by advanced persistent threats such as foreign intelligence services), ransomware and external adversaries with destructive intent, malicious insiders, 'business email compromise', and industrial control systems"[6]

In addition to organizations taking extra precautions and becoming more aware of cyber risks, law enforcement authorities must also be prepared to handle cyberattacks. Typically, law enforcement offices have departments that handle cybersecurity-related issues. However, due to the increased network activity occurring during quarantine, these departments may become short-handed, and traditional officers may need to step in to assist. As stated by WHO [43], Interpol [44], and Digitpol [46], hotlines have opened up for people to call or write tickets to report any scam attempts or cyberattacks. Given the increase in cyberattacks worldwide, these organizations need to be prepared and familiar with cybersecurity.

General users are also encouraged to implement cybersecurity defense and mitigation techniques in their homes. As mentioned earlier in this paper, users involved in remote work and study may be putting themselves at risk with the platforms and web applications being used. To prevent network compromise, malware attacks, phishing attempts, and service disruptions, users should utilize their router's built-in firewalls to control which traffic is allowed in or out of their home network. However, the users should be aware of which domains need to be blocked and which are safe to explore. With regards to the COVID-19 pandemic, organizations, such as Interpol and WHO, have issued warnings about false domains set up by cybercriminals to target the fear and confusion of people around the world.

Another way users can be protected from cyberattacks is to make sure that they have a strong, updated antivirus installed and running on their devices. Antiviruses will be able to detect suspicious or infected files passing through a device. During the pandemic, cyberattackers have been sending infected documents claiming to contain information regarding the Coronavirus. These documents tend to contain Trojans or

[5] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf.

[6] https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents.

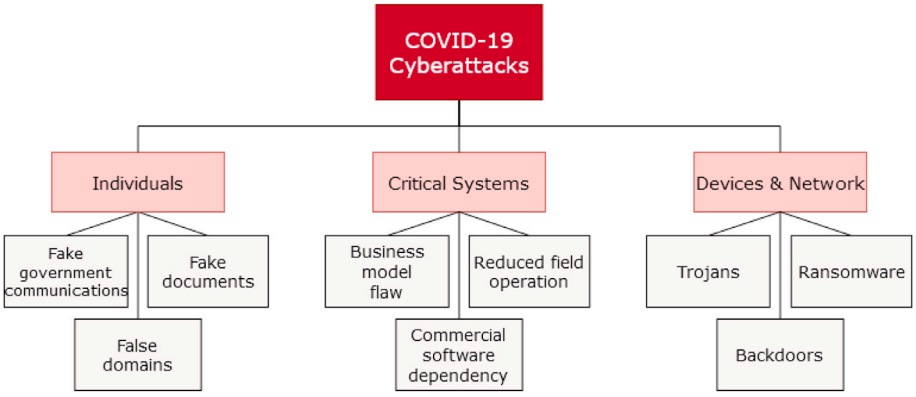


Fig. 10. A summary of the attacks and vulnerabilities that have occurred, as well as their respective targets.

Ransomware to easily exploit the oblivious user.

Children are also prone to these attacks, especially now that classes for school are being held online. Young children can be impressionable and curious, exploring all that they learn about and beyond. Additionally, teachers may use web applications to assist with their teaching methods, some of which may contain advertisements or be unsafe altogether. Cyberattackers may create web content that is flashy and enticing to children, leading them to click on malicious links or view visually harmful content. To prevent this, parents can install child protection software and adblockers. These tools will prevent specified content from appearing on the child's device or system profile.

The countermeasures used for each of the cyberthreats discussed in this paper are summarized in Table 5. It is important to note that in each of the cyberthreats that have been mentioned, awareness training is listed as one of the countermeasures. This is because once users, both professional and casual, become more informed of the cyberthreats that exist, the possibility and effectiveness of cyber incidents decreases. Becoming aware of potential attacks and how to mitigate and prevent them is an effective way to hinder the efforts of malicious parties. Whether it is during the COVID-19 pandemic or just in general, people all over the world that use information systems for studies, work, communication, and leisure must understand what is at stake and do their part to prevent becoming the target of attack.

