NETWORK SECURITY THREATS TO HIGHER EDUCATION INSTITUTIONS

Alexei Arina[1]

DOI: 10.24989/ocg.v341.24

Abstract
The Covid-19 pandemic has significantly changed the way higher education institutions (HEIs) operate around the world. Distance learning has become the unique opportunity that the process further education in conditions where most economic activities were put on hold. To ensure the quality of distance learning have been implemented and used extensively online learning platforms, applications, video conferencing and cloud computing facilities in HEIs. However, this has increased the threats to information security, so that in 2020, in the field of education in general, and HEIs in particular, the number of cyber-attacks has increased, which has led to significant financial losses but also to activity interruption and theft of personal data or intellectual property. In order to identify the biggest threats of the 2020 year, for HEIs, several security reports and scientific articles related to the studied field were analyzed, in order to identify the most common security threats. As a result, of the research conducted, the top Cyber threats of HEIs are: malware attacks, DoS / DDos attacks and phishing attacks. Securing university networks in 2020 was a challenge for specialists in this field.

1. Introduction

The 2020 year has been a real challenge for the whole world. The impact of the pandemic with Covid-19 on the field of Education was strong, the studies that until yesterday, took place in the auditoriums and classes, migrated this year in the virtual classes and online conferences. Higher education institutions are no exception, so the vast majority of institutions have continued to operate online. This decision was made by most institutions around the world to stop the spread of the virus.

The Covid-19 pandemic was a real test for digital educational resources, because no one expected such a big traffic explosion in such a short time.

Thus, modern information technologies have been widely implemented, replacing the classic hours, which until recently took place offline. Technologies such as: video conferencing applications, online learning platforms, websites and Cloud Computing (CC); have been used extensively and, according to the latest research conducted by 2023, the online education market will grow by an average of 16.4% annually [16]. Both students and university staff had to adapt to new conditions to ensure the continuity of education.

Online education has led to a substantial increase in cyber-attacks, in 2020 the education domain had a loss of $ 3.90 million for data breach, according to IBM & Ponemon Institute [14], which conducts cybersecurity research. Referring to another study realized by CheckPoint [3], a leading provider of cyber security solutions to governments and corporations globally and in Europe too,

[1] Technical University of Moldova; 168, Stefan cel Mare Bd., MD-2004, Chisinau, Republic of Moldova;
Email: arina.alexei@tse.utm.md

the average number of weekly cyber-attacks per academic organization in July-August 2020, increased by 24%. In contrast, the overall increase in the number of attacks in all sectors in Europe was only 9%.

The need to configure the new applications, used for distance learning, as optimal as possible in terms of information security, but also to ensure that students' home networks meet minimum security requirements, has become in the new reality a mandatory condition for ensure the availability, confidentiality and integrity of information conveyed.

This article will analyze and expose cybersecurity research data, which will reflect relevant security threats to higher education institutions, based on several 2020 reports submitted by companies such as: IBM & Ponemon Institute, Kaspersky, VMware, CheckPoint, Barracuda, Datanyze, ISO, Jisc; but also scientific articles published in international journals: Procedia Computer Science, Journal of Computer and System Sciences, IEEE Transactions on Professional Communication, Network Security, Computers & Security, etc.

The purpose of the analysis is to demonstrate that cyber security threats in higher education institutions have increased due to online activity, in 2020. The use of online learning platforms, video conferencing applications, centralized storage resources in university networks and intense email communication have created new vectors of attack to gain unauthorized access to the university network.

2. Background

HEIs are targeted by cyber-attacks because of the information they hold. Information that is of interest for attackers are:

- *Intellectual property*, in particular institutions that have conducted studies for the development of a vaccine against Covid-19 or various studies in this field. As with many institutions in the UK, which, according to a study by VMWare, who did research to explore the extent of cyber-attacks and the implementation of the IT security standard within HEIs in UK, at least 25% of universities have suffered intellectual property theft [17].
- *Personal data* of students, including dissertation materials, but also exam results, according to the same study [17], 43% of institutions experienced.
- *Research data* also represents a major vulnerability, about 28% of institutions have such experience.

The new challenges of 2020 are due to the vulnerabilities video conferencing applications and online learning platforms. An increased interest was the availability of network services and access to data, the aim being to interrupt the university activity and block the access to resources of authorized users such as students or employees.

