Bartın Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi,
BÜİİBFD, 2023, Cilt 14, Sayı 28

Bartın University Journal of Faculty of Economics and Administrative Sciences,
BUJFEAS, 2023, Volume 14, Issue 28

E-ISSN: 2148-2497
https://dergipark.org.tr/tr/pub/bartiniibf

Araştırma Makalesi, Gönderim Tarihi: 18.05.2023; Kabul Tarihi: 13.08.2023
DOI: 10.47129/bartiniibf.1299156

COVID-19-Related Cyberattacks and Precautions Taken by Countries

Mertkan SİNOPLU

Bartın Üniversitesi, Lisansüstü Eğitim Enstitüsü, Bilgisayar Teknolojisi ve Bilişim Sistemleri
mertkansinoplu@gmail.com, Orcid ID: 0000-0003-4642-5090

Eyüp Burak CEYHAN

Bartın Üniversitesi, Mühendislik, Mimarlık ve Tasarım Fakültesi, Bilgisayar Mühendisliği
eyupburak@gmail.com, Orcid ID: 0000-0002-5005-968X

Abstract

The coronavirus pandemic, which occurred at the end of 2019, started being seen worldwide in early 2020. Later, the number of deaths due to this pandemic increased rapidly in almost all countries. Since it has reached significant dimensions, the desire of people to learn about this pandemic and the decisions taken regarding the pandemic has increased. As a result, the number of cyberattacks has increased. Stealing user information via e-mails sent as if they are related to coronavirus, and attacks on the systems of health institutions and organizations are the leading coronavirus-related cyberattacks. In this study, a brief description of the coronavirus was made, the types of cyberattacks were mentioned, the cyberattacks originating from coronavirus and the precautions taken by the countries against these attacks were comprehensively examined, and the inferences obtained were presented.

Keywords: Cyberattack, cybersecurity, coronavirus, COVID-19, precaution

JEL Classification: L86, O50

APA: Sinoplu, M. & Ceyhan, E.B. (2023). COVID-19-Related Cyberattacks and Precautions Taken by Countries. *Bartın Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 14(28), 98-116.

COVID-19 Bağlantılı Siber Saldırılar ve Ülkelerin Aldıkları Önlemler

Öz

2019 yılının sonlarında ortaya çıkan koronavirüs pandemisi, 2020 yılının başlarında tüm dünyada görülmeye başlanmıştır. Daha sonra bu pandemi nedeniyle ölenlerin sayısı hemen hemen tüm ülkelerde hızla artmıştır. Ölüm sayıları önemli boyutlara ulaştığı için insanların bu pandemiyi ve pandemiyle ilgili alınan kararları öğrenme isteği artmıştır. Sonuç olarak, siber saldırıların sayısı artmıştır. Koronavirüs ile ilgiliymiş gibi gönderilen e-postalar yoluyla kullanıcı bilgilerinin çalınması ve sağlık kurum ve kuruluşlarının sistemlerine yönelik saldırılar, koronavirüs bağlantılı siber saldırıların başında gelmektedir. Bu çalışmada koronavirüsün kısa bir tanımı yapılmış, siber saldırı türlerinden bahsedilmiş, koronavirüs kaynaklı siber saldırılar ve bu saldırılara karşı ülkelerin aldığı önlemler kapsamlı bir şekilde incelenmiş ve elde edilen çıkarımlar sunulmuştur.

Anahtar Kelimeler: Siber saldırı, siber güvenlik, koronavirüs, COVID-19, önlem

JEL Sınıflandırması: L86, O50

1. Introduction

A new virus that could be transmitted to humans emerged in China towards the end of 2019 (Akbaba et al, 2014). This virus was first defined as a case of pneumonia (McIntosh, 2020). It is acknowledged that there were similar viruses before; however, they were identified not to be as fatal as the new virüs (Van der Hoek et al., 2004: 368). That the virus is fatal and encountered all around the world has caused cyberattacks to increase in number (Habertürk, 2020). Upon the emergence of the virus, the rates of fraud in March 2020 increased by 400%, which made the coronavirus the greatest cyber threat ever (ActionFraud, 2020). Since the number of cyberattacks has increased with coronavirus, the things to do against these two threats are presented in Table 1 (Arc, 2020).