Table 5
A summary of the malware detected during the COVID-19 pandemic.

Cyberthreat	Countermeasure	Additional Comments
Phishing	Awareness Training Multi-Factor Authentication	Phishing effects everyone, especially children and elderly users. The mentioned countermeasures can be integrated into the platforms being used, as opposed to placing it in the responsibility of the user
Malware	Awareness Training Antivirus Network Monitoring	–
Espionage	Awareness Training Encryption	Using a VPN for workplace communication can help with this
Malicious Domains	Awareness Training Network Monitoring Firewalls	–
Session Invasion	Awareness Training Password Hygiene Encryption	Ensuring that devices are shutdown during inactive hours prevents attackers from taking advantage of the inactivity for malicious purposes
Denial-of-Service	Awareness Training Network Monitoring Backups	–

5.2. Privacy

In a technologically advanced world like today's, data exists in many forms in multiple locations, especially with the amount of network connectivity available. With employees in all fields being ordered to work remotely, possibly sensitive data is being communicated through online platforms. However, as was mentioned throughout this paper, cyberattacks targeting everyone have been on the rise all around the world. Additionally, governments have ordered their people to install contact tracing applications on smartphone devices to keep track of locations and digital identities. With these events, the notion of digital data privacy becomes questionable, despite it being labeled as a human right.

Contact tracing applications use Bluetooth in order to determine who is in the vicinity of the device. However, Bluetooth technology has its own vulnerabilities that may expose device owners to attackers. Several recent attacks on Bluetooth include CVE-2020-0022, also known as 'BlueFrag [81,82], Bluetooth Impersonation Attacks (BIAS) [81,83,84], Bluejacking [81,82], Bluesnarfing [81,82], and Bluebugging [81,82]. With these attacks, hackers can compromise Bluetooth connections, force devices to share data with malicious devices, and steal data that is being broadcast to other Bluetooth-enabled devices. These attacks have affected devices running at least Android 8.0. However, approximately 40% of Android users are still using Android 6.0 or earlier versions that have stopped receiving security updates. Nevertheless, the government's reliance on Bluetooth technology for their advertised contact tracing apps may expose users to attack.

These contact tracing apps are also designed to remain running on the device continuously. This means that in order to successfully track users' locations, Bluetooth and other system services need to be enabled all the time. Cho et al. [85] discussed three notions of privacy:

1. Privacy from snoopers
2. Privacy from contacts
3. Privacy from authorities

Privacy violations are not always the result of malicious users attempting to steal data from users. Given the security permissions that these contact tracing applications require to function, there are concerns that they may be used as surveillance tools by governments and authorities [85,86]. However, authorities must be aware of data privacy regulations when advising people to install these applications.

In order to improve regulations on personal data collection and usage, the EU established the General Data Protection Regulation (GDPR) in 2016, and began to strictly enforce it with consequences for violators in 2018. The GDPR introduced the notion of 'consent,' which gives users the option to agree or disagree to informed data collection and processing decisions [87,88].

In the US, the HIPAA Privacy Rule regulates Personal Health Information (PHI) collection, processing, and disclosure. The COVID-19 pandemic, however, is an urgent matter that calls for special exceptions. To allow healthcare workers to participate in telemedicine, these

regulations have been relaxed [81,89].

6. Limitations, future research and recommendations

While conducting the research, some limitations are reported here. Firstly, cybersecurity and the COVID-19 outbreak are dynamic in nature; they can change on a day-to-day basis, they have the ability to rapidly evolve, and they are unpredictable to an extent. Although the material included in this paper is as recent as possible, the information shared may change after some time. This entails a close and sustained follow-up to new issues related to cybersecurity and COVID-19.