3. Network threats in HEIs

To argue that the distance study had the effect of increasing cyber threats in HEIs in 2020, several security reports provided by world-renowned companies or the Governments of specific countries were analyzed.

According to the report by IBM & Ponemon Institute [14], the main types of compromised registrations in 2020 are personal information (80%), which averaged a loss of $150 per record and intellectual property (32%) with a loss of $ 147 per record. If we analyze the percentage change in the average total cost for compromised data, in Europe, the Scandinavian countries recorded the highest increase (12.8%) in 2020 compared to 2019, followed by the United Kingdom (4.4%). Negative trends are recorded in Germany (-4.7%) and France (-5.2%).

As stated above, these data are specific to HEIs, personal data of students and employees and of course intellectual property, which as reported, were the most targeted data by cyber attackers. Which influenced cyber attackers' interest in HEIs.

Attack vectors are the methods or ways selected by hackers to access a network. The basic attack vectors in HEIs are:

- Compromised credentials are the most common and costly vector of attack, common to other industries, but also to education, which has been identified in 43% of cases in this area in 2020 [17]. The hackers' interest in HEIs is to steal databases containing student credentials, and then provide this data to darknet organizations, or more recently, use it to initiate phishing attacks, which appear to come from within HEIs.
- Cloud misconfiguration has the same weight, especially since a large part of organizations use the cloud intensively in its activity, to minimize equipment and maintenance costs. Using CC, HEIs are able to organize virtual laboratories and simulation environments for the practical activity of students or provide online platforms for study and access to educational resources. But improper CC configuration, increase university network vulnerabilities.
- The vulnerability of third-party software, in 2020, registered a rather significant increase and represents the third attack vector used by hackers. All applications that have been used by HEIs for online study have significant vulnerabilities. If you consider video conferencing applications in Europe, the applications used are shown in table 1, as shown by Datanyze [4], world leader in technography.

Ranking	Technology	Domains	Market Share
1	Zoom	30583	36,15%
2	GoToWebinar	18486	21,85%
3	Cisco Webex	14628	17,29%

Table 1: Use of VCs in Europe

Other vulnerabilities related to third party software are the vulnerabilities of online platforms, widely used by HEIs during the epidemic, for sharing courses content, but also, for online exams. On this segment, leader in Europe, is the platform Moodle (65%), Blackboard (12%), Ilias (4%) and Sakai (3%) [10].

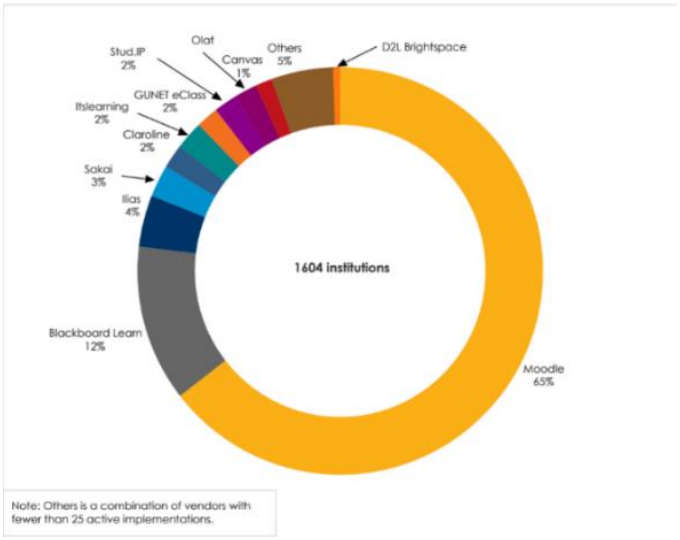

Figure 1: LMSs Distribution Percentage of European HEIs [10]

Learning platforms have several technical and human vulnerabilities, so that the number of vulnerabilities officially discovered and included in the CVE list [11], of the most used learning platforms is more than 400.

In 2020, the number of users who encountered various threats related to online learning platforms and video conferencing applications increased by 20455% [8]. It can be demonstrated by analyzing the data collected in January-June 2019 (left figure) versus January-June 2020 (right figure).

