A Study on how the Pandemic Changed the Cybersecurity Landscape

Tiberiu-Marian GEORGESCU
The Bucharest University of Economic Studies
tiberiugeorgescu@ase.ro

This article studies the main changes inflicted by COVID-19 on the cybersecurity field. First, we analyze the main changes in how people used technology during the pandemic compared to before. The changes are classified into two categories: those that take place in the personal life and those specific to the professional environment. Then, the article studies to what extent each of the two categories impacted the cybersecurity domain. The main types of attacks that raised in popularity during the pandemic are discussed, together with causes, consequences, and mitigation strategies. Our work shows that the most important changes in terms of incidents have been related to ransomware, phishing, and remote desktop protocol (RDP) attacks. We studied how COVID-19 restrictions generated the increase in phishing and RDP attacks. Then, to prove that ransomware was also influenced by the pandemic, we had to validate our hypothesis that the increase in both RDP and phishing attacks were the main causes of the intensification of ransomware attacks. We obtained strong correlation indicators which validated our hypothesis. The measures taken by companies are further discussed, whether they are cybersecurity-related companies or specialized in other areas. The paper also studies the evolution of cybersecurity companies' stocks before and after the start of the pandemic. A correlation matrix based on the stock price evolution was performed, which indicates the influence of the pandemic on cybersecurity.

Keywords: *Cybersecurity, COVID-19 Impact, Remote Work, Ransomware, Cybersecurity Stocks*
DOI: 10.24818/issn14531305/25.1.2021.04

1 Introduction

The COVID-19 pandemic had a major impact on all economic sectors. In order to adapt to lockdown measures, people started to use information technology at an increased rate. The growth in technology adoption took place in both personal and professional activities. Due to the restrictions, many people migrated some of their activities from physical to digital environment, in areas such as e-commerce (and m-commerce), communication, and entertainment [1], [2]. Many inexperienced users started to use IT much more often, becoming the ideal target for cyberattacks, such as phishing, impersonation, web-skimming, or credential stuffing. As a result, in 2020 there was a tremendous increase in server-side attacks, focused especially on shopping cart information [3].

Manifold problems have appeared or intensified in the professional environment as well. Most of the organizations had to relocate their activities and allow their employees to work from home. Not only was that a very difficult process, but it was also urgent since the spreading speed of Coronavirus came as a surprise for humankind. While working remotely, people couldn't benefit from the same cybersecurity protection as they had at work. The vast majority of technical reports analyzed in this paper paid close attention to the security breaches due to remote work, such as the use of vulnerable infrastructure or the use of unsecured remote desktop protocol (RDP) connections.

These changes also had an important impact on the web services providers since the web traffic increased significantly overnight. Internet providers faced an overuse of their infrastructure which led to a decrease in speed and even downtimes. Moreover, in the first couple of months after the start of the pandemic, many companies which provided video-conferencing platforms encountered technical problems.

Since everybody was more concerned with

how to adapt in order to continue the daily activity further, less attention was paid to security which created multiple opportunities for the attackers. In the context of the weakening of the companies' cybersecurity, there was a significant increase in incidents. Arguably, the worst consequences have occurred in the rise of ransomware attacks, in terms of the number of successful attacks as well as the ransom that was paid by companies. Other important changes were registered in phishing, supply chain attacks, RDP attacks, data breaches, brute-force, and DDoS attacks [4], [5], [6].

This article focuses on the changes related to cybersecurity in 2020 compared to 2019, especially those caused by the COVID-19 pandemic. Section 2 studies the main differences in how people are using the technology before and after the start of the pandemic and classifies the changes into two categories: personal and professional. Section 3 describes the main cybersecurity threats in 2020 and compares them with those of the previous year. In section 4 we study the main measures taken by companies to ensure the highest level of security. Their solutions are analyzed from the point of view of the companies which are specialized in cybersecurity, as well as those which are not. As expected, most of the new cybersecurity incidents were inflicted by COVID-19, since the pandemic determined changes in how people used information and communication technologies.

We also selected some of the leading cybersecurity companies and analyzed the evolution of their stock prices before and after the start of the pandemic, in order to better understand its impact. Section 5 presents several correlations that illustrate how the changes caused by COVID-19 in the way people use technology influence cybersecurity. The last section concludes the article and discusses new trends in computer security.

2 Main changes caused by the pandemic in the way people use technology

Lockdown measures adoption has significantly increased the technology usage and influenced how it was used. People needed technology for both personal and professional activities. Since 2009 the mobile device usage for internet navigation has been in continuous growth while desktop usage for the same purposes showed a continuous decline. In 2016, the use of mobile devices exceeded the use of desktops in terms of internet traffic. The trend continued until the beginning of 2020. During the Pandemic, from April 1st to December 31, 2020, there has been an increase in desktop usage compared to the same period in 2019, from 45.52% to 45.65%. However, smartphone usage continued to grow, from 50.82% to 51.57%, but tablet device usage decreased significantly from 3.50% to 2.77% [7]. The global increase in desktop usage can be attributed to the COVID pandemic since people changed their usual activities both in personal and professional life.

2.1 Personal Life Changes

E-commerce

The global e-commerce market size has increased by almost 27% in 2020. Figure 1 shows the global e-commerce growth for the last 6 years [8]. The yearly increase rate was declining and in 2020, in the absence of special events, a growth of around 12% was expected. This indicates that the pandemic had a strong impact on e-commerce.

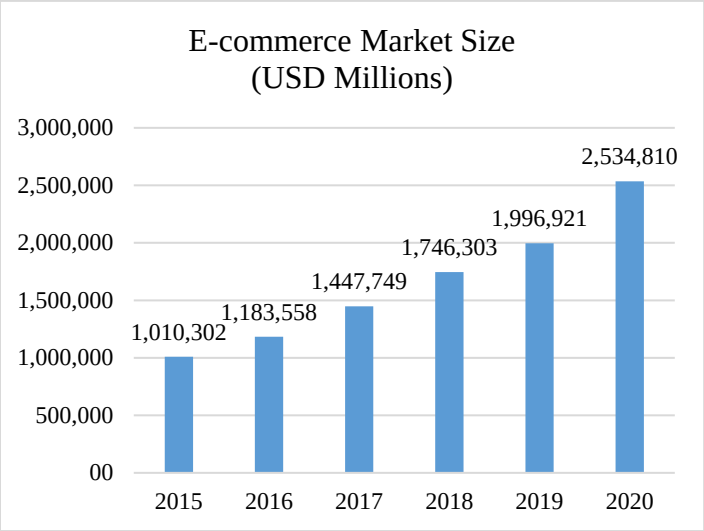

Fig. 1. Global e-commerce annual growth [8]

Communication and social media

Since face-to-face interaction has become less and less possible, people have started to communicate more on social media or video-conference platforms. In the first half of 2020, social media application usage grew by four percent. According to [9], an American is spending on average approximately seven more minutes online than before pandemic, and half of the American adults stated that they were using social media more than they ever did before.

After the start of the pandemic, social media started to be used more for distance learning, healthcare, remote monitoring, and dissemination of information. Alongside many advantages, social media was also massively used for misinformation [10].

The use of video conferencing platforms had an unprecedented increase which can be connected to COVID-19 consequences. The most spectacular growth was registered by Zoom, increasing from approximately 10 million users in December 2019 to over 200 million in March 2020 [11] and more than 300 million in April 2020 [12].