The cyberattacks that were covered in the previous Sections are very relevant to the time of this work. However, hackers are always actively attempting to compromise and take advantage of people and organizations, and their methods of doing so may evolve. This is how cybersecurity can be unpredictable; specialists can prepare for *known* cyberattacks and resolve *known* flaws and vulnerabilities, but they cannot foresee evolving versions of cyberattacks. In other words, cybersecurity specialists cannot foresee zero-day attacks, hence the name "zero-day."

The unpredictability of cybersecurity is also the result of the inability to predict a nation's next move. Earlier in this paper, several cyberattack attempts by Iran and other nations were mentioned. The plans to pull off these attacks are considered privileged knowledge, and only those involved in the attack know these plans. The most that people and organizations can do is to preemptively protect themselves from known behaviors and attacks. On the other hand, this is a sincere call to share knowledge and experiences globally to deal with cybersecurity threats and COVID-19.

Another limitation when studying the materials in this paper is the limited availability of information. To the best of our knowledge, most of the materials covered in this paper came from a variety of resources. Nevertheless, information regarding cyberattacks on organizations and critical infrastructures during this pandemic is very limited; there are articles about the attack occurring, but many of the details about the attack remain confidential. In addition to our previous recommendation of sharing experiences globally, there is a great push to research cybersecurity and COVID-19, and the coming weeks and months will witness a great growth in published material in this direction.

To reduce the number of cyberattacks during such difficult times and in the future, governments can inform their country's residents of cybersafety practices with the announcement of the home quarantine. Early awareness can let users understand the dangers of excessive Internet activity and how cybercriminals will attempt to harm their systems. Users should be encouraged not to share personal information immediately and to doubt the source of a message or email. Policy makers, educators and legislators should play a major role here in developing (and coaching) enforcing policies, procedures and guidelines to govern both cybersecurity and COVID-19 threats in order to surround the crisis and prevent chaotic situations.

Developers of web applications, such as Zoom or the interactive COVID-19 maps, should make sure that software development lifecycle steps are followed to reduce the number of flaws in the program code. The creator of Zoom, for example, has mentioned that the application was not designed for the large-scale usage, and therefore has security and privacy flaws [59–61]. Professionals all over the world should focus on developing innovative techniques, procedures and technologies to combat both cybersecurity and COVID-19 threats at different stages (i.e., before, during and after); preventive, tactical, reactive/treatment with more emphasis on preventive measures. For example, once the pandemic is over, a complete timeline of all attacks that occurred during the quarantine and major events around the world should be drawn. This way, cybercriminal interests and activity patterns can be inferred. Cybersecurity specialists can use the timeline to help prepare and improve attack prevention and mitigation methods during crises.

7. Conclusion

Cybersecurity has been a major issue during the COVID-19 pandemic. Standard users and organizations all over the globe have witnessed many cyberattacks since the start of the government-ordered quarantines. The increased digital device and network activity have attracted many hackers that seek to steal personal information or disrupt services. In addition to these, cybercriminals have also attempted to compromise hospitals and research centers for COVID-19 research. Cybersecurity awareness is very important and does not only affect professionals. Users of all ages need to be aware of the risks of the cyberworld and must be prepared to fend off hackers that attempt to infiltrate their networks and personal accounts. People need to avoid sharing personal information or opening suspicious webpages and applications.