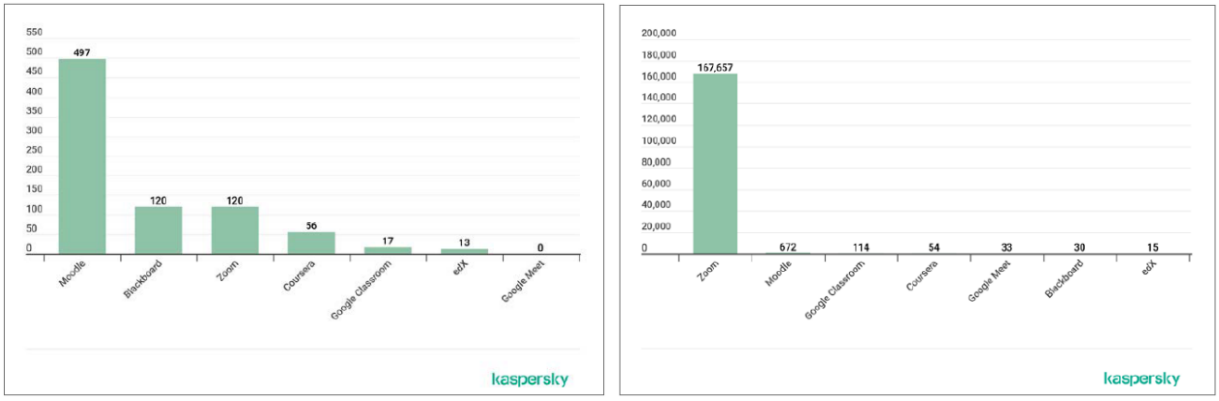

Figure 2: Number of unique users who encountered threats, related to online learning platforms/video conferencing platforms, January-June 2019 versus January-June 2020 [8]

Thus, it can be seen that the number of unique users who encountered threats in 2019 was 820, and in the same period in 2020 it was 168,550. Top 3 most targeted platforms being: Zoom, Moodle and Google Classroom. It can be seen that Zoom was the most vulnerable platform, which can be explained by the popularity of Zoom, which in April 2020, had 300M daily participants in the meeting. The more users download and use the platform, the more interest it has for hackers who want to attack it.

It can therefore be said that the number of cyber threats in HEIs has increased substantially in 2020, due to the distance study that allowed the continuity of the education process in HEIs. The detailed analysis of the threats will allow to identify the risks and to elaborate effective strategies to protect

the university networks and the users. The biggest threats in the education industry have been: malware attacks, denial of service or distributed denial of service (DoS / DDoS) and phishing [8].

3.1. Malware attacks

In June 2020, Microsoft Security Intelligence reported that 61% of the 7.7M malware attacks recorded in the last 30 days, were related to the education domain, more than any other sector of the industry [8]. From the report presented by Jisk [7], a UK company that analyzes the cyber security in educational field, malware infection ranks first in HEIs.

The malware that has targeted educational domain the most in 2020 is ransomware. Since August 2020, the UK Government has identified an impressive increase of ransomware attacks in education [13]. Ransomware is malicious software that allows a hacker to restrict access to authorized users, such as students or university staff, by encrypting disks and then requesting a form of payment to lift the restriction [2].

University networks are open to provide educational services to students, so attackers can exploit this by attacking authorized user and gaining access to the network. Once on the network, ransomware encrypts all drives, limiting legitimate users' access to resources. The administration can only: pay the reward to restore access to the data, restore the backup data, lose the data or break the encryption key using brute force [9]. For the reward, bitcoin payment is most often used because it does not require a financial institution to manage the process. Restoring from backup also presents problems, because most often ransomware programs will search the disks specifically for backups to encrypt them, and if this has been done, respectively, it will not be possible to recover the data. Breaking encryption keys is a difficult process that can take years to break.

Other families of malicious programs are adware and downloaders, due to the fact that students have had to download several applications. Downloaders are malicious programs with the goal to subversively download and install malware (eggs) on a victim’s machine [15]. Adware is software which generally makes pop-up, banner etc. advertisements to appear on the user’s computer [19].

