Analysis of cyber-attacks intensified during the pandemic

Moraiti Christina

Abstract

During the pandemic the governments around the world came across an unseen before situation however an expected one. As the coronavirus pandemic became the "new normal" in our individual lives but moreover in our working place, getting familiar with specific technologies became more essential. Due to the increased presence of technology, cybercrime is on the rise and the number of cyber-attacks has increased significantly. Cybercriminals saw the pandemic as an opportunity to exploit, victimize and profit over the disoriented public. This situation raises the flag for a reinforcement in the security systems but also in the user education and training to enhance the cybersecurity awareness.

Introduction

The Covid-19 pandemic, is an ongoing global pandemic of SARS-CoV-2 virus causing severe acute respiratory syndrome. The new virus was discovered in December 2019 during an epidemic in Wuhan, China. Attempts to contain it weren't successful, allowing the virus to spread to other parts of China and, eventually, the rest of the world. On January 30, 2020, the World Health Organization (WHO) declared the outbreak a public health emergency of worldwide concern, which on March 11 of the same year was declared a pandemic. Up until September the 14th of 2022, the pandemic has globally caused 607,083,820 confirmed cases, including 6,496,721 deaths, making it one of the deadliest in history.[1]

The virus had a great impact in many jobs as the physical workplace shifted to a virtual workplace considering the reports of pandemic getting worse spread. Moreover, school hours were now conducted from home. The necessity of communication caused by the growing portion of the global population now living under some kind of government lockdown, led to a big increase of the usage of applications that helped employees perform their work, students attend to school via a screen and citizens to stay in touch with their colleagues, family, and friends. This high-level change implied a number of changes in the way work was conducted, particularly in terms of security. Remote working involved digital systems operating in largely insecure and unmanaged environments. In addition, a lot of employees were not accustomed to working remotely and had not received any formal training on how to do so safely. The rise of the cyber-risks ultimately led to a major spike in cyberattacks. [2]

Back in the old days sharing, transmitting and collaborating was on paper. With the progress of technology, everything came to be computerized. Everything is data now. Especially in the pandemic most of the collaborations were done over computer systems with incredible bandwidth. While the world anticipated for a potential cure in order to contain the spread of the pandemic, all the information related to Covid-19 gained great attention of the netizens. Scammers used this avenue to distribute malicious attacks to victims, frequently disguised as the government or tax authorities, with links that claimed assistance for Covid-19. The average cost of a data breach has increased by 2.6% over a year, from 2021 to 2022 reaching a cost of USD 4.35 million. A total of 12.7% average cost over 2020. [3]

Cybersecurity issues during the Covid-19 pandemic

- *Remote working*

Compared to an organizational internal network, a home network is less secure. According to data from the UK Cyber Security Breaches Survey of 2020 (Figure 1), there are ten steps on towards providing a cyber secure environment in an organization. Meanwhile, the amount to which organizations are truly complying

with those ten steps varies, with just 12% taking action against all of them. [13] It is noticeable that most firms tend to invest more in the technology-related aspects of security instead of the more policy- and people-centric aspects. The graphic clearly shows a lack of attention to the processes associated with working from home education and awareness, with just a quarter to a third of organizations claiming to have addressed them.