This study attempts to include the latest literature to shed light on the dangers of cybersecurity in the ongoing COVID-19 pandemic, while raising important alarms. This is an emerging and a growing phenomenon and a global threat. This requires the cooperation and collaboration of different global stakeholders to control COVID-19 and hence, limit and stop the growth of cybersecurity threats. The research provided different recommendations and implications for both professionals and researchers, paving the way for more research in this crucial area.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] World Health Organization, Coronavirus disease 2019 (covid-19) situation report, URL, https://apps.who.int/iris/handle/10665/332388.
[2] C. Sohrabi, Z. Alsafi, N. O'Neill, M. Khan, A. Kerwan, A. Al-Jabir, C. Iosifidis, R. Agha, World health organization declares global emergency: a review of the 2019 novel coronavirus (covid-19), Int. J. 76 71–76.
[3] S. AlDaajeh, H. Saleous, S. Alrabaee, E. Barka, F. Breitinger, K.-K.R. Choo, The Role of National Cybersecurity Strategies on the Improvement of Cybersecurity Education, Computers & Security, 2022, 102754.
[4] S. Alrabaee, R. Manna, Boosting students and teachers cybersecurity awareness during covid-19 pandemic, in: 2021 IEEE Global Engineering Education Conference (EDUCON), IEEE, 2021, pp. 726–731.
[5] S. Alrabaee, M. Al-Kfairy, E. Barka, Efforts and suggestions for improving cybersecurity education, in: 2022 IEEE Global Engineering Education Conference (EDUCON), IEEE, 2022, pp. 1161–1168.
[6] M. Jakovljevic, S. Bjedov, N. Jaksic, I. Jakovljevic, Covid-19 pandemia and public and global mental health from the perspective of global health security, Psychiatr. Danub. 32 (1) (2020) 6–14.
[7] J. K. Wagner, Health, housing, and "direct threats" during a pandemic, J. Law Biosci..
[8] S. Hakak, W.Z. Khan, M. Imran, K.-K.R. Choo, M. Shoaib, Have you been a victim of covid-19-related cyber incidents? survey, taxonomy, and mitigation strategies, IEEE Access 8 (2020) 124134–124144.
[9] J. Hawdon, K. Parti, T.E. Dearden, Cybercrime in America amid covid-19: the initial results from a natural experiment, Am. J. Crim. Justice (2020) 1–17.
[10] Resource guide for cybersecurity during the COVID-19 pandemic. https://www.cisecurity.org/blog/resource-guide-for-cybersecurity-during-the-covid-19-pandemic/ (Accessed on March, 2020).
[11] M. Chakraborty, B. Jana, Impact of Covid-19 on Cyber Security Threat Landscape in New Reality, Available at SSRN 3668692.
[12] B. Vail, Canada: cybersecurity in the age of covid-19 (and beyond) (Accessed on March, 2020), http://www.mondaq.com/canada/security/946112/cybersecurity-in-the-age-of-covid820819-and-beyond.
[13] COVID-19 cyberwar: how to protect your business), Accessed on March, 2020), https://www.ibm.com/downloads/cas/Y5QGA7VZ.
[14] COVID-19's impact on cybersecurity). https://www2.deloitte.com/ng/en/pages/risk/articles/covid-19-impact-cybersecurity.html (Accessed on March, 2020).
[15] V. Chamola, V. Hassija, V. Gupta, M. Guizani, A comprehensive review of the covid-19 pandemic and the role of iot, drones, ai, blockchain, and 5g in managing its impact, IEEE Access 8 (2020) 90225–90265.
[16] B.J. Freedman, Cybersecurity and the COVID-19 pandemic (Accessed on March, 2020), https://cybersecuritylaw.ca/home/2020/4/28/cybersecurity-and-the-COVID-19-pandemic.
[17] Working from home during COVID-19 pandemic. https://www.ama-assn.org/system/files/2020-04/cybersecurity-work-from-home-covid-19.pdf (Accessed on March, 2020).