Entertaining

As a form of entertainment, the main changes in digital activities consist in spending more time on social media, watching video-streaming, or playing games.

Between Q2 and Q1 2020, Netflix registered a growth of over 10 million users, compared to only 2.7 million users in the same time frame in 2019 [13]. On Twitch, the number of hours streamed in January 2019 was approximately 41.5 million decreasing to 39.3 million in January 2020 but growing to a record of 88.7 million in January 2021 [14], which can be directly attributed to the lifestyle changes generated by the pandemic measures.

News

Besides the direct medical implications, COVID-19 influenced the population at an emotional level. People have often become impatient and wanted to find out as soon as possible about new information on Covid-19-related topics, such as vaccines, new treatment solutions, or restrictions. Study [15] discusses to what extent COVID-19 influenced how people consume news. In the middle of March 2020, a third of the total time reading news was spent on pandemic-related topics.

Education

During lockdown measures, the educational process was moved to the digital environment relying on e-learning platforms. In addition to e-learning platforms, social media and video conferencing platforms have been widely used in the online educational process. Article [16] states that Google Classroom had already doubled the number of users on April 10, compared to the beginning of March.

2.2 General changes at work

Organizations had to adapt urgently to the restrictions, therefore many technological changes were made to keep the operational processes functional. Some of the most important changes connected to IT are discussed below.

Many inexperienced users started using new technologies

Facing the lockdowns, many companies had to change their operational technology, forcing employees to adapt in a very short amount of time. Many users had to switch to virtual communication and start using various applications, such as video-conferencing ones. Although these types of applications are considered easy-to-use, a lack of experience can be considered an opportunity for attackers.

Working from home

This is arguably the most important change for most companies in 2020. While working from home, employees were deprived of the protection they usually had at the office, such as corporate network, advanced firewall, receptionist, or safety guard to make sure no stranger has access to the intranet, etc. Accordingly, people had to rely on much more vulnerable infrastructure. Some of the organizations adapted fast and provided portable devices to employees, which were configured by IT staff. However, the level of security was much lower for several reasons such as:

a. the short adaptation period suffocated the IT staff, and many of the configurations were not properly done;
b. numerous unsecured RDP connections were created;
c. even when virtual private networks (VPNs) were used, that did not fully ensure the security of the connection, since some of them were misconfigured
d. working from home, people tended to follow less strictly the procedures, rules, and recommendations;
e. vulnerable home Wi-Fi connections were used;
f. the use of personal computers for work.

Many organizations did not afford to buy and configure devices for their employees, therefore they had to work on personal devices. This has generated numerous security issues. First, there was a lack of security restrictions, without which people are more liable to install various applications that may contain malware. Also, there was a lack of proper software protection, such as a professional firewall or antivirus. Not least, a personal computer is more likely to be used by more than only one person in the household [17].

Increase in cloud-based solution usage

Facing lockdown restrictions, many companies chose to migrate from local solutions to cloud-ones. The cloud computing services market had increased by 32% from 2019 to 2020 [18].

The rise in video-conferencing usage

Since the face-to-face meetings were not possible, the video-conference applications came as the only viable solution.

3 Cybersecurity Changes due to COVID-19 Pandemic

The pandemic generated numerous opportunities that black hat hackers were ready to take advantage of. According to [19], during the shift from work at the company to remote work, more than one-third of companies surveyed experienced breaches, and subsequently 60% were experiencing more cybersecurity incidents than before the pandemic.

This section describes the types of cyber incidents which showed the highest increases in the number or/and impact in 2020 compared to previous years. We analyzed the particularities of those events in relation to the changes caused by COVID-19 in both people's personal and professional lives. Table 1 presents the main categories identified. Subsequently, they are discussed one by one.

Table 1. The main types of incidents during the pandemic

		Specificity	
No	**Type of incident**	**Personal life changes**	**Professional environment changes**
1	Ransomware	To a small extent	To a large extent
2	Phishing	To a large extent	To a large extent
3	RDP attacks	No	Yes
4	Brute-force	No	Yes
5	Supply chain attacks	No	Yes
6	Web-skimming	Yes	Insignificant
7	Data exfiltration	To a small extent	To a large extent

3.1 Ransomware

The most significant change in 2020 consisted of the rise of ransomware attacks. There are several reasons behind it, discussed in this section, but the most important seems to be the shift from work at the office to work from home. Personal changes also influenced the ransomware attacks, but to a smaller degree.

The first critical period was during March 2020, when many companies were forced to urgently close their offices and shift their activities to the digital environment. Since their main concerns were at the operational level, for an amount of time security was severely neglected and many black hat hackers found numerous opportunities [20].

Due to the increase in RDP connections, attackers could easily enter a virtual space, which previously was open just for the organization's members. They no longer needed to physically reach the office where the devices were used, but it was enough to compromise the computers used by employees in their homes.

According to [17], people have an increased tendency to use their personal computers (PCs) when working from home. This is bad for several reasons: (1) PC-s usually have two times more infections compared to business devices (11.2% compared to 5.62% in 2020), (2) working home users often use unencrypted online services for sharing files, (3) usually household members share a single admin account, (4) applications, OS and browsers are not updated on PCs as frequently as they are on business devices [17].

Another important cause of ransomware consists of phishing emails. In a study performed by [21], 73% of the small to medium-sized businesses (MSPs) reported phishing e-mails as one of the main causes of ransomware in 2020.

Changes in the mode of operation of the attackers

In the first half of 2020, there was an increase of 72% in new ransomware samples targeting organizations [22]. The study performed by [23] shows that the vast majority of cybersecurity incidents suffered by companies in 2020 involve malware with ransomware (approx. 70%) and only 30% malware without.

The rise of malware in 2020 was massively influenced by COVID-19 changes, but also due to the technical evolution of the attacks. As [17] points out, in the last 12 months the attacks involved methods that are associated with complex targeted attacks, similar to those performed by nation-state actors [24], "in which adversaries employ credential theft and lateral movement methods traditionally associated with targeted attacks such as those from nation-state actors" [24]. According to [25], data exfiltration techniques were very popular lately, doubling from Q2 2020 to Q3 2020.

Those larger attacks can be divided into three phases: (1) the initial infection, (2) the lateral movement, and (3) the ransomware attack. In the second phase, the attackers look for important assets, such as sensitive data. Based on the estimated value of the assets they set a ransom amount. In the last phase, they launch the attack, usually during the weekend or holidays when there is a smaller chance of reactions. Sometimes, there can be one to three weeks between the second and third phase [23] and

this is a crucial time for companies to react and minimize the damages. Article [25] discusses the rentability of paying ransoms after suffering a ransomware attack, as well as the risks of not getting back the assets or/and new possible attacks.

Since ransomware has already been a threat for several years, many companies have developed damage control solutions to recover from ransomware attacks. In the last year, to counterattack the decision of companies that refuse to pay the ransom, cybercriminals very often launched threats to release sensitive data [26]. Compared to a few years ago, now there is not only the risk of losing data, but also other risks such as damaged reputation which may lead to loss of clients, or even fines for violating laws such as GDPR.

To mediate and facilitate communication between victims and attackers, specialized organizations were created. Such actors help the compromised companies to recover their data. Besides negotiating a smaller ransom or better conditions, they also increased the chances of getting back the assets after paying the ransom, since they publish periodical lists about which ransomware organizations respect their agreement and which not [26]. Such agreement violations include re-extortion weeks or months later, threatening to post the same data, data posted although the company has paid, fake files showed as proof of deletion [25].