The vectors of malicious attacks [13] are:

- Remote Desktop Protocol (RDP) is a Microsoft proprietary protocol, which provides a graphical user interface for remote access connections over the network. It is one of the most scanned service on the Internet owing to its security importance [6].
- Vulnerable software or hardware is very often used for unauthorized access.
- Phishing emails that contain a malicious link or file that hosts malware.

Famous cases of malware infection in HEIs 2020 are:

- Malicious programs caused the shutdown of European supercomputers working on Covid-19 research in the spring of 2020, and the affected academic institutions were forced to temporarily take their systems offline. Data centers in the UK, Spain, Germany and Switzerland have confirmed the intrusions.
- Newcastle University in England was infected in August 2020 by a ransomware attack that affected almost all IT systems and the network.
- The University of California San Francisco (UCSF), in June 2020, paid $ 1.14 million in Bitcoin to recover data from their medical school.

- The University of Utah paid $ 40,000,000 in August 2020 to unlock its systems IT from ransomware.

Research to identify the Covid-19 vaccine, or related research, has increased the interest of hackers in HEIs in 2020, which has resulted in increased attacks with malicious ransomware programs that have encrypted sensitive information. Another aspect of interest is the access to educational resources, because all university activities went online, the encryption of storage units of university networks had the effect of interrupting the activity. Thus, the attackers obtained access to intellectual property and could manage academic activities.

3.2. DoS/DDoS attacks

In the latest report published by Kaspersky [8], DOS/DDoS attacks have increased, in educational domain, by 350-500% in 2020 compared to the same period in 2019. Denial of Service (DOS) and (DDOS) Distributed Denial of Service attacks have become a major security threat to university campus network security [12].

The substantial increase in DoS / DDoS attacks in HEIs is primarily due to distance learning, as the vast majority of university services, such as: access to the university library, study hours, access to course resources, exams and intermediate assessments, admission to studies; this year have been in the online environment, and disruption of these services shall interrupt academic activity.

This statement is also supported by experts from Kaspersky [8], which states that the increase in DoS / DDoS attacks in the field of education, which can be seen in Figure 3 is due to distance learning.

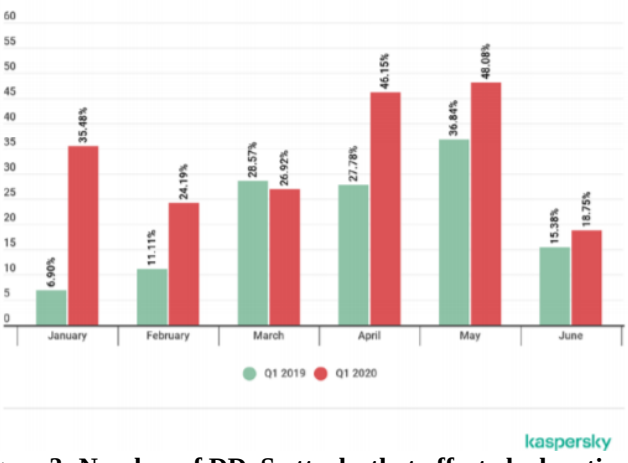

Figure 3: Number of DDoS attacks that affected educational resources in 2020, versus the same period in 2019 [8]

In most scenarios, the targets are:

- *Web servers*, each university has at least one web page, which informs students and employees, it contains personalized information, such as: personal data, academic situation, study schedule. Disruption of access to the page will lead to misinformation authorized users.
- *End devices and network devices*, such as switches and routers. Blocking network devices makes it impossible to access online learning platforms, access to virtual labs or other

university services provided online. In cloud environment also DDoS can reduce the performance of cloud services significantly by damaging the virtual servers [20].

The vectors of DoS / DDoS attacks are:

- The depletion of the bandwidth through flood attacks, that are launched by an attacker sending huge volume of traffic to the victim with the help of zombies that clogs up the victim's network bandwidth with IP traffic [5]. Another attack that uses that vector is the amplification attack, the attacker sends a large number of packets to a broadcast IP address [5].
- Resource depletion that is used to exploit protocols and attacks using malformed packages [5].

Famous cases of DoS / DDoS attacks in HEIs 2020 are:

- In April, a large Turkish university was forced entirely offline for 40 minutes after it was hit with a DDoS attack on the morning of exams [8],
- In June, a major university in the northeastern United States had its exams disrupted after a DDoS attack affected its online test platforms [8].