Table 1: Coronavirus-related Cyberattacks

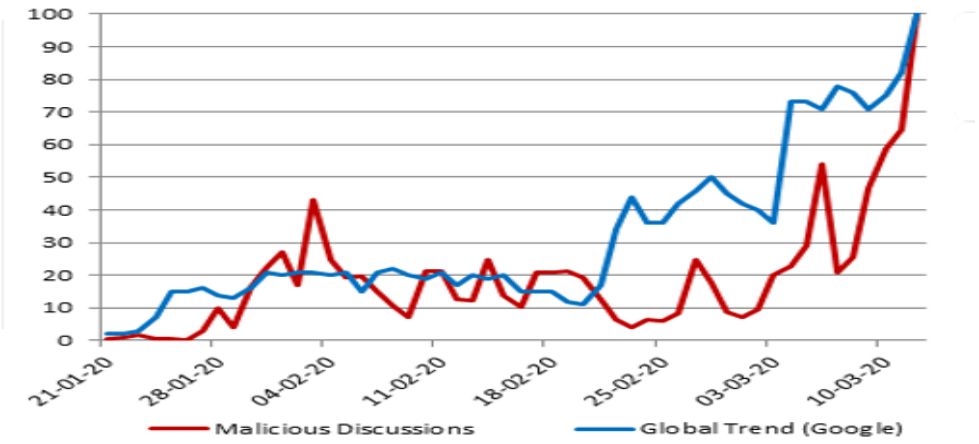
		Coronavirus	Cybersecurity
Avoiding Entry	**Raising Awareness**	Travel consultants encouraging citizens to avoid high-risk areas to decrease the chance of getting infected	Security awareness training and tools to prevent people from risking personal information and passwords
	Interference	Border tests or those entering the country Quarantine of those with symptoms	DMZ, perimeter firewalls, virtual spaces, software for protection from malware
R ed	**Protection**	Restrictions regarding schools and social activities in regions	Network segmentation

		with active cases	
	Hygiene	Hand-washing and regional sanitation	Security hygiene – Vulnerability, policy and concession management
Managing Infections	**Early Detection**	Encouraging those with symptoms to get medical help in time	Detecting abnormalities and violations, and SIEM
	Rapid Diagnosis and Treatment	Distributing test kits – special response teams and facilities - vaccines	SOAR and other tools to help defenders identify, isolate and fix concessions
Reducing Future Threats	**Prevention**	Distributing vaccines	Developing malware signatures and IOCs
	Advanced Warning	Continuous monitoring of health warnings	Threat intelligence

Source: (Arc, 2020)

After the coronavirus pandemic got around the world, cyber criminals used the internet to benefit from this chaos. When Figure 1 is examined, it is observed that malicious discussions and cybercrimes increase as the number of Google search on coronavirus increases (Checkpoint, 2020a).

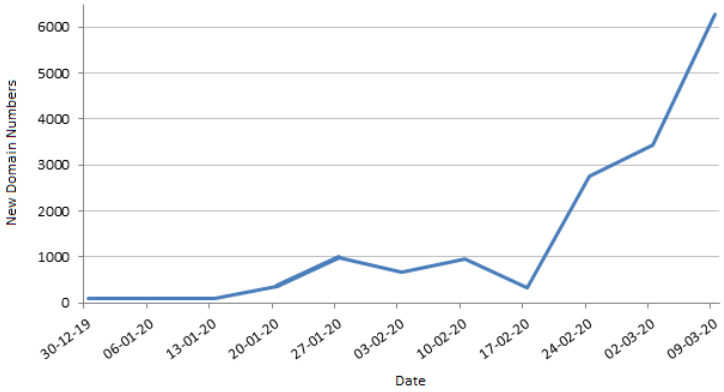
Figure 1: Coronavirus-related Malicious Discussions and Trends



Source: (Checkpoint, 2020a)

Along with the increase in Figure 1, a substantial increase in the number of coronavirus-related domain names is observed in Figure 2 (Checkpoint, 2020a).

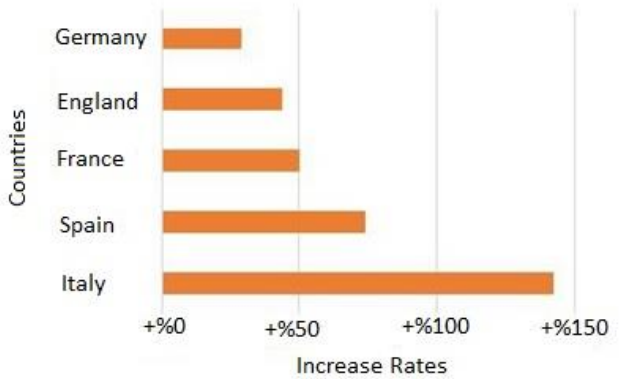
Figure 2. Weekly Change in the Number of Coronavirus-related Domains



Source: (Checkpoint, 2020a)

Moreover, individuals' desire to receive information about the coronavirus and visits to news sources on the Internet have increased dramatically in number. For instance, the increase in visits to news websites and applications in Europe between 5 January 2020 and 15 March 2020 is presented in Figure 3 (Statista, 2020).

Figure 3: Increase Rates of Visits to News Websites and Applications in Some Countries After the Coronavirus



Source: (Statista, 2020)

Cyberattacks are generally used to hack personal information or systems (Aslay, 2017: 25). The hacked personal information or systems can also affect the things that they interact as well as the target itself. For example, as a result of an attack on an electronic shopping website, both the website and its users may get harmed.

It can be stated that cybersecurity has become more important with the developing technology. Consequently, it can be observed that cybersecurity and cyberattack analyses are increasing day by day. For instance, in the study by Case (2016), an analysis on the cyberattack against an electric network in Ukraine was conducted. It was identified that system computers were attacked through a virus preventing computers from restarting. Due to the attack, 700 thousand people had no electricity for hours.

Cybersecurity precautions are taken by governments as well as companies. In her study, Halchin (2004) revealed the effects of attacks on the websites of public institutions. In addition, she investigated the countries' security capacity in the electronic environment and the precautions that they took.