The most damaging ransomware types in Q3 of 2020 were Sodinokibi, Maze, and Netwalker, totalizing around 40% of the market share [25]. According to [25] the average downtime caused by a successful Ransomware attack was 19 days in Q3 of 2020, three days longer than in Q2 of 2020 [27], and seven days longer than the average downtime in Q3 2019.

3.2 Phishing

Phishing is considered one of the main techniques used to deliver malware. For this reason, phishing is often connected with ransomware. As expected, phishing remained very successful in 2020, since COVID-19 created a series of favorable premises. According to [28] the attackers reacted very quickly to changes, and the phishing attacks involving Coronavirus increased by over 650% in just one month, from February to March 2020. Phishing raised during COVID-19 because of both personal and professional activities changes.

Phishing in e-commerce

Many phishing attacks target card information. In March 2020, just when most of the countries all over the world were implementing lockdown measures, web skimming increased by 26% [29].

Phishing social media/communication

Since people started to spend more time on social media, there has been an increase in social media use for targeted attacks. Technical report [30] assesses this as a serious trend that can reach different domains and generate different types of threats.

Phishing via news

As soon as a significant event happens, attackers are ready to create posts with news about it. In these articles which may appear legitimate, they attach phishing links that can compromise the users' security. The pandemic generated many emotions for people all over the world, which attackers were ready to take advantage of [3].

Companies were largely affected by COVID-19 changes which lead to a significant increase in phishing. Due to the magnitude of the pandemic, many people became nervous when facing the COVID-19 related information. At the beginning of the pandemic, there has been an overwhelming number of COVID-related emails. Besides using emails, "powerful phishing lures include phone scams, smishing, fake invoices, payments, quotations and purchase, and sales orders" [24].

Phishing is often connected to spam tactics, leading inexperienced or unfocused users to a compromised website, from which unnoticed malware is downloaded. The main cause of successful phishing attacks (as well as cyberattacks in general) consists of a lack of

security education amongst employees. Study [31] highlights that "only 3% of penetration tests included social engineering" drawing attention to the fact that organizations do not make sufficient efforts to reduce this risk.

Phishing is usually launched via emails to a huge number of users, from which a relatively small percentage will take the bait. However, in 2020, it was very effective a particular form of phishing, called spear phishing, which is a targeted type of attack where the attackers study carefully the victim before the interaction. Thereby, "the scam appears more authentic, making spear phishing one of the most successful types of attack on enterprises' networks". This was one of the most successful forms of cyberattacks launched against companies lately [32].

Attackers use many social engineering techniques to convince recipients to navigate to malicious websites or to open infected attachments. Usually, spear phishing e-mails contain macro-enabled Microsoft Office files which contain malware. More and more often, business email compromise (BEC) attacks are successful. According to [33] there has been a 15% increase in BECs from Q2 to Q3 2020.

Also, in 2020 has been observed a significant increase in emails with malicious documents attached, usually containing pandemic-related information "seemingly sent from trusted sources – such as the Center of Disease Control and Prevention (CDC) and the World Health Organization (WHO). The operators of the Emotet banking Trojan were among the first to leverage the coronavirus scare to try and distribute their malware this way" [34].

3.3 Remote Desktop Protocol attacks

The Microsoft system of remote controlling machines is mostly used by admins to connect to machines via the network. Unfortunately, due to lockdown measures, more and more RDP connections were left open, allowing attackers to target them. Report [17] states that RDP became in 2020 the favorite method of attackers to deliver ransomware, topping spam campaigns.

Study [17] estimates an increase of 40% in unsecured RDP machines from February to March 2020. Figure 2 illustrates the evolution of brute-force generic RDP attacks in 2020 compared to 2019. As it can be observed, attackers began to be very active just when the lockdown measures started. Also, many compromised RDP connections were sold on Dark Web this year [13].

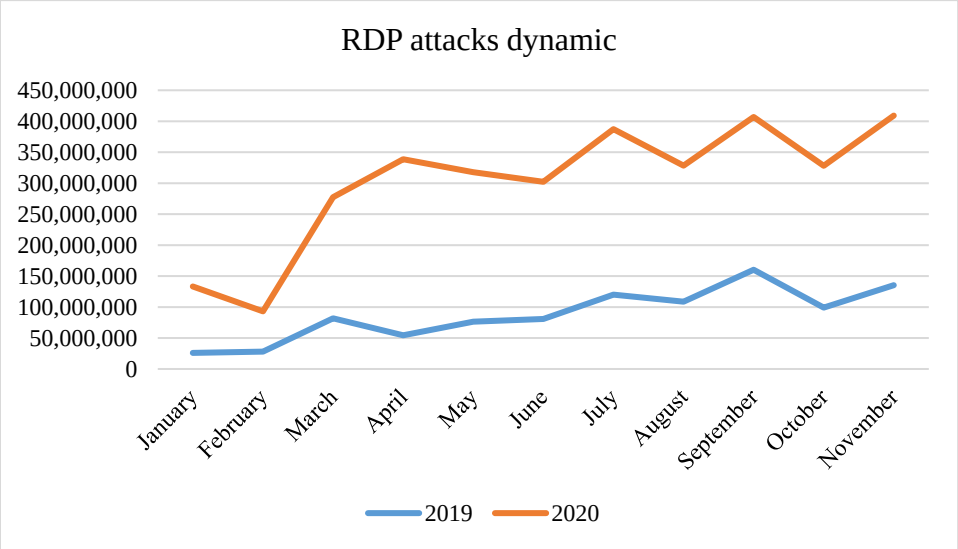

Fig. 2. The number of brute-force generic RDP attacks [35]

Although RDP attacks were already very popular in 2020, report [4] anticipates another growth in 2021 in terms of RDP, VPN, and other remote services exploits.

The good part regarding RDP incidents is that these kinds of problems can be relatively

easily mitigated by using multi-factor authentication and/or by implementing RDP over VPN. However, during COVID-19 the operational process was the priority, and many such security measures were neglected. These measures are not expected to be taken overnight, furthermore [4] states that many attackers consider that although VPNs offer increased security, they are still a potential gateway into an organization's network.

3.4 Brute-force attacks

Forced by circumstances, many organizations migrated their activities to the cloud or used RDP and VPN connections. These changes have generated a significant growth of brute-force attacks, as discussed above.

3.5 Supply chain attacks

This type of attack consists of compromising the security of a target, by penetrating a third-party software package that interacts with the victim. It was very popular in 2020 since over 60% of attacks are traced to third parties. The most targeted type of software was the open source, where it was registered an increase of approximately 430% attacks [4].

The attacker's interest in supply chain attacks resides in the fact that any vulnerability/breach found in a third-party is a potential breach to all other software that uses that third-party.

The most popular supply chain attack in 2020 was by far the SolarWinds hack. By managing to push malware in an update package of the Orion software, over 18000 SolarWinds customers were affected, including US agencies, as well as big tech companies such as Microsoft or Intel [4].

3.6 Web Skimming

Web skimming, also known as card skimming, refers to internet or carding fraud which involves stealing payment information. The attack usually happens on a payment page of a compromised website. The malware is usually injected into the website via a compromised third-party.