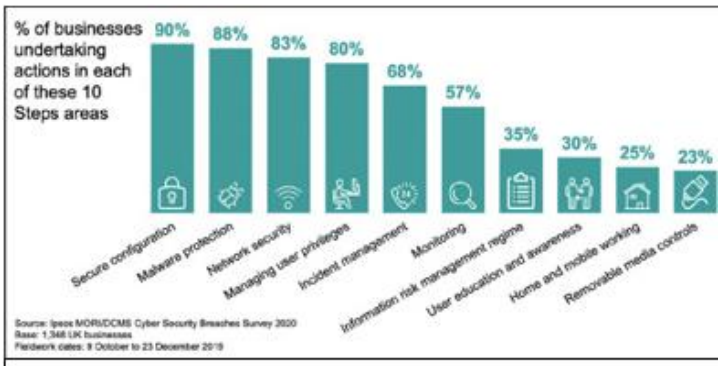

Figure 1

- *Social Scams and Phishing*

Covid-19 phishing exploded in 2020 and 2021. This happens to echoes back in 2005 when the Hurricane Katrina took place and plenty of fraudulent websites and emails solicited fake donations. Many of these scams seemed to come from organizations such as the World Health Organization (WHO) and the Centers of Disease Control (CDC). [6] For example, a citizen could receive an email which provided via registration or by clicking into a file, the service of getting in line for the vaccine for Covid-19 or an antibody test. Many people were deceived by those spear-phishing emails. The heightened fear and pressure to protect oneself over the pandemic created a less questionable attitude from the citizen over the viability and the verifiability of the email they were given and thus clicking. [8] The attacks were conducted by different platforms like emails, texts, social media posts, and robocalls, for impersonation schemes. [11]

It has been observed that between February 2020 and March 2020, the number of phishing email attacks using the COVID-19 as lure grew by 667%. These recent occurrences show that phishing attacks continue to pose a serious concern, and more research is needed to reduce that threat. Due to the obvious absence of publicly accessible phishing email datasets and the fact that over 70% of the articles using outdated datasets, phishing email detection research is severely constrained.

- *Fake Websites, Domains, Themes, and Mobile Apps*

The pandemic resulted to a construction of more than 4000 domains associated with coronavirus being operational by the end of January 2020. Out of these domains 3% were asserted as malicious and another 5% were found as suspicious. Actually, the urge to be up-to-date with every new outcome of the pandemic and to gain knowledge upon this new virus, could easily lead a user to click on a malicious domain. The plethora of replicating domains and the uncertainty of the user who didn't knew which information was trustworthy, made the user a potential victim. [12]

- *Secure Communication Channels*

Zoom was the most notable example, which first received acclaim and praises in the early days of home working and lockdown, but quickly became the object of severe criticism after security vulnerabilities began to emerge. Although modifications were rapidly made available, it is easy to foresee some users continuing to use Zoom without updating it, as is the fact with many software on self-managed systems. [9] Effective and secure digital communication channels are required since the remote workforce has to carry out their tasks in a consistent, accurate, and safe manner. Organizations must have security standards in place, in order to effectively interact with their workforce and moreover to monitor these channels for security related vulnerabilities.

- *Information Security Governance*

Organizations handle a great amount of information, thus needing to maintain an optimal level of integrity, confidentiality and availability of these information. Information security takes the lead to protect. [14] Unsecured information system protocols and inadequate data management procedures contribute to cybersecurity vulnerabilities. [12] Organizations must disclose information in line with legal and regulatory authorities, as well as digital regulations, because data may be crucial when it comes to business, industry, and personal life. Moreover, it is of great importance the enforcement of relevant legislation upon the people of the organization.

- *High-tech crimes*

This software that is able to gain control over a computer and manipulate information or even damage data, include ransomware, scareware, adware, trojans, worms, spyware, file infectors etc. Especially ransomware can put an organization in most risk as the cybercriminal creates a situation where the host is locked out of the system and all the information are kept encrypted for ransom. Either by an email attachment, a link or even if the user's credentials were already compromised, the social engineer (hacker) is able to infect the system and offer you a chance to pay a ransom or else the data will be kept for their personal use. It is often that many of them offer their ransomware-as-a-service on the dark web. [10]

In February 2020, it was first observed a new ransomware tool named "CoronaVirus". This tool was spread via a fake Wise Cleaner (system optimization software) website, where the netizens were lured to download the fake setup file. Once someone installed the file, it encrypted every file and created a text file containing the payment instructions. [10] RAT, AZORult, Emotet, KPOT, Nanocore, and Sphinx were the most commonly used across the trojan family during the Covid-19 Pandemic. Emotet was mostly utilized for banking and financial cyber-attacks. Meanwhile, the ransomware family that includes Netwalker, MAZE, Stealer, Maillot, Covid-lock, Dopper-paymer, and Agent Tesla were frequently utilized as a threat for demanding money and financial benefit. Loki-Bots were widely used, while Spider, Remcos, and Info-Stealer were often used for cyber-attacks/threats throughout the pandemic. [11]