As an example of the studies in the literature dealing with cyberattacks on healthcare institutions, Wright et al. (2016) discussed studies conducted in US health institutions in their study. In the study, they focused on explaining phishing attacks. The difference of the study from this study is that it deals with the cyberattacks that took place during the coronavirus period.

The difference of this study from literature is that scope of this study is coronavirus-related cyberattacks that took place at the time of the coronavirus pandemic. Within the scope of this comprehensive study, only cyberattacks that took place during the coronavirus pandemic were discussed and reviewed. In this purpose, the cyberattacks were examined in terms of different criteria as the target, purpose, method and result of the attack.

The purpose of this study is to compare the coronavirus-related cyberattacks between 2020 and 2023 and the precautions that governments have taken against these attacks. In addition, the types of cyberattacks and how to act against these attacks are explained. In the second section of the study, a brief description of coronavirus was made. In the third section, the types of cyberattacks were mentioned. In the fourth section, the coronavirus- related cyberattacks and the precautions taken by the governments against these attacks were investigated comprehensively, and in the last section, the inferences obtained were presented.

2. Coronavirus

Coronavirus is a type of virus that can cause illness in humans and animals, and it was first encountered in China in 2002 (Van der Hoek et al, 2004). However, the coronavirus discussed in this study is a different member of the same family, was first identified in the last days of 2019, and is called COVID-19 or 2019-nCoV (Lu et al., 2020: 566). After being identified in China, this virus soon began to be encountered all around the world, and caused a great number of deaths (World Health Organization, 2020a).

The most prominent symptoms of the virus are respiratory diseases including high fever, cough and shortness of breath; however, in serious cases, there can be renal failure

and severe respiratory tract infection, and these symptoms are known to be followed by the risk of death (Til, 2020).

The best ways for protection from the coronavirus are washing your hands, wearing a mask, keeping your hands away from your eyes and nose, and attending to social distance rules (Alıcılar and Meltem, 2020).

3. Cyberattacks

Cyberattacks can be classified as attacks on systems and attacks on individuals. They are generally used to shut down or get in systems and steal or change data (Öztürk, 2018: 211). Types of cyberattacks used for these purposes are as follows:

- **Infiltration:** It is the type of cyberattack usually known as hacking. It aims at obtaining data by infiltrating into systems (Değirmenci, 2006).

- **Virus:** Viruses are mostly used to harm systems and steal information (Arc, 2020).

- **Super Zapping:** These are the attacks to lock systems with failures (Turhan, 2006).

- **Data Diddling:** These are the attacks in which data are incorrectly inserted into computer or changed while saving (Çubukçu and Bayzan, 2013: 154).

- **Phishing:** It is mostly used for fraud through fake websites, which are generally composed of the same themes as the original websites. In this way, it is difficult for users to differentiate (Çubukçu and Bayzan, 2013: 154).

- **Logic Bombs:** They are usually used to wipe out the data on a system (Arc, 2020).

- **Spam:** It includes sending a huge number of emails without recipient request (Yetim, 2014).

- **DOS/DDOS:** DOS/DDOS (Denial of Service/Distributed Denial of Service) attacks are used to disable systems and servers by inundating the bandwidth of the target systems (Öztürk, 2018: 211).

It can be said that the biggest effects of cyberattacks are the disruption of systems, the seizure of private information such as database, identity and bank information, and the blackmailing of this information. The security of visited web pages and downloaded resources plays an important role in preventing these attacks. In addition, it can be stated that these are the most frequently encountered cyberattacks.

3.1. Cyberattacks on Systems

Cyberattacks on systems generally include super zapping, logic bombs, data diddling, DOS/DDOS and infiltration.

As an example, Can and Şahingöz (2015) in their study focused on developing a system that could detect infiltration attacks on systems. They aimed that the system would work faster by making use of artificial neural networks while developing the system. At the end of the study, they could detect the incoming attacks by 98.64%.

As another example regarding attacks on systems, Karaarslan and Akbaş (2017) focused on blockchain-based cybersecurity systems in their study. They presented the advantages and disadvantages of using blockchain technology in the field of cybersecurity systems. Furthermore, they emphasized that these systems could be utilized in banking, smart city systems and computer networks.

It is observed that cyberattacks targeting systems can be against public institutions as well as private companies. It is possible to see that public institutions take precautions against these attacks. In their study, Abrams and Weiss (2008) identified what kind of cyberattacks that the institution of Maroochy Water Services situated on Maroochy river in Australia could encounter and made suggestions on what kind of precautions could be taken against these attacks and what could be done to improve cybersecurity

3.2. Cyberattacks on Individuals

Cyberattacks on individuals generally include phishing, spam, infiltration and DOS/DDOS attacks.

There is a great deal of research on cyberattacks launched against individuals. For instance, Buber et al. (2017) focused in their study on a system to detect phishing attacks from website extensions. With this system, they planned to increase user security against phishing attacks. As a result of the study, they could develop a system to identify the URLs used in phishing attacks.