The rise of e-commerce during the pandemic quickly attracted the interest of villains for two reasons: (1) there has been an increase in the number of new e-commerce users during lockdowns, who are generally very poorly trained in terms of security and (2) the current users have started using e-commerce more often. In March 2020 has been an increase of over 25% in online credit card skimming in the context of the massive growth of e-commerce [36].

3.7 Data exfiltration

Data exfiltration consists of one or more unauthorized data transfers. Some of the most common causes for data exfiltration include outbound email, downloads to unsecured devices, uploads to external devices, or non-secured behavior in the cloud [37].

Due to the increase in various types of successful attacks in 2020 such as phishing, RDP attacks, credential theft, brute-force, or DDOS, numerous cases of data leakage have been registered lately. Some of the stolen data has been available to be purchased on Dark Web.

A major interest in 2020 was related to healthcare data, with a 25% increase in the number of data breaches of 500 or more records compared to the previous year in the US. However, significant growth was registered from 2018 to 2019 as well [38], from which we can deduce that the attackers' increased interest in healthcare data cannot be attributed solely to the pandemic, but most likely to the regulations related to the protection of personal data adopted in the last several years, which involved increased sanctions.

In 2020 compared to 2019, there has been a decrease of approximately 30% in the number of data breaches in the US, as well as the number of individuals impacted [39]. Also, according to [40] there has been a decrease in the average total costs caused by data breaches in 2020 compared to 2019 in the USA.

It is very interesting that despite the overall growth in the number of cybersecurity incidents during pandemic we have a decrease in terms of data breaches. This can be attributed to several reasons such as (1) many companies switched to cloud solutions which increased data security, (2) authorities were milder with

penalties in the context of the pandemic. As the fines were lower, the attackers were no longer as motivated in data exfiltration as before, because the rewards they could claim would have been reduced.

In the last several years, companies have been obliged to take many measures to protect their clients' data through legislative measures such as GDPR. However, [31] points out that during pandemic many companies violated standards and regulations most of the time unintentionally to urgently implement remote work. "Throughout 2020, Supervisory Authority/ Regulatory activity was light" compared to normal standards and the number of fines remained very low [31].

4 Cybersecurity Measures taken by Companies

Due to COVID-19, worldwide companies were suddenly and severely affected and needed to quickly adapt. The main concern was the operational level, which had to be restored on very short notice, and at the beginning of the pandemic, companies had a short time to pay due attention to cybersecurity. Therefore, the first couple of months after the global lockdowns started were the most difficult. According to the study [41], half of the companies have registered an increase in terms of alerts after the start of the pandemic. The average rise in alerts for these companies was 34.2%. Facing such difficulties, companies had to react, below are discussed the main changes.

The increase of the cybersecurity budget

Until the end of 2020, according to [23] companies increased their cybersecurity budgets by 39%, planning to continue to increase spending in the future. Also, compared to 2019, twice as many companies responded to cybersecurity incidents by increasing the security, either by adding more software solutions or by investing in the training of employees.

Report [19] conducted a survey on big companies in the middle of 2020 and found that most companies were planning to make major investments to secure remote work. 92% of the respondents were expecting an increase in the budget of remote work technologies, and around 60% were planning to invest over 250.000 USD in the next 2 years for investments. 75% of the participants consider investing in cloud security, VPNs, or network access control technologies. Other investments considered were IT personnel (50%), endpoint detection and response (48%), and business continuity plan (48%).

The migration to cloud solutions

According to [31], in 2020 it has been a drop in terms of outdated software as the main critical vulnerability identified in penetration tests. In 2018 and 2019, 50% of the penetration test reports identified outdated software as a critical flaw, but in 2020 it decreased to 32%. The possible explanation consists of the mass adoption of cloud solution services, where the provider maintains the components up to date [31].

It is expected that more and more companies will migrate to the cloud, many companies becoming entirely cloud-based. This tendency will have a massive impact on the cybersecurity landscape. The attackers will try different strategies and cybersecurity experts will need to adapt. As an example, the penetration testing process will meet new limitations on what can and what cannot be tested [31].

Companies paid more ransom than before

In 2020, ransomware generated substantial losses for companies. According to [42], the global average cost necessary to remedy a successful ransomware attack performed on a corporation was 761.106 USD. Considering the financial potential losses, more than 6% of the companies chose to pay the ransom in 2020 [23], since for the large companies the average downtime cost is 24 times higher than the cost of ransom [21].

Besides direct financial losses, ransomware can also imply other types of losses such as a decrease in business productivity, important data losses, damaged reputation, loss of customers, payment of fines, or other types of compensation.

Best practices for companies in 2020

Several papers discuss the best solutions taken by companies to ensure an optimal level of security [43], [44], [45]. Report [46] surveyed over 4800 cybersecurity specialists and identified the main characteristics specific to companies that have managed COVID well in terms of cybersecurity:

(1) They had good procedures and maintained adequate security staffing levels. Moreover, they invested in training their people focusing on role-based scenarios.
(2) Kept a proactive tech strategy by maintaining their systems up-to-date and by using high-quality information technology.
(3) Invested in security technologies.
(4) They had transparent and efficient communication with superiors "through a clear reporting on the activities and effectiveness of the security program" [46].

Other important best practices include securing remote access, increase attention in the protection of core information system security and availability, including cybersecurity as a key part of business, "refactoring security program priorities, architectures, and budgets", "aligning with business leadership" [29].

Study [47] identifies the key priorities for investing: perimeter security, best-of-breed identity and access controls, securing remote access, automation of the routine tasks, security training, better security for trusted third parties.

Technical report [48] identifies the essential cyber hygiene practices for working from home: the use of antivirus protection, improve cybersecurity and phishing awareness, the use of home network security, the use of a VPN, identifying weak spots, frequent reviews taken by companies to evaluate cybersecurity risk, renew business continuity and crisis plans. Other more advanced measures identified include applying new technologies and tools, using intelligence techniques, having good risk management, perform frequent cyber crisis simulation exercises to be prepared for attacks, implement zero trust strategy, where only "authenticated and authorized users and devices are permitted access to applications and data" [48]**.**

The evolution of cybersecurity companies during COVID-19

Technical report [31] states that in 2020 SecOps teams had too many alerts to process, which led employees to fatigue and even burnout. This indicates that the demand in the cybersecurity labor market is still much higher than the offer. Also, they point out an increasing tendency "of homogenization in underlying web technologies, which presents often-overlooked risks to a business" [31].

A key direction for cybersecurity companies discussed in [17] was to get more involved in the security of the third parties with which their client's software interacts. Besides the intrinsic motivation of improving the clients' security, there is also a business reasoning, since often an incident caused by a third-party breach is put into the account of the cybersecurity company.

Top cybersecurity stocks evolution

Although the pandemic has been a global tragedy, from the point of view of cybersecurity, there were also positive aspects. Many organizations understood the importance of cybersecurity and increased the budgets allocated for it. This led to a significant increase of the cybersecurity market. We selected some of the most important players in the field and compared the stock price evolution before and after COVID-19. We gathered the daily closing price from January 2018 to February 2020 from [49].

Table 2 illustrates the companies' stock price variation from February 2020 compared to February 2019, respectively February 2021 compared to February 2020. We chose February as the month of reference since February 2020 is the last month in which companies have not been heavily affected by the global restrictions.