[18] C. Jaikaran, Federal Telework during the COVID-19 Pandemic: Cybersecurity Issues in Brief (Accessed on March, 2020).
[19] c. pwc, Managing the impact of COVID-19 on cyber security (Accessed on March, 2020), https://www.pwccn.com/en/issues/cybersecurity-and-privacy/covid-19-impact-mar2020.html.
[20] ECS, COVID-19 CYBERSECURITY RESPONSE PACKAGE an ECSO cyber solidarity campaign (Accessed on March, 2020), https://www.ecs-org.eu/documents/uploads/covid-19-package-last-update.pdf.
[21] H. Wen, Q. Zhao, Z. Lin, D. Xuan, N. Shroff, A study of the privacy of covid-19 contact tracing apps, in: International Conference on Security and Privacy in Communication Networks, 2020.
[22] D. Winder, Cyber attacks against hospitals have 'significantly increased' as hackers seek to maximize profits, Forbes[Online]. Available: https://www.forbes.com/sites/daveywinder/2020/04/08/cyber-attacks-against-hospitals-fighting-covid-19-confirmed-interpol-issues-purple-alert/#76bd11ba58bc.
[23] D. Winder, Hospitals on covid-19 frontline facing 'double extortion' cyber threat, Forbes[Online]. Available: https://www.forbes.com/sites/daveywinder/2020/04/16/hospitals-on-covid-19-frontline-face-double-extortion-threat-security-experts-caution/#2bed22973c27.
[24] A. Peters, I. Mehta, This is not the time to leave our hospitals unprotected against cyberattacks, The Washington Post[Online]. Available: https://www.washingtonpost.com/opinions/2020/03/19/this-is-not-time-leave-our-hospitals-unprotected-against-cyberattacks/.
[25] G. Ratnam, Cyberattacks on us health care raise alarms among senators, Bakersfield [Online]. Available: https://www.bakersfield.com/ap/national/cyberattacks-on-us-health-care-raise-alarms-among-senators/article_70906d1b-4b86-5d99-83f9-88a3e2701ba3.html.
[26] National Cyber Security Center, Cyber warning issued for key healthcare organisations in UK and USA [Online]. Available: https://www.ncsc.gov.uk/news/warning-issued-uk-usa-healthcare-organisations.
[27] C. Cimpanu, Czech hospital hit by cyberattack while in the midst of a covid-19 outbreak, ZDNet[Online]. Available: https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/.
[28] L. Matthews, Cyberattack on a hospital leads to the first ransomware-linked death, Forbes[Online]. Available: https://www.forbes.com/sites/leemathews/2020/09/17/ransomware-attack-hospital-leads-to-death/#44967baf3f05.
[29] M. Eddie, N. Perlroth, Cyber attack suspected in German woman's death, New York Times[Online]. Available: https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html.
[30] D. Pressey, C-u public health district's website held hostage by ransomware attack, The News-Gazette[Online]. Available: https://www.news-gazette.com/news/local/health-care/c-u-public-health-district-s-website-held-hostage-by/article_2dadedcd-aadb-5cb1-8740-8bd9e8800e27.html.
[31] S. Stein, J. Jacobs, Cyber-attack hits u.s. health agency amid covid-19 outbreak, Bloomberg[Online]. Available: https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response.
[32] D. Windey, 'elite hackers' thought behind cyber attack on world health organization, Forbes[Online]. Available: https://www.forbes.com/sites/daveywinder/2020/03/25/hackers-target-world-health-organization-as-cyber-attacks-double-during-covid-19-pandemic/#5d21ba512e5c.
[33] R. Satter, J. Stubbs, C. Bing, Exclusive: elite hackers target who as coronavirus cyberattacks spike, Reuters[Online]. Available: https://www.reuters.com/article/us-health-coronavirus-who-hack-exclusive/exclusive-elite-hackers-target-who-as-coronavirus-cyberattacks-spike-idUSKBN21A3BN.
[34] H. Samsel, World health organization facing cyber attacks during coronavirus response, Forbes[Online]. Available: https://securitytoday.com/articles/2020/03/26/world-health-organization-facing-cyber-attacks-during-coronavirus-response.aspx.