In their study, Uysal et al. (2012) focused on a system to identify spam texts sent to individuals' phones. While developing this system, they made use of the decision tree algorithms. They also proved which decision tree algorithm worked better in terms of performance. Accordingly, they decided that the best algorithm to be used in the system was k-Nearest Neighbors algorithm.

4. Coronavirus Related Cyberattacks

With coronavirus encountered throughout the world and the number of infected people increasing, cyberattacks have also increased in number (Yeni Şafak, 2020). To set an example, the 4 possible cybersecurity threats related to the coronavirus include attacks

on ventilation and life support devices, phishing attacks via email, attacks on cloud systems due to homeworking, and attacks on remote healthcare services (AHA, 2020).

These attacks can be examined in two categories as attacks on systems and attacks on individuals.

4.1. Coronavirus-related Cyberattacks on Individuals

Phishing can be stated to be the most frequently used method for coronavirus-related cyberattacks on individuals. That Pakistan-related hackers sent phishing emails to citizens as if they were from the Indian Government and stole user information can be presented as an example (T. Print, 2020). In this attack, hackers used a mail extension quite similar to that of the Indian government, and sent users a link directing them to an informative website about coronavirus. They directed users who clicked on this link to a fake website and stole their personal information such as passwords, credit card information and location. When the Indian Government realized this attack, they consulted to Subex, an Indian-based cybersecurity company. Subex started to work on the emails to see what kind of harm that the attack did to users' computers. At the end of their work, Subex explained those individuals what needs to be done.

Another case is that the website of the World Health Organization was replicated by hackers, and personal information of the users visiting this website was stolen (Hürriyet, 2020). It was stated that the documents with information on coronavirus in these websites contained malicious software and were used to spread malware. Besides, on the same websites, they tried to raise a fund by bitcoin for coronavirus-related health expenses under the title of "COVID-19 Solidarity Response Fund". Sophos security company identifying some of these websites stated that users should check the extensions while visiting websites and not rely on information except for that coming from reliable sources. In addition, they emphasized that those requesting bitcoin for donation should not be believed.

In their statement regarding coronavirus-related cyberattacks, the World Health Organization indicated that the number of cyberattacks on their staff increased dramatically due to coronavirus (Word Health Organization, 2020b). The Organization stated that their 450 email addresses and passwords were hacked within the week of the statement. It was also notified to be possible that, with the hacked email addresses, personal data of the users could be stolen by sending them emails as sent by the staff of the World Health Organization. People were requested to be alert against this kind of emails and to make use of reliable sources for health issues. As a precaution, the Organization switched to a more advanced system.

4.2. Coronavirus-related Cyberattacks on Systems

Coronavirus-related cyberattacks on systems generally involve infiltration and virus attacks. Virus attacks on healthcare institutions and organizations can be an example of these attacks (Threat Post, 2020). The purpose of these attacks was to prevent

institutions and organizations conducting studies on coronavirus from working. These attacks affected the United States of America defense research companies, Turkish Ministry of Foreign Affairs, German industrial firms and Korean chemical production firms as well as medical research companies in Japan and Canada. The attacks were determined to be performed via email containing a kind of virus called AgentTesla in the attachment.

The cyberattack on the computer systems of the US Department of Health and Human Services can be presented as another example for these attacks (Bloomberg, 2020). The attack is known to have been performed through infiltrating into the computer systems of the US Department of Health and Human Services, stealing and changing important data. The government who started an investigation about this attack stated that its source could be extraterritorial but it had not been confirmed yet. With DDOS attacks launched in the meantime, it was aimed to slow down and disable the systems. However, according to the statement, the impacts of DDOS attack were not felt.

Another cyberattack against government websites was that Vietnamese hackers attacked on China Department of Emergency Management and Wuhan government (Reuters, 2020). In this attack, a hacker group called APT32 stole the email accounts of officials working for China Department of Emergency Management and Wuhan government. In the statement made by FireEye Security Company, it was indicated that this hacker group could be working with the Vietnamese government, and the previous attacks of the group were presented as the reason. The Vietnamese government remained unresponsive to this statement.

In another case, cyberattacks targeted the hospitals and airports situated in Czech Republic (Washington Post, 2020). The attacks aimed at wiping out the systems and important data that they contained. According to the statement by the Czech government, these attacks were suppressed successfully, and precautions were required against greater cyberattacks in the future. Besides, Czech authorities gave no names regarding the attacks but stated to be worried that the attacker was a hacker supported by the government rather than a criminal.

Cyberattackers are observed to launch attacks against institutions conducting studies on the coronavirus. For instance, Russian spies carried out cyberattacks on institutions researching the coronavirus in England, the USA and Canada (BBC News, 2020a). It was indicated that, in these attacks, the attackers aimed at stealing the studies to develop a vaccine against the coronavirus. The institutions exposed to the attacks were not revealed in the statement but it was announced that the attackers failed to obtain the studies. The Russian government declared not to assume responsibility for this issue.

In another cyberattack against institutions conducting research on the coronavirus, Japanese vaccine producers were the targets (Anadolu Agency, 2020). Japanese vaccine producers indicated to have been exposed to these attacks starting from April 2020. According to the American CrowdStrike security company, the attack was carried out in Japan for the first time, and the attackers were Chinese. The attack was also stated to be

performed by sending the vaccine producers emails containing viruses. Scott Jarkoff, the Asia-Pacific regional manager of the company declared that the cyberattacks were on Japan that could be the first country to produce vaccine against the coronavirus, and it was to slow down the vaccine production. According to the statement, no data was stolen during the attack.