Table 2. Cybersecurity companies' stock price evolution [49]

No.	Company name	Feb 2019-2020	Feb 2020-2021	Variation	Description
1	Palo Alto Networks	2.26%	39.09%	↗	Threat detection & prevention
2	Fortinet	37.78%	29.39%	↘	Security solutions
3	Splunk	23.55%	0.83%	↘	Big data security
4	Check Point Software	-4.10%	3.95%	↗	Unified threat management
5	Proofpoint	4.04%	6.25%	↗	Security-as-a-Service
6	Cloudflare	N/A	77.03%	-	Web performance and security
7	NortonLifeLock	-14.24%	6.92%	↗	Endpoint, cloud & mobile security
8	CrowdStrike	N/A	72.50%	-	Cloud delivered endpoint protection
9	FireEye	-10.68%	26.41%	↗	Advanced threat protection
10	Zscaler	-2.91%	35.64%	↗	Cloud security
11	Cisco Systems	-5.59%	0.83%	↗	Networking, and cybersecurity solutions
12	SecureWorks	-30.03%	-0.08%	↗	Managed security services
13	Vmware	-7.51%	-6.43%	↗	Cloud computing and virtualization software and services
14	SolarWinds	0.90%	-13.52%	↗	IT management software & monitoring tools
15	Okta	58.72%	52.36%	↘	Identity and access management

As it can be observed, out of the 15 companies studied, there is no data for two of them in the 2019–2020 timeframe: CloudFlare and Crowdstrike. However, their stock price evolution from February 2020 to February 2021 is over 70%, which can be considered a massive increase. Out of the remaining 13 companies, nine registered a bigger increase in 2020-2021 compared to 2019-2020. It is worth mentioning that SolarWinds Corporations' decrease can be attributed to the important security issues in the second part of 2020. On the other hand, although Okta and Fortinet's growth variation decreased, they are still on a very good trend in February 2020-2021 timeframe (29.39% and 52.36% respectively). It remains to be analyzed the reasons why Splunk did not maintain the same positive trend. Table 3 illustrates the monthly average stock values for the selected companies and table 4 shows the correlation matrix.

Table 3. The monthly average stock value from February 2020 to February 2021 in USD Dollars [49]

	Months												
Companies	**Feb-20**	**Mar-20**	**Apr-20**	**May-20**	**Jun-20**	**Jul-20**	**Aug-20**	**Sep-20**	**Oct-20**	**Nov-20**	**Dec-20**	**Jan-21**	**Feb-21**
Cloud Flare	19.06	21.22	23.78	27.37	32.41	37.85	39.66	37.36	52.31	64.15	80.11	78.82	83.00
Crowdstrike	62.22	49.52	63.81	77.26	98.51	107.05	109.60	133.41	140.13	138.32	187.56	218.39	226.29
Okta	132.56	118.26	139.99	176.09	192.46	210.25	209.42	205.64	229.79	225.90	256.30	255.89	278.23
Palo Alto	233.04	159.92	184.48	219.32	229.88	243.89	261.57	243.59	242.60	267.51	329.68	359.20	382.62

Zscaler	890.03	872.15	849.32	843.38	868.78	893.48	903.79	996.30	1,053.97	1,144.75	1,209.38	1,370.78	1,382.80
Fortinet	114.86	92.33	105.93	133.16	137.30	136.43	132.15	118.48	124.55	116.90	136.82	147.36	162.66
FireEye	15.31	11.30	10.64	11.44	12.65	13.08	15.00	13.01	13.72	14.74	17.70	22.20	20.80
Norton Life Lock	19.54	17.99	19.80	20.81	20.48	20.40	22.94	21.66	20.90	19.50	20.11	20.87	21.00
Proof Point	122.91	104.24	114.95	117.28	110.83	118.40	110.02	105.62	106.97	98.80	122.11	135.06	131.11
Check Point	113.88	95.02	103.91	106.06	107.79	119.55	125.89	120.66	122.15	118.71	125.40	129.60	118.55
Splunk	164.17	124.08	126.48	159.36	187.34	203.23	204.51	189.94	207.03	197.65	169.65	168.65	165.55
Cisco	46.13	38.06	41.52	43.74	46.18	46.48	44.25	39.90	38.66	40.03	44.51	45.04	46.51
SecureWorks	15.32	11.36	11.50	12.02	12.15	12.02	12.27	12.10	11.34	11.16	13.14	14.12	15.31
VMware	152.94	111.33	128.43	136.36	146.96	143.14	141.30	141.62	146.10	141.65	141.73	138.25	143.71
SolarWinds	18.68	15.39	16.20	17.38	18.77	18.17	20.03	19.84	21.23	22.11	19.08	15.62	16.46

Except for CloudFlare, all the companies registered significant losses from February to March 2020, the period that marks the beginning of the global lockdown measures. However, after the stock market crash in March, companies began to quickly recover. Except for FireEye, all companies increased from March to April 2020. The positive trend has continued for most companies until February 2021, the last month analyzed.

A correlation matrix was made based on monthly average stock values, shown in table 4. Subsequent, Table 5 illustrates the frequency of correlation coefficients classified on confidence intervals. The greener a cell is colored, the stronger is the positive correlation, on the contrary, the redder a cell is, the stronger the negative correlation is.

Table 4. Correlation matrix

	Cloud Flare	Crowdstrike	Okta	Palo Alto	Zscaler	Fortinet	FireEye	Norton Life Lock	Proof Point	Check Point	Splunk	Cisco	SecureWorks	Vmware
Crowdstrike	0.96													
Okta	0.92	0.95												
Palo Alto	0.92	0.95	0.89											
Zscaler	0.95	0.95	0.83	0.91										
Fortinet	0.68	0.77	0.82	0.84	0.62									
FireEye	0.84	0.88	0.75	0.95	0.91	0.71								
Norton Life Lock	0.23	0.37	0.51	0.39	0.14	0.57	0.26							
Proof Point	0.44	0.52	0.37	0.67	0.52	0.67	0.72	0.15						
Check Point	0.70	0.75	0.80	0.75	0.62	0.60	0.69	0.64	0.33					
Splunk	0.27	0.31	0.54	0.29	0.12	0.40	0.15	0.61	-0.21	0.69				
Cisco	0.20	0.27	0.29	0.49	0.17	0.71	0.46	0.29	0.73	0.29	0.14			
SecureWorks	0.36	0.45	0.28	0.65	0.50	0.55	0.74	0.12	0.82	0.32	-0.11	0.68		
Vmware	0.26	0.34	0.46	0.45	0.21	0.55	0.35	0.50	0.25	0.62	0.70	0.54	0.44	
SolarWinds	0.09	0.03	0.25	-0.01	-0.06	-0.05	-0.14	0.31	-0.58	0.43	0.79	-0.23	-0.32	0.57

Table 5. Correlation coefficients

	Positive correlation		**Negative correlation**	
	Interval	Count	Interval	Count
	0-1	96	(-1) - 0	9
Very strong	0.8-1	17	(-1) - (-0.8)	0
Strong	0.6-0.8	26	(-0.8) - (-0.6)	0
Moderate	0.4-0.6	20	(-0.6) - (-0.4)	1
Weak	0.2-0.4	23	(-0.4) - (-0.2)	3
Very weak	0-0.2	10	(-0.2) - 0	5

As it can be observed, out of the total 105 correlations, 96 are positive and only 9 are negative. It is worth pointing out that SolarWinds was involved in 6 out of the 9 negative correlations. This is another proof that SolarWinds' decrease can be attributed to the cybersecurity major incident [4] in which they were involved in 2020.