Most at risk organizations and industries in terms of cyber-attack

1) *Healthcare organizations*

Due to their inadequate security systems, but mostly because of the value of their data, hospitals and the healthcare industry are the top targets. Many attacks upon critical infrastructures have been reported, including the troubling incident on March 12th 2020, where an attack on the Brno University Hospital at Czech Republic forced the entire IT network to shut down, impacting also two of the hospital's other branches, the Children's Hospital and the Maternity Hospital. [5] Ransomware attacks were also conducted over hospitals, medical centers and public institutions by cybercriminals, since they are overwhelmed with the health crisis and cannot afford to be locked out of their systems, the criminals believe they are likely to pay the ransom. An example of this threat-to-life crime is the one of 14 May 2021, where the Health Service Executive (HSE), which provides all of Ireland's public health services was subjected to a serious cyber-attack, through the criminal infiltration of their IT systems using Conti ransomware. The HSE engaged its Critical Incident Process and switched off all HSE IT systems, disconnecting the National Healthcare Network (NHN) from the internet. The attackers demanded ransom in order for the organization to gain back the access in their data, which were encrypted. The efforts to recover over this incident continued for over four months. The attack came to an ease for the cybercriminal due to the low level of cybersecurity maturity. [7]

It is a fact that many healthcare organizations still operate outdated software or no longer supported operating system (OS) like Windows 7 or Windows XP to control medical devices throughout the hospitals. According to Europol healthcare facilities are an accessible and profitable target for ransomware. Nowadays, computers and the Internet of Things (IoT) are utilized heavily in modern hospitals to store and monitor patients' data but even more to control specific medical devices such as an intensive care unit (ICU), ventilators or even cardiac pacemakers. [8] [5]

Other components of the healthcare industry supply chain, such as the medical manufacturers rushing to supply the enormous global demand for COVID-19 critical goods, are also susceptible to attacks, in addition to frontline healthcare services. Intellectual property belonging to research organizations developing novel medications, tests, and vaccinations is increasingly being targeted.[6] Another example of cybersecurity breaches during the pandemic was the theft of information relating to research on a vaccine for Covid-19, by targeting organizations related to the development of the vaccine in Canada, the United States and the United Kingdom. In relation to this it has been reported that the "APT29" also known as Cozy Bear, a cyber espionage group, alleged to be anchored in Russia, was using published exploits for Citrix and VPN (Virtual Private Network) vulnerabilities to target groups involved in COVID-19 vaccine. [9] It is reported that the healthcare sector tops the list of cybercriminals, with a 45% increase of cyberattacks directed at health care worldwide. [14]

Date	*Institution/Country*	*Reported details*
03/13/2020	*Brno University Hospital, Czech Republic*	*Shut down of the IT network that caused postponement of urgent surgeries and compromised emergency medical care (https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/).*
03/13/2020	*World Health Organization (WHO)*	*Creation of a malicious site mimicking the WHO internal email system which aimed to steal employee passwords (https://tech.newstatesman.com/security/who-cyber-attack-covid19).*
03/14/2020	*Hammersmith Medicines Research Group, UK (COVID-19 Vaccine Trial Group)*	*Ransomware attack resulting in the publication of personal details of former patients, and a failed attempt to disable the network (https://www.computerweekly.com/news/252480425/Cyber-gangsters-hit-UK-medical-research-lorganisation-poised-for-work-on-Coronavirus).*
03/22/2020	*Paris Hospital Authority (AP-HP), France*	*Unspecified attack on AP-HP servers (https://www.bloomberg.com/news/articles/2020-03-23/paris-hospitals-target-of-failed-cyber-attack-authority-says).*
04/04/2020	*UK and Spanish Healthcare Workers*	*Ransomware attack attempting to deactivate anti-virus software (https://www.computing.co.uk/news/4012969/hospitals-coronavirus-ransomware; https://www.digitalhealth.net/2020/04/neither-covid-19-nor-cyber-criminals-care-who-gets-infected-and-suffers/).*
05/13/2020	*UK's ARCHER Academic High-Performance Computing (HPC) network*	*Exploitation of login nodes forcing rewriting on all user passwords (https://www.theregister.com/2020/05/13/uk_archer_supercomputer_cyberattack/).*
06/10/2020	*Babylon Health (Appointment and video-conferencing software for NHS doctors)*	*Data breach due to software error (https://www.mobihealthnews.com/news/europe/babylon-health-admits-gp-hand-app-data-breach-caused-software-issue).*
07/16/2020	*US, UK and Canadian authorities*	*Alleged unspecified state-sponsored cyber-attacks on institutions working on COVID-19 vaccines (https://www.theguardian.com/world/2020/jul/16/russian-state-sponsored-hackers-target-covid-19-vaccine-researchers).*
09/27/2020	*Universal Health Services/USA*	*Ransomware attack-Ryuk attack, (https://doi.org/10.7326/M20-7191)*