As a result of the attack on Indian-based Dr. Reddy's Medicine Company developing a vaccine for the coronavirus (BBC News, 2020b); England, Russia, Brazil, India and the USA websites of the company were stated to be affected. The company indicated to isolate all the data center services in order to bring the attack under control, and refused to comment on whether their manufacturing facilities were affected by the attack or not. On the other hand, the local press in India reported that production was interrupted in some facilities of Dr. Reddy's company.

In the attack by North Korean hackers on Pfizer Company developing and producing the coronavirus vaccine, the hackers attempted to steal the vaccine data (Computer Weekly, 2020). According to the intelligence service of South Korea, the attack was carried out by North Korea. Since the attack was detected in time, no harm was done. Nevertheless, Pfizer Company made no statement about this attack.

Coronavirus-related cyberattacks have been against communities as well as countries. The cyberattack on the United Nations health agency can be given as a relevant example (ZDNet, 2021b). It was declared that data related to the coronavirus treatment and vaccine were stolen in this attack. It was also announced that vaccine-related data of third-party companies were leaked. No statement was made regarding who or which country conducted the attack.

It is observed that coronavirus-related cyberattacks are mostly against public institutions. In addition, universities have also been targeted in coronavirus-related cyberattacks. In the attack on COVID-19 laboratory of Oxford University (We Live Security, 2021), it was aimed to obtain the studies on COVID-19. In the statement, it was indicated that there was no data regarding the patients and vaccine development in the system attacked. Even though the impacts of the attack were not revealed, those who wanted to buy the stolen data were indicated to be rich people and even some governments. In Table 2, a summary of coronavirus-related cyberattacks is presented

Another cyberattack was the attack on the Brazilian Ministry of Health (ZDNet, 2021a). Hackers acquired and deleted the COVID-19 vaccination data of millions of citizens from government's databases. International hacker group called "Lapsus$" has claimed responsibility for the attack. Less than a week later, they leaked the data of millions of Brazilians online. The Brazilian government is still investigating this issue.

Another method of cyberattack is hacking mobile apps. Chinese Shanghai government had the same issue in their COVID-19 health app called "Suishenma" (Reuters, 2022). Chinese hackers with the username "XJP" hacked the health app and

acquired 48.5 million user's personal data and offered to sell it for $4000. Shanghai government has yet to make a statement on the matter.

As another example of attacks on systems is the cyber attack on the St. Margaret hospital (SC Media, 2023). In this attack, the attackers attacked the hospital's network services such as email and patient portal. As a result of this attack, the hospital suffered a enterprise network outage that lasted several weeks but patient care continued uninterrupted, thanks to the previously applied closure procedures.

Cyberattack on Johnson Memorial Health hospital (NPR, 2023) is one of the another coronavirus related cyberattack on hospitals. Hackers attack the hospital's servers and left a ransom note on every server. They demand three million dollars in Bitcoin in the next few days. As a result, hospital's personel have to use paper and pen for medical reports for weeks. In the end, hospital did not pay the ransom and rebuild new servers for the records and fortified the security of the systems.

As seen, there have been many coronavirus-related cyberattacks against systems and individuals. Details of all the above-mentioned coronavirus-related cyberattacks are given in Table 2.

Table 2: Coronavirus-related Cyberattacks

ID	Attack	Target	Purpose	Method	Result
1	Stealing user information by pretending to be Indian government (T. Print, 2020)	Individuals	Obtaining user information such as passwords, credit card numbers etc.	Phishing	Attackers obtained users' personal information. Indian government started investigation.
2	Stealing personal information by replicating the World Health Organization website (Hürriyet, 2020)	Individuals	Obtaining user information such as passwords, credit card numbers etc. Requesting Bitcoin as if donation	Phishing	It was stated that users should check the extensions while visiting websites and not rely on any information other than that of reliable sources.
3	Cyberattacks on the World Health Organization staff (Word Health	Individuals	Obtaining users' personal information	Phishing	450 active email accounts of the World Health Organization staff were hacked. As a result, World Health Organization switched to a more advanced