The purpose of DoS / DDoS attacks within HEIs is to disrupt access to educational resources, especially during time-sensitive activities such as intermediate or final tests. It can therefore be deduced that with the transition to distance learning, DoS / DDoS attacks have increased considerably, the availability of university services being the main target.

3.3. Phishing attacks

The leader of cyber threats in HEIs, is phishing. According to new research conducted by Barracuda Networks [1], HEIs were targeted in June-September 2020 by more than 3.5M phishing attacks, more than 25% of phishing attacks occur in the educational sector. In the UK, according to a Jisc survey, phishing is the biggest threat to corporate network security in HEIs [7].

The most common attack vectors are:

- *Email-based*, where a perpetrator camouflages emails to appear as a legitimate request for personal and sensitive information [18]. For example, emails sent to students, informing them that they have missed or are late to an online course scheduled by teacher. When students accessed the link attached to the email, there was a risk of downloading various malicious programs to personal devices.
- *Video conferencing applications*, that expanded the possibilities for phishing attacks. In the data presented by Check Point Research, between the end of April and the middle of June 2020, approximately 2449 Zoom-related domains were registered, of which 32 were malicious and 320 were suspicious [3].
- *University Online platforms* and *web pages*, that provide false authentication pages for students or staff, to compromise their credentials, such as logins and passwords.

Famous cases of phishing attacks in HEIs 2020 are:

- Louisiana State University (LSU) in the United States, and Oxford, Brighton, and Wolverhampton Universities in the United Kingdom were hit by Shadow Academy, from July to October 2020.

- From June through September 2020, Barracuda researchers evaluated over 3.5 million phishing attacks, including attacks against more than 1,000 educational institutions such as schools, colleges, and universities [1].

The transition to education remotely, when teachers had to communicate with students via email, motivated hackers to make university email accounts a target. Using university platforms for studies and access to educational resources and video conferencing applications to provide online courses have caused also a great interest for cyber attackers, by creating new opportunities to gaining unauthorized access.

4. Recommendations and discussion

Following the analysis carried out in point 3, whose purpose was to identify the biggest threats to HEIs in 2020, it can therefore be said that most cyber-attacks that take place within HEIs refer to the violation of the principles of availability and confidentiality. The purpose of attackers is to disrupt users' access to data and gain control over sensitive data. Sensitive data held by HEIs are in particular the personal data of students and employees and research data.
The basic recommendations, are reflected in Table 2.

Actions	Arguments
Update systems	Software developers develop system updates and security patches to correct vulnerabilities identified in the software usage process. So timely installation of updates will result in more secure and robust systems.
Back Up	Backing up is an important step in not losing access to data and verifying data integrity after an attack. An important factor is to keep backups on off-network storage units to limit their encryption in the event of an attack.
User education	User education refers to both students and employees. This involves constantly informing users about cybersecurity and associated risks. Conducting extensive training and information campaigns within HEIs is a good practice to implement and quite effective, because 90% of attacks within HEIs are based on Social Engineering, it tries to influence authorized users to gain unauthorized access to the information system.
Implementing Defence in depth Model	Implementing the defense-in-depth model involves activating network-level firewalls, intrusion detection systems (IDS), intrusion prevention systems, network-level antivirus. This model allows to approach network security as a multi-level system that is based on the principle that it is more difficult to break a protection system that has several levels than a single level. In addition, an advantage is the extended time that will allow the system administrator to implement security measures until the attacker has escalated all levels.
Inspect network protocols and open ports	The services provided in university networks are quite extensive. Monitoring open ports and the protocols used to provide services will allow administrators to manage with them. Thus, non-essential services can be disabled. Creating a sheet containing information about the basic ports and protocols will allow after the network scan the identification of illegal services and unauthorized open ports. Disabling unused ports, using secure communication protocols, and disabling non-essential services is a good practice to limit unauthorized access to the university network.
Implementing Network Access Control (NAC) system	New devices, such as students', employees' or partners' devices, are often connected to university networks. To ensure that these devices do not bring new vulnerabilities to the university network, it is important to implement the Network Control Access System (NAC). NAC will detect any new devices trying to connect and will allow the connection if the

	devices comply with security policies (updating the system, activating the antivirus and firewall). NAC also allows you to configure user access by roles.
Control administrative access	Monitoring the activity of administrators will also allow to identify illegal actions. The password policy should be strict and passwords should have a limited duration. Also, the administrator account must be linked to a single person, who will not use it for anything else (checking e-mail or browsing the Internet) than for managing and monitoring the system.
Use of corporate emails	The use of corporate emails will allow centralized management, so it will be possible to set strict rules for filtering emails.