2) *Banks and financial institutions*

During the period of February and April of 2020, cyberattacks and threats on financial services reached globally an increase of 238%. While the world was tirelessly fighting Covid-19, cybercriminals took advantage of the vulnerabilities occurred by the pandemic to launch cyberattacks, money laundering and terrorist financing. A wide range of phishing scams were circulated, seemingly send from a trusted source and requesting confidential information. The fact that most of the clients were conducting banking transactions from home, meaning that transactions were often conducted via devices with little or no security protocols, resulted to a high risk of personal information exposure. [12] In the early days of the pandemic, Agari Cyber Intelligence Division reported a Business Email Compromise attack, where the attack was carried out by a cybercrime organization, named "Ancient Tortoise". The intruders took advantage of the situation with Covid-19, targeted the bank accounts to take information about the customers and then send them emails, posing as a legit organization requesting them to change their bank information and payment methods due to the novel coronavirus. Furthermore, in a typical circumstance, fintech users are primarily the victims of social engineering, in which hackers apply particular tactics to pose as a legitimate individual and gain access to personal information such as password recovery. [10]

There are actually more than 1500 high-risk domains, containing both a Covid-19 and financial theme aiming to steal from the unsuspecting user or firm. [12] In 2020, First National Bank, Standard Bank and Nedbank became targets of cyberattacks and had business emails being compromised. In February 2020, Nedbank had more than 1.7 million of their users' accounts being hacked. However, these breaches in their security systems could have resulted in a much more extent damage if not for the sensitivity of cybersecurity systems.

3) Education

Another area that has witnessed significant disruption is education, with most countries closing their educational institutions in the early phases of the epidemic. These facilities retain many information such as personal identification information, academic research, billing information. Academic institutions are also vulnerable to a variety of specific dangers, such as the leaking of sensitive research data or confidential patient trial data. The risk of a cyber-attack is especially high for medical academic institutions working on highly sought-after Covid-19 vaccines or innovative therapies. Many researchers were also caught in the public eye because of their working experience or their work in progress, making them easy targets towards a cyber-attack. [9]

The World Economic Forum in April of 2020, reported that the school environment shifted into a digital education revolution for a total of 1.2 billion of student from 186 countries. [16] School computer systems were targeted by rendering their systems unable to function or by slowing the access. Confidential student information was also at risk of being leaked if the ransom was not paid. A sad example is that of Lincoln College, a private institution dating back in 1865 in rural Illinois. The college struggled with a financial crisis due to a decline in enrollment and their large investments in technology. In December of 2021 a ransomware attack hit the system of the institute by making it unable to access. The college closed in May as it never recovered after the attack. While being the first school to shut down due to a cyber-attack, Lincoln College is only one of over 1,000 other institutions that were affected by ransomware last year. [17]

4) Corporations

Google claims to prevent more than 100 million phishing emails per day, with an accuracy rate of 99.9 percent. As the “work from home” employees increased, it was inevitable that many businesses would become attractive targets. Because of how sudden this situation was, most of the businesses weren’t prepared accordingly. The results of a report back in 2020 claimed that 53% of the participants hadn't receive any security guidelines from their employers regarding the remote work, but also 44.44% of the employees that didn't have any experience

in remote working, stated they no security advice on their new working reality was provided by their employers. [18] This inability to enforce and provide the proper training to the workforce, during a stressful and demanding period, raises concerns about the management procedures of an organization and its security awareness. As a result, it calls into question whether the corporate security officers were aware of the upcoming increase of cybercrime and actually realized the risks at hand in combination with the new employment status.