	Organization, 2020b)				system, and also warned users against scammers.
4	Attacks on healthcare organizations (Threat Post, 2020)	Systems	Preventing the studies conducted	Virus, Infiltration	As a result of the attack, studies on health were disrupted. The attacks were determined to be via mail by using a virus called AgentTesla.
5	Cyberattack on computer systems of the US Department of Health and Human Services (Bloomberg, 2020)	Systems	Stealing and changing important information	Infiltration, Data Diddling, DDOS	The source of the attacks could not be identified. Also, the DDOS attack failed.
6	Attack of Vietnamese hackers on Wuhan government (Reuters, 2020)	Systems	Stealing email accounts of the staff working for the institutions	Infiltration, Virus	Attackers were stopped before they could harm the system.
7	Attacks on hospitals and airports in Czech Republic (Washington Post, 2020)	Systems	Destroying the data and the system	Infiltration, Virus, Super Zapping	The attacks were successfully suppressed, and it was stated that precautions should be taken against greater attacks in the future.
8	Attacks on institutions conducting studies on coronavirus (BBC News, 2020a)	Systems	Hacking the data	Infiltration, Virus	Works of health institutions were slowed down and data about treatment were stolen.
9	Cyberattacks on Japanese vaccine producers (Anadolu Agency, 2020)	Systems	Disrupting works, data theft	Infiltration, Virus	Vaccine studies were disrupted. No information was stolen. The attackers were identified to be Chinese. After the attack, system security has been increased.
10	Cyberattack on India-based Dr. Reddy's	Systems	Disrupting works	Infiltration, Virus	The company websites were deactivated. It was also announced that production was disrupted in some

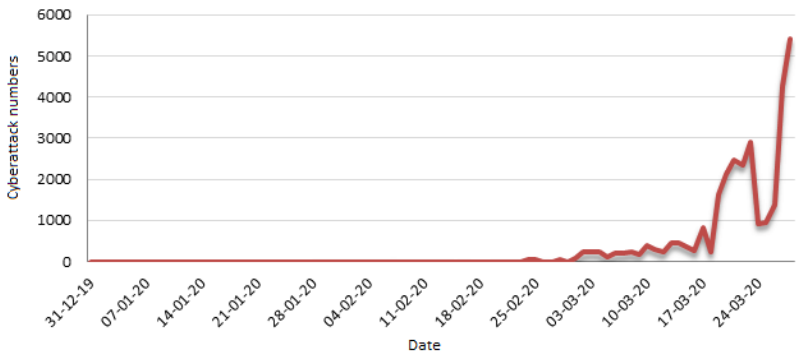
	medicine company BBC News, 2020b)				manufacturing plants of the company in India.
11	Cyberattack on Pfizer company (Computer Weekly, 2020)	Systems	Data theft	Infiltration	There was no harm due to early detection of the attack.
12	Cyberattack on the United Nations health agency (ZDNet, 2020b)	Systems	Data theft	Infiltration	Information about coronavirus treatment and vaccines was leaked.
13	Attack on Oxford University COVID- 19 laboratory (We Live Security, 2021)	Systems	Data theft	Infiltration	Even though the effects of the attack were not disclosed, it was indicated that those who wanted to pay for the stolen data were rich people and even governments.
14	Attack on Brazilian Ministry of Health (ZDNet, 2020a)	Systems	Data theft, destroying data	Infiltration	Millions of citizen's vaccination data deleted from databases. Also, citizen's data is leaked and shared online.
15	Attack on Chinese health app (Reuters, 2022)	Systems	Data theft	Infiltration	48.5 million citizen's data was stolen. Hacker offered to sell the data. Government has yet to comment about attack.
16	Attack on St. Margeret hospital (SC Media, 2023)	Systems	Data theft	Infiltration	The hospital suffered a enterprise network outage that lasted several weeks.
17	Attack on Johnson Memorial hospital (NPR, 2022)	Systems	Data theft	Infiltration	Hospital's personel have to use paper and pen for medical reports for weeks and need to rebuilt servers. They have also increased the security of the systems.

Conclusions

Regarding the coronavirus-related cyberattacks, it is observed that phishing method is generally used against individuals, and infiltration and DOS/DDOS methods against systems. It can be stated that the purpose of attacks on individuals is usually to steal personal information whereas the purpose of coronavirus-related cyberattacks on systems is usually to steal data and deactivate the systems.

As a result of the study, it was seen that cyberattacks increased with the coronavirus pandemic. Increasing number of cyberattacks related to the coronavirus can be seen in Figure 4 (Checkpoint, 2020b) that supports this result.

Figure 4: Increasing Numbers of Coronavirus Related Cyberattacks



Source: (Checkpoint, 2020b)

As a result of the coronavirus-related cyberattacks both on individuals and systems, it is observed that governments have tried to identify the sources of these attacks through state-owned or other companies. Moreover, following these attacks, government officials and cybersecurity companies have informed users about what kind of precautions that they need to take to protect themselves from this kind of attacks.

Against the cyberattacks related to coronavirus, it is recommended that information should be received only from official sources, extensions in the emails should be checked, and attention should be paid that the donations requested for coronavirus are from the right sources.

It is foreseeable that the majority of coronavirus- related cyberattacks can be avoided mainly by taking the aforementioned criteria into account. As a similar suggestion to this suggestion, Alawide et al. (2022) emphasized that the government and companies should take more measures to inform people about these attacks, as a result of their studies examining the cyberattacks related to the coronavirus.

In future studies, it is anticipated that a more comprehensive cyberattack review study can be made by including other attacks against health institutions as well as coronavirus-related cyberattacks. With help of more comphrehensive study, what has been done and what can be done against cyberattacks can be specified more comprehensively.

References

Abrams, M., and Weiss, J. (2008). Malicious Control System Cyber Security Attack Case Study–Maroochy Water Services, Australia, McLean, VA: The MITRE Corporation.