Since most of the companies registered significant increases in the chosen timeframe and 96 out of 105 correlations are positive, we can state that the field of cybersecurity is on a positive trend. Also, the overall variation of cybersecurity companies' stock prices in 2020 was significantly influenced by the pandemic.

5 Correlation between Changes caused by COVID-19 and their Impact on the Cybersecurity Field

The most important difference in terms of attack is the overwhelming increase in ransomware attacks. As discussed, the most successful ways of starting a ransomware attack are usually via phishing, RDP exploits, and social engineering. This section studies if the increase of ransomware can be correlated with phishing, RDP, or both.

Methodology

We gathered data regarding ransomware, RDP attacks, and phishing. The most recent and relevant data found regarding ransomware was the average ransom paid quarterly by companies. It is relevant since the value of ransom is usually set by an attacker in concordance with the magnitude of the damage caused by the attack. Regarding RDP attacks, we gathered the number of brute-force generic attacks per quarter, since this was the main method to compromise RDP connections.

Also, we studied the evolution of the numbers of unique phishing websites and correlated it with the evolution of average ransom.

Our hypothesis is that the increase in both RDP attacks and phishing represented the main cause for the intensification of ransomware attacks.

We studied the quarterly evolution from 2019 Q1 to 2020 Q3. The first correlation made was between the quarterly average ransom paid (shown in figure 3) and the number of brute-force generic RDP attacks (illustrated in figure 4).

The correlation formula used in the study is:

$$(1) \quad r = \frac{\sum(x-\underline{x})(y-\underline{y})}{\sqrt{\sum(x-\underline{x})^2\sum(y-\underline{y})^2}},$$

where r is the correlation coefficient and x and y are the variables analyzed.

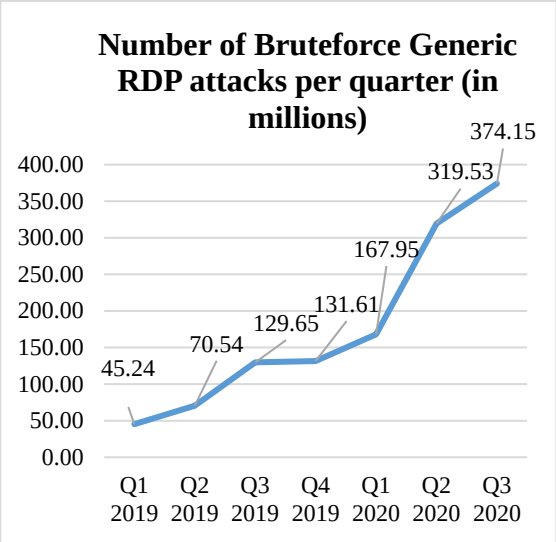

Fig. 3. The dynamic of ransom paid by companies [25]

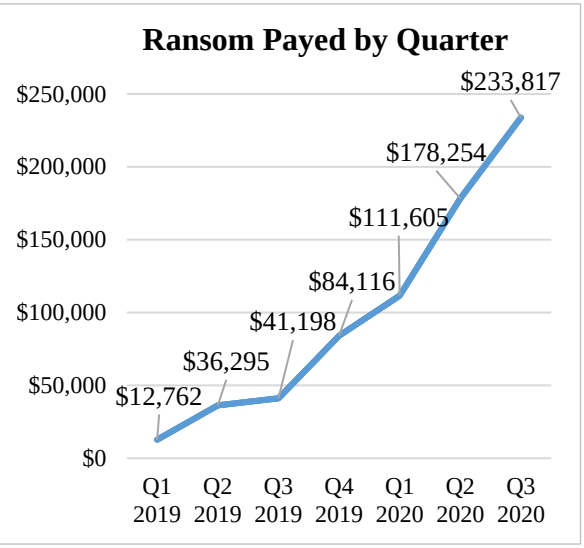

Fig. 4. The dynamic in number of brute-force RDP attacks [35]

Results

To validate our first hypothesis, the value of the correlation coefficient needed to be as close as possible to 1. We applied the correlation formula to the two datasets and obtained an r coefficient equal to 0.9803, which illustrates an almost perfect correlation. This strong positive linear relation indicates that when one dataset increases in its values, the other dataset increases through a very similar linear rule.

Since the number of RDP Brute Force Attacks are mainly caused by the increase of RDP connections and the increase of RDP connections is attributed to the shift to working from distance as a result of COVID-19 lockdowns, we can affirm that the pandemic measures had an important impact on the rise of the ransomware.

Regarding phishing, we collected three relevant datasets: the number of unique phishing websites detected, unique phishing email subjects, and the number of brands targeted by phishing campaigns. Data was gathered from the quarterly reports available at [50].

The quarterly evolution regarding those three datasets is illustrated in figures 5, 6, and 7.

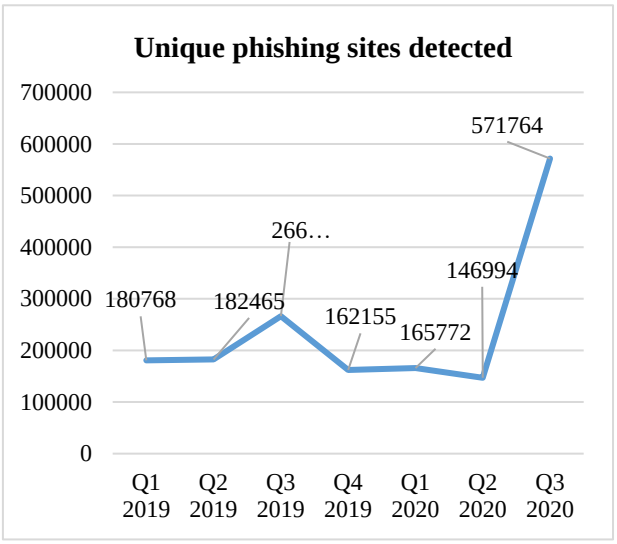

Fig. 5. Unique phishing website [50]

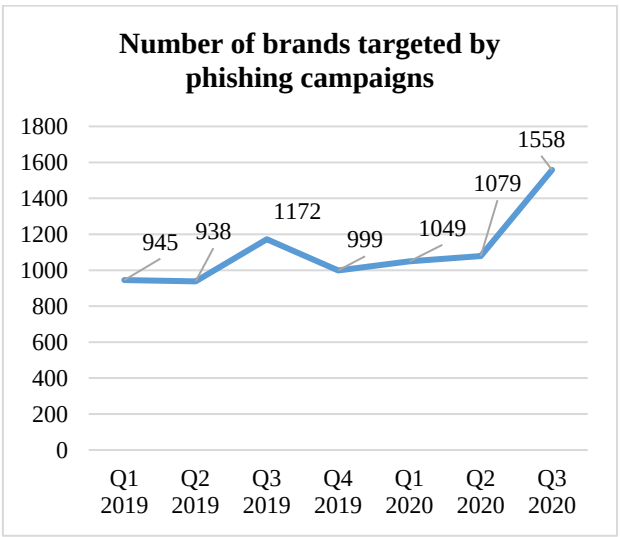

Fig. 6. Number of brands targeted by phishing campaigns [50]

Fig. 7. Unique phishing email subjects [50]

As can be observed, all datasets had a turning point between Q2 and Q3. Table 6 illustrates the correlation coefficients between phishing datasets and the ransom paid by quarter.