[35] FBI Internet Crime Complaint Center (IC3), Cyber actors take advantage of covid-19 pandemic to exploit increased use of virtual environments [Online]. Available: https://www.ic3.gov/media/2020/200401.aspx.
[36] R. Quinones, Remote learning: cybersecurity and compliance in the covid-19 age, District Administration[Online]. Available: https://districtadministration.com/remote-learning-cybersecurity-and-compliance-in-the-covid-19-age/.
[37] M. Catricala, Why education is more susceptible to cyber attacks during covid-19, Uzado[Online]. Available: https://www.uzado.com/blog/why-education-is-more-susceptible-to-cyber-attacks-during-covid-19.
[38] B. Barth, Rush to adopt online learning under covid-19 exposes schools to cyberattacks, SC Media[Online]. Available: https://www.scmagazine.com/home/security-news/news-archive/coronavirus/race-to-adopt-online-learning-under-covid-19-exposes-schools-to-cyberattacks/.
[39] G. Corera, Coronavirus: cyber-spies hunt covid-19 research, us and UK warn, BBC [Online]. Available: https://www.bbc.com/news/technology-52551023.
[40] C. Osborne, Hackers are targeting UK universities to steal coronavirus research, ncsc warns, ZDNet[Online]. Available: https://www.zdnet.com/article/hackers-are-targeting-uk-universities-to-steal-coronavirus-research-ncsc-warns/.
[41] J. Grierson, H. Devlin, Hostile states trying to steal coronavirus research, says UK agency, The Guardian[Online]. Available: https://www.theguardian.com/world/2020/may/03/hostile-states-trying-to-steal-coronavirus-research-says-uk-agency.
[42] P. Muncaster, State hackers target UK unis for covid19 vaccine research, Info Security Group[Online]. Available: https://www.infosecurity-magazine.com/news/state-hackers-uk-unis-covid19/.
[43] World Health Organization, Beware of criminals pretending to be who [Online]. Available: https://www.who.int/about/communications/cyber-security.
[44] Interpol, Covid-19 cyberthreats [Online]. Available: https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats.
[45] WHO, World health organization warns of coronvirus phishing attacks, BleepingComputerNews[Online]. Available: https://www.bleepingcomputer.com/news/security/world-health-organization-warns-of-coronavirus-phishing-attacks/.
[46] Digitpol, Covid-19 cyber attack investigation [Online]. Available: https://digitpol.com/covid-19-cyber-attack-investigation/.
[47] TrendMicro, Developing story, Covid-19 used in malicious campaigns, TrendMicro [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains.
[48] S. P, A. Karnik, L. Grindstaff, Covid-19 – malware makes hay during a pandemic, McAfee[Online]. Available: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/covid-19-malware-makes-hay-during-a-pandemic/.
[49] J. Walter, Threat intel — cyber attacks leveraging the covid-19/coronavirus pandemic, SentinelOne[Online]. Available: https://labs.sentinelone.com/threat-intel-update-cyber-attacks-leveraging-the-covid-19-coronavirus-pandemic/.
[50] S. Desai, New android app offers coronavirus safety mask but delivers sms trojan, zScaler[Online]. Available: https://www.zscaler.com/blogs/research/new-android-app-offers-coronavirus-safety-mask-delivers-sms-trojan.
[51] L. Abrams, Hackers hijack routers' dns to spread malicious covid-19 apps, Bleeping Computer[Online]. Available: https://www.bleepingcomputer.com/news/security/hackers-hijack-routers-dns-to-spread-malicious-covid-19-apps/.
[52] E. Brumaghin, H. Unterbrink, New hawkeye reborn variant emerges following ownership change, Cisco Talos[Online]. Available: https://blog.talosintelligence.com/2019/04/hawkeye-reborn.html.
[53] J. Lyons Hardcastle, Ransomware attacks spike 148SDXCentral[Online], Available: https://www.sdxcentral.com/articles/news/ransomware-attacks-spike-148-amid-covid-19-scams/2020/04/.