ActionFraud (2020). Coronavirus-Related Fraud Reports Increase by 400% in March. Available: https://www.actionfraud.police.uk/alert/coronavirus-related-fraud-reports-increase-by-400-in-march (Accessed 16.05.2023).

AHA (2020). 4 Possible Cybersecurity Risks Related to COVID-19. Available: https://www.aha.org/sites/default/files/inline-images/cyber%20corona%20blog.jpg (Accessed 16.05.2023).

Akbaba, M., Kurt, B. ve Nazlıcan, E. (2014). Yeni Coronavirus Salgını", *Turk J Public Health*, *12*(3), 217-227.

Alawida, M., Omolara, A. E., Abiodun, O. I., and Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University-Computer and Information Sciences*, *34*(10), 8179-8026.

Alıcılar, H. E. ve Meltem, Ç. (2020). Yeni Koronavirüs Salgını: Korunmada Etkili Yaklaşımlar", Available: https://korona.hasuder.org.tr/yeni-koronavirus-salgini-korunmada-etkili-yaklasimlar/ (Accessed 16.05.2023).

Anadolu Agency (2020). Japanese Vaccine Producers Under Cyber Attacks: Reports. Available: https://www.aa.com.tr/en/asia-pacific/japanese-vaccine-producers-under-cyber-attacks-reports/2011306 (Accessed 16.05.2023)

Arc (2020). Coronavirus Lessons for Industrial Cybersecurity. Available: https://www.arcweb.com/blog/coronavirus-lessons-industrial-cybersecurity (Accessed 16.05.2023)

Aslay, F. (*2017*). Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi. *International Journal of Multidisciplinary Studies and Innovative Technologies*, 11, 24-28.

BBC News (2020a). Coronavirus: Russian Spies Target Covid-19 Vaccine Research. Available: https://www.bbc.com/news/technology-53429506 (Accessed 16.05.2023).

BBC News (2020b). Dr Reddy's: Covid Vaccine- Maker Suffers Cyber-Attack. Available: https://www.bbc.com/news/technology-54642870 (Accessed 16.05.2023).

Bloomberg (2020) . Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak. Available: https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response (Accessed 16.05.2023).

Buber, E., Diri, B., and Şahingöz Ö. K. (2017). Detecting Phishing Attacks from URL by Using NLP Techniques, *International Conference on Computer Science and Engineering (UBMK)*, 337-342.

Can, O., and Şahingöz, Ö. K. (2015). An Intrusion Detection System Based on Neural Network. *23nd Signal Processing and Communications Applications Conference* (SIU), 2302-2305.

Case, D. U. (2016). Analysis of the Cyber Attack on the Ukrainian Power Grid. *Electricity Information Sharing and Analysis Center (E-ISAC)*, 388, 1-29.

CheckPoint (2020a). COVID-19 Impact: As Retailers Close their Doors, Hackers Open for Business – Check Point. Available: https://cyberriskleaders.com/covid-19-impact-as-retailers-close-their-doors-hackers-open-for-business-check-point/ (Accessed 16.05.2023).

CheckPoint (2020b). Coronavirus update: In the cyber world, the graph has yet to flatten. Available: https://blog.checkpoint.com/security/coronavirus-update-in-the-cyber-world-the-graph-has-yet-to-flatten/ (Accessed 20.07.2023).

Computer Weekly (2020). North Korea Accused of Pfizer Covid Vaccine Cyber Attack. Available: https://www.bbc.com/news/technology-54642870 (Accessed 16.05.2023)

Çubukcu, A. ve Bayzan, Ş. (2013). Türkiye'de Dijital Vatandaşlık Algısı ve bu Algıyı Internetin Bilinçli, Güvenli ve Etkin Kullanımı ile Artırma Yöntemleri. *Middle Eastern & African Journal of Educational Research*, 5, 148-174.

Değirmenci, O. (2002). Bilişim Suçları. Unpublished Master Thesis. Marmara University, İstanbul.

Habertürk (2020). Koronavirüs Salgınıyla Beraber Siber Saldırılar Arttı. Available: https://www.haberturk.com/koronavirus-salginiyla-beraber-siber-saldirilar-artti-2626969-teknoloji (Accessed 16.05.2023)

Halchin, L. E. (2004). Electronic Government: Government Capability and Terrorist Resource. *Government Information Quarterly, 21*(4), 406-419.

Hürriyet (2020). Koronavirüs Odaklı Yeni Siber Saldırı Tekniklerine Dikkat!. Available: https://www.hurriyet.com.tr/teknoloji/koronavirus-odakli-yeni-siber-saldiri-tekniklerine-dikkat-41472847 (Accessed 16.05.2023).

Karaarslan, E. ve Akbaş, M. F. (2017). Blokzinciri Tabanlı Siber Güvenlik Sistemleri. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, *3*(2), 16- 21.

Lu, R. et al. (2020). Genomic Characterisation and Epidemiology of 2019 Novel Coronavirus: Implications for Virus Origins and Receptor Binding. *The Lancet*, 395 10224, 565-574.

McIntosh, K. (2020). Coronaviruses. Available: https://www.uptodate.com/contents/coronaviruses (Accessed 16.05.2023).