Prospective Solutions

1) Training and Awareness

The cybersecurity team need to provide an initial level of security awareness for all employees, including the regular change of password or the application of a multi-factor authentication password, the secure sharing of data and information, software updates, cookies and session hijacking, detection of malicious URLs, home-based network and router security. Likewise, the cybersecurity team of an organization plays a key role as to remain focused on the detection of technologies for traffic stream initiating from remote employees. An effective way of learning could be via simulation of a cyber-attack and the way of detecting one, dealing with it and how to recover over time. It is important to teach the employee how to respond in a case of a cyber-attack and build a relationship of reliance between the employee and the cybersecurity team. [11]

2) Artificial Intelligence

Machine learning is based on a model that represents the connection of brain cells. Artificial intelligence applies machine-learning algorithms on data in order to execute statistical analysis, resulting to predictions about behavioral patterns between data. In cybersecurity, these artificial intelligence-tools are able to predict and identify any possible threat/cyber-attack. At present, artificial intelligence systems are applied for traffic pattern and behavioral detection of zero-day cyber-attacks and continue to progress by using self-learning, generating faster and more precise results. [11] An example of a popular algorithm for cybersecurity that can achieve high accuracy levels, is Naïve Bayes. Naïve Bayes applies the Bayes theorem, wherein anomalous activities are assumed to originate from independent events instead of one attack. [19]

3) Big Data and Cyber Resilience

Big Data Analytics reviews vast amounts of data from various past cyberattacks, allowing analysts to assess and detect anomalies in computer systems and networks to protect systems from possible future cyberattacks. By putting into use big data analytics and various correlation algorithms to detect anomalies, combined with strong cybersecurity principles, there can be a big change in cyber resilience. Big data analytics are crucial for gathering all the data concerning previous cyberattacks and threats related to the Covid-19 pandemic in order to predict future incoming cyberthreats. [11]

4) Blockchain and the Internet of Things

Wearable and IoT devices are growing very quickly due to the popularization of cloud services. However, they are found really vulnerable to cyber-attacks, and in need of protection because of their sensitive information and user's personal data. A possible way of protecting these devices is by implementing the concept of blockchain technology. [11] Blockchain is a series of technologies that keeps track of anything of value and record data in blocks, that are connected in chronological ways to form chains. If someone wants to change something in a block this is not possible and instead a new block will be added with the change and its timestamp after inspection of the change by a computers cluster which is not owned by any single person. Trust is distributed among all nodes. Blockchain reminds of a ledger by using a chronological logging method. It is designed to be decentralized and distributed over a large network of many computers worldwide. Researchers have found that the blockchain has several auditing consequences that will fundamentally alter the field. Researchers think that

a proper implementation of the blockchain is also required in a variety of industries, including auditing and accounting, cyber security, and accounting. [19] A prospective of applying this technology in the healthcare IoT could cause a great impact in the reduce of cyber-attacks and the security of data. Blockchain technology is stepping up to overcome security problems in the appearance of current cybersecurity breaches.

Conclusion

A healthcare provider can't help but notice the lyrical parallelism between malware entering a computer network via imitation and the global spread of a virus that uses a ubiquitous respiratory receptor. A malware and a virus have the ability to cross entire continents, taking advantage of our enthusiasm for connection. Both had received numerous warnings from security specialists. Both uncover the problems of a deteriorating infrastructure and a workforce already on the edge of burnout. Both have the potential to kill immediately and create unquantifiable damage through delayed as a result of an omitted treatment, a medical error, and the moral injury of providing inadequate care. Both leave us by feeling powerless. Despite the lockdowns ending, Covid-19 still holds our way of life for ransom. [15]

The cyber-crime and the techniques and tactics are continuing to evolve. Cyber criminals are very opportunistic in terms of how they react to what's happening in the outside world and they will look for any which way possible to gain an access in the inside. It is of high importance to be aware of the external threat as such as the internal threat. As the technology evolves, cyber criminals are also evolving the technology and utilizing it to their advantage. Moreover, specific cyber criminals are organized in essence and well-funded.

The single individual has to change their mindset and the way of operations are being done. In spite of all the technology and monitoring there might be a way for someone to gain access, so assuming that the right question is "What can I do to prevent that movement?". Nowadays, the cyber-security sector has a lot of machine learning capabilities in order to look for anomalous behavior. The objective is reducing the mean time to respond and to recover as quickly as possible, assuming being compromised.