Table 6. The correlation coefficients between ransomware and phishing indicators

	Average ransom
Number of unique phishing Web sites detected	0.6065
Unique phishing email subjects	0.7391
Number of brands targeted by phishing campaigns	0.7902

All the selected phishing datasets have a positive correlation with the average ransom paid by companies, which validates our hypothesis.

Limitations

Although we obtained a very strong correlation between ransomware indicators and RDP attacks and strong correlations between ransomware and phishing indicators, there are some limitations in our work. We consider that studying more indicators specific to all three types of attacks and making different analyses could illustrate more clearly to what extent unsecured RDP connections and phishing impacted ransomware.

6 Conclusion and Future Trends

This paper studied the impact of the COVID-19 on cybersecurity. First, the article studied how the pandemic influenced the way humankind used technology. Major changes were identified on both personal and professional levels. Then, we studied the main types of attacks that were preferred by villains before and after the pandemic started. By analyzing several datasets, we noticed significant increases of several types of attacks, such as ransomware, phishing, RDP attacks, or supply chain attacks. The validation of our hypothesis highlighted some of the impacts of the pandemic on the cybersecurity field.

Companies all over the world were affected, therefore important actions were taken, and cybersecurity budgets have been increased. Thus, we studied the companies' measures taken to ensure an adequate cybersecurity level.

This context created both challenges and opportunities for security companies. From a technical point of view, they needed to quickly adapt to very dynamic changes such

as the increase in attacks or company changes. We also explored the stock evolution of some of the main global cybersecurity companies and noticed that most of them had significant increases in shares since the beginning of the pandemic.

Future trends

The very intense period that started after the beginning of the pandemic has had a major impact on the cybersecurity field. Several trends have been identified and we are expecting them to be of great importance in the future.

A worrying aspect is that we are witnessing an increasing process of democratization of cyberattacks. If in the past only a relatively limited number of people were able to arrange such attacks, nowadays there is an important growth in "as a service" attacking solutions such as Malware as a Service, Ransomware as a Service, Phishing of a Service or Botnets as a Service [17]. Also, the sales volume of compromised data on the Black Market has increased and we expect it to continue to grow. It is expected that ransomware and phishing attacks will continue to rise.

Another important trend is connected to the interest of cybersecurity companies to secure third-party software. This trend can be attributed to two main causes: (1) the rise in supply chain attacks and (2) the fact that usually the clients associate incidents caused by third-parties' security issues to their cybersecurity company provider.

Many changes analyzed in this paper are permanent, meaning they will be essential after the pandemic ends as well. "A long-term shift to telework is anticipated" [19]**,** which will lead to the increase of RDP, VPN, and cloud usage.

Cybersecurity companies lacks professionally trained staff and it is expected that this will continue in 2021 since cybersecurity education require a relatively long period of training. According to [6], the main cybersecurity roles in which global companies are interested are related to cloud solutions, security intelligence, data analysis, and data management.

Acknowledgment

This paper presents results obtained within the PN-III-P1-1.2-PCCDI-2017-0272 ATLAS project ("Hub inovativ pentru tehnologii avansate de securitate cibernetică / Innovative Hub for Advanced Cyber Security Technologies"), financed by UEFISCDI through the PN III–"Dezvoltarea sistemului national de cercetare-dezvoltare", PN-III-P1-1.2-PCCDI-2017-1 program.

[1] R. N. Subudhi and P. Debajani, "Impact of Internet Use during COVID Lockdown," Horizon, vol. 2, pp. 59-66, 2020.

[2] F.-V. PANTELIMON, T.-M. GEORGESCU and B.-Ș. POSEDARU, "The Impact of Mobile e-Commerce on GDP: A Comparative Analysis," Informatica Economică, vol. 24, no. 2, 2020.

[3] D. Manky and A. Lakhani, "Evaluating Cyber Threat Landscape Trends in the New Year," 2021. [Online]. Available: https://www.fortinet.com/blog/industry-trends/evaluating-cyber-threat-landscape-trends-in-the-new-year. [Accessed 2021].

[4] CTM360, "The Cyber Forecast - Top 9 Cybersecurity Threats For 2021," 2021. [Online]. Available: https://www.ctm360.com/the-cyber-forecast-top-9-cybersecurity-threats-for-2021. [Accessed 2021].

[5] B. Pranggono and A. Arabo, "COVID-19 pandemic cybersecurity issues," Internet Technology Letters, vol. 4, no. 2, 2020.

[6] PricewaterhouseCoopers, "2021 Global Digital Trust Insights," 2021. [Online]. Available: https://www.pwc.ch/en/publications/2020/ch-Digital-Trust-Insights-Survey-2021-report.pdf. [Accessed 2021].

[7] StatCounter, "Desktop vs Mobile vs Tablet Market Share Worldwide - February 2021," 2021. [Online]. Available: https://gs.statcounter.com/platform-market-share/desktop-mobile-tablet. [Accessed 2021].

[8] Euromonitor International, "E-Commerce in World," 2021. [Online]. Available: https://www.euromonitor.com/. [Accessed 2021].

[9] Broadband Search, "Surprising Social

Media Statistics - The 2021 Edition," 2021. [Online]. Available: https://www.broadbandsearch.net/blog/social-media-facts-statistics#post-navigation-2. [Accessed 2021].

[10] A. Goel and L. Gupta, "Social Media in the Times of COVID-19," Journal of Clinical Rheumatology, 2020.

[11] E. S. Y. (CEO), "A Message to Our Users," 2020. [Online]. Available: https://blog.zoom.us/a-message-to-our-users/. [Accessed 2020].

[12] Zoom Video Communications, "90-Day Security Plan Progress Report: April 22," 2020. [Online]. Available: https://blog.zoom.us/90-day-security-plan-progress-report-april-22/. [Accessed 2020].

[13] Netflix, "Netflix Investors," 2020. [Online]. Available: https://ir.netflix.net/financials/quarterly-earnings/default.aspx. [Accessed 2020].

[14] Twitch Tracker, "Twitch Statistics & Charts," 2021. [Online]. Available: https://twitchtracker.com/statistics. [Accessed 2021].

[15] J. Nicholson, "What happens when coronavirus fatigue sets in? Our traffic and engagement analysis," Chartbeat, 2020. [Online]. Available: https://blog.chartbeat.com/2020/04/08/coronavirus-data-news-traffic-trends/. [Accessed 2021].

[16] G. D. Vynck and M. Bergen, "Google Classroom Users Doubled as Quarantines Spread," Bloomberg, 2020. [Online]. Available: https://www.bloombergquint.com/business/google-widens-lead-in-education-market-as-students-rush-online. [Accessed 2020].

[17] K. Murray, "The Nastiest Malware of 2020 for SMBs," Webroot, 2020. [Online]. Available: https://www.brighttalk.com/webcast/18665/433425. [Accessed 2020].

[18] Canalys, "Global cloud infrastructure market - Q4 2021," 2021. [Online]. Available: https://canalys-com-public-prod.s3.eu-west-2.amazonaws.com/static/press_release/2021/Cloud-pr-Q4-2020.pdf. [Accessed 2021].

[19] Fortinet, "Enterprises Must Adapt to Address Telework Security Challenges - 2020 Remote Workforce Cybersecurity Report," 2020. [Online]. Available: https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/08_Report/report-teleworker-security.pdf.