NPR (2022). Cyberattacks on health care are increasing. Inside one hospital's fight to recover. Available: https://www.npr.org/sections/health-shots/2023/05/08/1172569347/cyberattacks-on-health-care-are-increasing-inside-one-hospitals-fight-to-recover (Accesed 16.05.2023)

Öztürk M. S. (2018). Siber Saldirilar, Siber Güvenlik Denetimleri ve Bütüncül bir Denetim Modeli Önerisi. *Journal of Accounting & Taxation Studies (JATS)*, Special Issue of the 10th Year, 208-232.

Reuters (2020). Vietnam-linked Hackers Targeted Chinese GovernmentOver Coronavirus Response: Researchers. Available: https://www.reuters.com/article/us-health- coronavirus-cyber-vietnam/vietnam-linked-hackers-targeted-chinese- government-over-coronavirus-response-researchers-idUSKCN2241C8 (Accessed 16.05.2023)

Reuters (2022). Hacker offers to sell data of 48.5 million users of Shanghai's COVID app. Available: https://www.reuters.com/world/china/hacker-offers-sell-data-485-mln-users-shanghais-covid-app-2022-08-12/ (Accessed 16.05.2023)

SC Media (2023). Citing cyberattack, COVID-19 impacts, Illinois hospital suspends operations. Available : https://www.scmagazine.com/analysis/ransomware/citing-cyberattack-covid-19-impacts-illinois-hospital-suspends-operations (Accesed 16.05.2023)

Statista (2020). Coronavirus Drives European Hunger For News. Available: https://www.statista.com/chart/21215/incr ease-in-news-consumption-europe-covid19/ (Accessed 16.05.2023)

T. Print (2020). Pakistan-linked Hackers Pose as Indian Govt. Carry Out Cyberattacks Under Covid-19 Cover. Available: https://theprint.in/tech/pakistan-linked-hackers-pose-as-indian-govt-carry-out-cyberattacks-under-covid-19-cover/407366/ (Accessed 16.05.2023)

Threat Post (2020). Cyberattacks Target HealthcareOrgs on Coronavirus Frontlines. Available: https://threatpost.com/cyberattacks-healthcare-orgs-coronavirus-frontlines/154768/ (Accessed 16.05.2023)

Til, U. D. A. (2020). Yeni Koronavirüs Hastalığı Hakkında Bilinmesi Gerekenler. *Ayrıntı Dergisi*, (8 85, 53-57.

Turhan, O. (2006). Bilgisayar Ağları ile İlgili Suçlar (Siber Suçlar). State Planning Organization Undersecretariat of Legal Counsel, Planning Specialization Thesis, Ankara.

Uysal, A. K., Günal, S., Ergin, S., and Günal, E. Ş. (2012). Detection of SMS Spam Messages on Mobile Phones. *20th Signal Processing and Communications Applications Conference (SIU)*, 1-4.

Van der Hoek, L. et al. (2004). Identification of a new human coronavirus. *Nature medicine*, *10*(4), 368-373.

Washington Post (2020). The Cybersecurity 202: Coronavirus Pandemic has not Stopped Cyberattacks on Hospitals and Other Vital Infrastructure. Available: https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2020/04/20/the-cybersecurity-202-coronavirus-pandemic-has-not-stopped-cyberattacks-on-hospitals-and-other-key-targets/5e9caee2602ff10d49ae8640/ (Accessed 16.05.2023)

We Live Security (2021). Oxford University COVID-19 Lab Hacked. Available: https://www.welivesecurity.com/2021/02/26/oxford-university-covid19-laboratory-hack/ (Accessed 16.05.2023)

World Health Organization (2020a). Coronavirus Disease 2019 (COVID-19): Situation Report 73. Available: https://apps.who.int/iris/handle/10665/331686 (Accessed 16.05.2023)

World Health Organization (2020b). WHO Reports Fivefold Increase in Cyber Attacks, Urges Vigilance. Available: https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance (Accessed 16.05.2023)

Wright, A., Aaron, S., and Bates, D. W. (2016). The big phish: cyberattacks against US healthcare systems. Journal of General Internal Medicine, 31, 1115-1118.

Yeni Şafak (2020). "Koronavirüs, Siber Saldırıları Tetikliyor." Available: https://www.yenisafak.com/teknoloji/koronavirus-siber-saldirilari-tetikliyor-3534225 (Accesed 16.05.2023)

Yetim, S. (2014). Siber Suçlar, Yargilama Yetkisi ve Yeni bir Model Önerisi. *Türkiye Adalet Akademisi Dergisi*, 17, 177 – 230.

ZDNet (2021a). Brazilian Ministry of Health suffers cyberattack and COVID-19 vaccination data vanishes. Available: https://www.zdnet.com/article/brazilian-ministry-of-health-suffers-cyberattack-and-covid-19-vaccination-data-vanishes/ (Accessed 16.05.2023).

ZDNet (2021b). Hackers have Leaked the COVID-19 Vaccine Data They Stole in a Cyberattack. Available: https://www.zdnet.com/article/hackers-have-leaked-the-covid-19-vaccine-data-they-stole-in-a-cyberattack/ (Accessed 16.05.2023)