[54] L. Arsene, Global ransomware and cyberattacks on healthcare spike during pandemic, BitDefender[Online]. Available: https://labs.bitdefender.com/2020/05/global-ransomware-and-cyberattacks-on-healthcare-spike-during-pandemic/.
[55] I. Ilascu, Covid-19 testing center hit by cyberattack, Bleeping Computer[Online]. Available: https://www.bleepingcomputer.com/news/security/covid-19-testing-center-hit-by-cyberattack/.
[56] J. Stubbs, C. Bing, Exclusive: Iran-linked hackers recently targeted coronavirus drugmaker gilead - sources, Reuters[Online]. Available: https://www.reuters.com/article/us-healthcare-coronavirus-gilead-iran-ex/exclusive-iran-linked-hackers-recently-targeted-coronavirus-drugmaker-gilead-sources-idUSKBN22K2EV.
[57] Reuters, Coronavirus: Iran-linked hackers targeted drug maker gilead, The National [Online]. Available: https://www.thenational.ae/world/the-americas/coronavirus-iran-linked-hackers-targeted-drug-maker-gilead-1.1016790.
[58] Combating covid-19: video app zoom rockets to fame, with some hiccups, amid pandemic, Khaleej Times[Online]. Available: https://www.khaleejtimes.com/coronavirus-pandemic/combating-covid-19-video-app-zoom-rockets-to-fame-with-some-hiccups-amid-pandemic.
[59] S. Patnail, Zoom pulls in more than 200 million daily video users during worldwide lockdowns, Reuters[Online]. Available: https://www.reuters.com/article/us-health-coronavirus-zoom/zoom-pulls-in-more-than-200-million-daily-video-users-during-worldwide-lockdowns-idUSKBN21K1C7.
[60] J. Davis, Fbi: covid-19 spurs increase in zoom, video-conferencing hijacking, Health IT Security[Online]. Available: https://healthitsecurity.com/news/fbi-covid-19-spurs-increase-in-zoom-video-conferencing-hijacking.
[61] J. Novet, Intruders are hijacking zoom calls with noise and gross images — here's how to avoid becoming a victim of 'zoombombing', CNBC[Online]. Available: https://www.cnbc.com/2020/04/03/how-zoom-rose-to-the-top-during-the-coronavirus-pandemic.html.
[62] D. Evans, How zoom became so popular during social distancing, CNBC[Online]. Available: https://www.cnbc.com/2020/04/02/how-to-avoid-becoming-a-victim-of-a-zoombombing-on-zoom-video-calls.html.
[63] E. Yu, Contact tracing apps unsafe if bluetooth vulnerabilities not fixed, ZDNet [Online]. Available: https://www.zdnet.com/article/contact-tracing-apps-unsafe-if-bluetooth-vulnerabilities-not-fixed/.
[64] K. O'Flaherty, The u.k.'s covid-19 contact tracing app: everything you need to know, Forbes[Online]. Available: https://www.forbes.com/sites/kateoflahertyuk/2020/05/06/the-uks-covid-19-contact-tracing-app-everything-you-need-to-know/#320afa3bda4d.
[65] A. Greenberg, India's covid-19 contact tracing app could leak patient locations, Wired[Online]. Available: https://www.wired.com/story/india-covid-19-contract-tracing-app-patient-location-privacy/.
[66] Digitpol Cyber Security, Contact tracing smartphone apps raise privacy concerns, Digitpol[Online]. Available: https://digitpol.hk/contact-tracing-smartphone-apps-raise-privacy-concerns/.
[67] G. Volpicelli, The nhs coronavirus app could track how long you spend outside, Wired[Online]. Available: https://www.wired.co.uk/article/nhs-coronavirus-tracking-app.
[68] Folding@Home, Diseases[Online]. Available: https://foldingathome.org/diseases/.
[69] J. H, A. F, Proofpoint threat insight team, new redline password stealer malware, Proofpoint[Online]. Available: https://www.proofpoint.com/us/blog/threat-insight/new-redline-stealer-distributed-using-coronavirus-themed-email-campaign.
[70] L. Abrams, Redline info-stealing malware spread by folding@home phishing, Bleeping Computer[Online], Available: https://www.bleepingcomputer.com/news/security/redline-info-stealing-malware-spread-by-folding-home-phishing/.
[71] US HHS, Fake Online Coronavirus Map Delivers Well-Known Malware, Health Sector Cybersecurity Coordination Center.