References

1. World Health Organization (WHO). WHO Coronavirus (COVID-19) Dashboard. Retrieved from https://covid19.who.int/.
2. Alawida M, Omolara AE, Abiodun OI, Al-Rajab M. A deeper look into cybersecurity issues in the wake of Covid-19: A survey. Journal of King Saud University - Computer and Information Sciences. 2022 Aug 11. doi: 10.1016/j.jksuci.2022.08.003. Epub ahead of print.
3. IBM. Retrieved from https://www.ibm.com/security/data-breach.
4. De' R, Pandey N, Pal A. Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. Int J Inf Manage. 2020 Dec. doi: 10.1016/j.ijinfomgt.2020.102171.
5. Al-Qahtani AF, Cresci S. The COVID-19 scamdemic: A survey of phishing attacks and their countermeasures during COVID-19. IET Inf Secur. 2022 Jul 4. doi: 10.1049/ise2.12073. Epub ahead of print.
6. Menaka Muthuppalaniappan, LLB, Kerrie Stevenson, MBChB BMedSci (Hons) FHEA, Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health, *International Journal for Quality in Health Care*, Volume 33, Issue 1, 2021, mzaa117, https://doi.org/10.1093/intqhc/mzaa117.
7. Commissioned by the HSE Board in conjunction with the CEO and Executive Management Team (2021). Conti cyber-attack on the HSE. https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf.
8. Pranggono B, Arabo A. COVID-19 pandemic cybersecurity issues. Internet Technology Letters. 2020 Oct 03. doi: https://doi.org/10.1002/itl2.247.

9. Bispham, Mary and Creese, Sadie and Dutton, William H. and Esteve-González, Patricia and Goldsmith, Michael, Cybersecurity in Working from Home: An Exploratory Study (August 1, 2021). TPRC49: The 49th Research Conference on Communication, Information and Internet Policy, Available at SSRN: https://ssrn.com/abstract=3897380 or http://dx.doi.org/10.2139/ssrn.3897380.
10. Khan N. A., Brohi S. N., and Zaman N., "Ten deadly cyber security threats amid COVID-19 pandemic," *TechRxiv*, to be published, doi: 10.36227/techrxiv.12278792.v1.
11. Hijji M, Alam G. A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats During the COVID-19 Pandemic: Challenges and Prospective Solutions. IEEE Access. 2021 Jan 1. doi: 10.1109/ACCESS.2020.3048839. PMID: 34786300; PMCID: PMC8545234.
12. Chigada J, Madzinga R. Cyberattacks and threats during COVID-19: A systematic literature review. South African Journal of Information Management. SAJIM (Online) vol.23 n.1 Cape Town 2021. Doi: http://dx.doi.org/10.4102/sajim.v23i1.1277.
13. Furnell S, Navin Shah J. Home working and cyber security – an outbreak of unpreparedness? Computer Fraud & Security. Volume 2020, Issue 8. 2020. Pages 6-12. ISSN 1361-3723. Doi: https://doi.org/10.1016/S1361-3723(20)30084-1.
14. Mannebäck, E., Padyab, A. Challenges of Managing Information Security during the Pandemic. Challenges 2021, 12, 30. https://doi.org/10.3390/challe12020030.
15. Akselrod H. Crisis Standards of Care: Cyber Attack During a Pandemic. Annals of Internal Medicine. Volume 174, Issue 5. Page: 713-714. 19 Jan 2021. Doi: https://doi.org/10.7326/M20-7191.
16. Venkatesha, S., Reddy, K.R. & Chandavarkar, B.R. Social Engineering Attacks During the COVID-19 Pandemic. *SN COMPUT. SCI.* **2**, 78 (2021). https://doi.org/10.1007/s42979-020-00443-1.
17. Chung C. Lincoln College to Close, Hurt by Pandemic and Ransomware Attack. The New York Times. 9 May 2022. Retrieved from https://www.nytimes.com/2022/05/09/us/lincoln-college-illinois-closure.html.
18. Georgiadou, A., Mouzakitis, S. & Askounis, D. Working from home during COVID-19 crisis: a cyber security culture assessment survey. Secur J 35, 486–505 (2022). https://doi.org/10.1057/s41284-021-00286-2.
19. Kuzlu, M., Fair, C. & Guler, O. Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity. Discov Internet Things 1, 7 (2021). https://doi.org/10.1007/s43926-020-00001-4.