[20] J. Robertson, "What Does Covid Teach Us About OT Cybersecurity?," 2020. [Online]. Available: https://www.fortinet.com/blog/industry-trends/what-does-covid-teach-us-about-ot-cybersecurity. [Accessed 2020].

[21] Datto Inc, "Datto's ANZ State of the Channel - Ransomware Report," 2019. [Online]. Available: https://www.datto.com/resource-downloads/Datto2019_StateOfTheChannel_RansomwareReport_NL-8.pdf. [Accessed 2020].

[22] Skybox Security, "Tear Up The Cybersecurity Rule Book - Research Report," 2020. [Online]. Available: https://www.skyboxsecurity.com/trends-report/. [Accessed 2020].

[23] Hiscox, "Hiscox Cyber Readiness Report," 2020. [Online]. Available: https://www.hiscox.co.uk/sites/uk/files/documents/2020-06/Hiscox_Cyber_Readiness_Report_2020_UK.PDF. [Accessed 2020].

[24] ENISA - European Union Agency for Cybersecurity, "Main incidents in the EU and worldwide," 2020. [Online]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl-2020-main-incidents-1. [Accessed 2020].

[25] Coveware, "Ransomware Demands continue to rise as Data Exfiltration becomes common, and Maze subdues," 2020. [Online]. Available: https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report. [Accessed 2020].

[26] Fortinet, "Cyber Threat Predictions for

2021," 2021. [Online]. Available: https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-cyber-threat-predictions-for-2021.pdf. [Accessed 2021].

[27] CoveWare, "Ransomware Attacks Fracture Between Enterprise and Ransomware-as-a-Service in Q2 as Demands Increase," 2020. [Online]. Available: https://www.coveware.com/blog/q2-2020-ransomware-marketplace-report. [Accessed 2020].

[28] F. Shi, "Threat Spotlight: Coronavirus-related phishing," 2020. [Online]. Available: https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/. [Accessed 2020].

[29] T. Weil and S. Murugesan, "IT Risk and Resilience—Cybersecurity Response to COVID-19," IT Professional, vol. 22, no. 3, pp. 4-10, 2020.

[30] European Union Agency for Cybersecurity, "ENISA Threat Landscape - The year in review," 2020. [Online]. Available: https://www.enisa.europa.eu/publications/year-in-review. [Accessed 2020].

[31] Bullet Proof, "BulletProof Anual Cybersecurity Report," 2021. [Online]. Available: https://www.bulletproof.co.uk/industry-reports/bulletproof-annual-cyber-security-report-2021. [Accessed 2021].

[32] European Union Agency for Cybersecurity, "Phishing. Enisa Threat Landscape," 2020. [Online]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl2020-phishing. [Accessed 2021].

[33] Abnormal Security, "Abnormal Quarterly BEC Report Q3 2020," 2020. [Online]. Available: https://info.abnormalsecurity.com/Q3-2020-Quarterly-BEC-Report.html. [Accessed 2020].

[34] Fortinet, "Global Threat Landscape Report - A Semiannual Report by FortiGuard Labs," 2020. [Online]. Available: https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-h1-2020.pdf. [Accessed 2020].

[35] Kaspersky, "The story of the year: remote work - Kaspersky Security Bulletin," 2020. [Online]. Available: https://securelist.com/the-story-of-the-year-remote-work/99720/. [Accessed 2020].

[36] J. Segura, "Online credit card skimming increased by 26 percent in March," 2020. [Online]. Available: https://blog.malwarebytes.com/cybercrime/2020/04/online-credit-card-skimming-increases-by-26-in-march/. [Accessed 2020].

[37] Forcepoint, "Cyber Edu: What is Data Exfiltration? Data Exfiltration Defined, Explained, and Explored," [Online]. Available: https://www.forcepoint.com/cyber-edu/data-exfiltration. [Accessed 2021].

[38] Hippa Journal, "Healthcare Data Breach Statistics," 2021. [Online]. Available: https://www.hipaajournal.com/healthcare-data-breach-statistics/. [Accessed 2021].

[39] Identity Theft Resource Center, "ITRC's 2020 Annual Data Breach Report," 2020. [Online]. Available: https://notified.idtheftcenter.org/s/2020-data-breach-report. [Accessed 2020].

[40] International Business Machines Corporation, "IBM Security: Cost of a Data Breach Report," 2020. [Online]. Available: https://www.capita.com/sites/g/files/nginej291/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf. [Accessed 2021].

[41] Cortex by Palo Alto Networks, "The State of SOAR 2020," 2020. [Online]. Available: https://www.paloaltonetworks.com/cortex/xsoar-state-of-soar-report-2020. [Accessed 2020].

[42] Sophos, "The State of Ransomware 2020," 2020. [Online]. Available: https://secure2.sophos.com/en-us/content/state-of-ransomware.aspx. [Accessed 2020].

[43] Deloitte, "COVID-19 People, technology, and the path to organizational resilience," 2020. [Online]. Available:

https://www2.deloitte.com/content/dam/Deloitte/global/Documents/About-Deloitte/Corona-Virus_POV_People%20Technology%20Path_Global_Final%20(002).pdf. [Accessed 2020].

[44] D. Buil-Gil, N. Lord and E. Barrett, "The Dynamics of Business, Cybersecurity and Cyber-victimization: Foregrounding the Internal Guardian in Prevention. Victims & Offenders," Taylor & Francis Online: Victims & Offenders, vol. 16, 2021.

[45] Meghisan-Toma, Georgeta-Madalina and V. C. Nicula., "ICT Security Measures for the Companies within European Union Member States–Perspectives in COVID-19 Context," in Proceedings of the International Conference on Business Excellence 14 (1), Bucharest, 2020.

[46] Cisco, "Security Outcomes Study," 2020. [Online]. Available: https://www.cisco.com/c/en_au/products/security/security-outcomes-study.html. [Accessed 2020].

[47] V. Anant, J. Caso and a. A. Schwarz, "COVID-19 crisis shifts cybersecurity priorities and budgets," 2020. [Online]. Available: https://www.mckinsey.com/business-functions/risk/our-insights/covid-19-crisis-shifts-cybersecurity-priorities-and-budgets. [Accessed 2020].

[48] Deloitte, "Impact of COVID-19 on Cybersecurity," 2020. [Online]. Available: https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html?fbclid=IwAR1gbu6-4Q6_MnWapSVZIMsgnfQDYAU4IS-JJOL-gk_FE9QHY1i4qkuDOGlM. [Accessed 2020].

[49] Nasdaq, "Stocks," 2021. [Online]. Available: https://www.nasdaq.com/market-activity/stocks. [Accessed 2021].

[50] Anti-Phishing Working Group, Inc, "Phishing Activity Trends Reports," 2019-2020. [Online]. Available: https://apwg.org/trendsreports/. [Accessed 2021].

Tiberiu-Marian GEORGESCU graduated from the Faculty of Cybernetics, Statistics and Economic Informatics in 2012. In 2015 he graduated from the Informatics Systems for the Management of Economic Resources Master program. He completed his Ph.D. program in Economic Informatics in September 2019 at the Bucharest University of Economic Studies. Currently, he is working as a Research Assistant in the Department of Economic Informatics and Cybernetics at the Bucharest University of Economic Studies. His main fields of interest are cybersecurity, machine learning, and natural language processing.