[72] A. Holmes, Hackers are using these fake coronavirus maps to give people malware, Business Insider[Online]. Available: https://www.businessinsider.com/hackers-are-using-fake-coronavirus-maps-to-give-people-malware-2020-3.
[73] T. Brewster, Coronavirus scam alert: covid-19 map malware can spy on you through your android microphone and camera, Forbes[Online]. Available: https://www.forbes.com/sites/thomasbrewster/2020/03/18/coronavirus-scam-alert-covid-19-map-malware-can-spy-on-you-through-your-android-microphone-and-camera/?sh=62ecd04375fd.
[74] McAfee Labs, Mcafee Labs Covid-19 Threats Report.
[75] University of Virginia, Fake coronavirus map delivers azorult malware, Information Security at UVA[Online]. Available: https://security.virginia.edu/fake-coronavirus-map.
[76] Kaspersky, It threat evolution q1 2020. statistics, SecureList[Online]. Available: https://securelist.com/it-threat-evolution-q1-2020-statistics/96959/.
[77] SonicWall, Sonicwall Cyber Threat Report, 2020.
[78] Scribd, Cyberattack report 2019, [Online]. Available: https://www.scribd.com/document/43353177-June-2019/.
[79] Interpol, Interpol launches awareness campaign on covid-19 cyberthreats, Interpol [Online]. Available: https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-launches-awareness-campaign-on-COVID-19-cyberthreats.
[80] D. Galov, Remote spring: the rise of rdp bruteforce attacks, Secure List[Online]. Available: https://securelist.com/remote-spring-the-rise-of-rdp-bruteforce-attacks/96820/.
[81] A. Akinbi, M. Forshaw, V. Blinkhorn, Contact Tracing Apps for Covid-19 Pandemic: Challenges and Potential, Aug 2020, https://doi.org/10.31219/osf.io/6xbcs. URL osf.io/6xbcs.
[82] K. Crawley, Bluetooth security risks explained, AT&T[Online]. Available: https://cybersecurity.att.com/blogs/security-essentials/bluetooth-security-risks-explained.
[83] D. Antonioli, N.O. Tippenhauer, K. Rasmussen, Bias: bluetooth impersonation attacks, in: 2020 IEEE Symposium on Security and Privacy (SP), 2020, pp. 549–562, https://doi.org/10.1109/SP40000.2020.00093.
[84] M. R. Hussein, A. B. Shams, E. H. Apu, K. A. A. Mamun, M. S. Rahman, Digital Surveillance Systems for Tracing Covid-19: Privacy and Security Challenges with Recommendations, arXiv preprint arXiv:2007.13182.
[85] H. Cho, D. Ippolito, Y.W. Yu, Contact Tracing Mobile Apps for Covid-19: Privacy Considerations and Related Trade-Offs, 2020 arXiv:2003.11511.
[86] A. Mauro, Coronavirus contact tracing poses serious threats to our privacy, The Conversation[Online]. Available: https://theconversation.com/coronavirus-contact-tracing-poses-serious-threats-to-our-privacy-137073.
[87] S.A. Tovino, The hipaa privacy rule and the eu gdpr: illustrative comparisons, Seton Hall Review 47 (4) (2017) 973–993.
[88] European Commission, The general data protection regulation[Online], Available: https://gdpr.eu/tag/gdpr/.
[89] Office for Civil Rights, Notification of enforcement discretion for telehealth remote communications during the covid-19 nationwide public health emergency, US Health & Human Services[Online]. Available: https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html.