Table 2: Recommendations for network security in HEIs

The recommendations proposed above should be applied systematically, HEIs should implement an effective information security management system that will take into account all areas that need to be secured, for the protection of sensitive data.
In order to implement an effective information security management system, it is important to annually identify the real threats facing HEIs, and in this regard, it is advisable for governments to conduct annual studies to identify cybersecurity threats in this domain. The results of the studies will, on the one hand, allow HEIs to identify security risks and prevent cyber-attacks, and on the other hand, for governments, the results of the study will serve as a basis for developing security policies.

5. Conclusion and Future work

Analyzing several international cyber security reports, it was possible to identify the most current cyber security threats in higher education institutions, both globally and in Europe. The personal data of students / employees, intellectual property and research results are of increased interest from cyber attackers.

Thus, malware attacks, DoS / DDoS attacks and phishing attacks have been identified as the most used. The interest of the attackers towards HEIs, in 2020, due to the online university activity only increased.

To ensure data protection, a number of actions have been recommended aimed at limiting unauthorized access to the university network and monitoring it to detect illegal attempts in real time.

It is necessary to implement complex systems to ensure data security in HEIs. In this sense, in the future, it is necessary to identify through research, an information security management system dedicated to HEIs, by analyzing international security standards such as ISO 27000, COBIT, NIST, to promote an efficient and cost-effective security framework**.**

6. References

[1] BARRACUDA, Threat Spotlight Spear Phishing Education, available at: https://lp.barracuda.com/rs/326-BKC-432/images/BEU-AMER-Spear-Phishing-Vol5-2020L.pdf, accessed: December 12, 2020.

[2] BREWER, R., Ransomware attacks: detection, prevention and cure, in: *Network Security*, 2016(9).

[3] CHECK POINT RESEARCH, Cyber Security Report, available at: https://www.checkpoint .com/downloads/resources/cyber-security-report-2020.pdf, accessed: December 19, 2020.

[4] DATANYZE, MARKET SHARE: Web Conferencing, available at: https://www.datanyze. com/market-share/web-conferencing--52/Datanyze%20Universe, accessed: December 5, 2020.

[5] DESHMUKH, R.V. and DEVADKAR, K. K., Understanding DDoS Attack & its Effect in Cloud Environment, in Procedia Computer Science, 202–8p. 49. 2015.

[6] DURUMERIC, Z., BAILEY, M. and HALDERMAN, J. A., An internet-wide view of internet- wide scanning, in: USE NIX Security Symposium, pp. 65–78. 2014.

[7] JISC, Cyber Impact Report, available at: https://repository.jisc.ac.uk/8165/1/cyber-impact-report.pdf, accessed: December 9, 2020.

[8] KASPERSKY, Education Report, available at: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2020/09/04113558/education_report_04092020_2.pdf, accessed: December 9, 2020.

[9] MAURYA, A. K., KUMAR, N., AGRAWAL, A., and KHAN, R. A., Ransomware Evolution, Target and Safety Measures, in: International Journal of Computer Sciences and Engineering, vol. 6, no. 1, Jan. 2018.

[10] MINDWI res LLC, e-Literate European LMS Market Dynamics, available at: https://www.dropbox.com/s/2wnhrfpooa1kid6/eLiterate%20European%20LMS%20Market% 20 Dynamics%20Fall%202016.pdf?dl=0, accessed: December 3, 2020.

[11] MITRE Corporation, Moodle: Vulnerability Statistics, available at: https://www.cvedetails. com/product/3590/?q=moodle, accessed: December 4, 2020.

[12] NAAGAS, M. A., MIQUE, JR, E. L., PALAOAG, T. D. and DELA CRUZ, J. S., Defense-through-Deception Network Security Model: Securing University Campus Network from DOS/DDOS Attack, in: Bulletin of Electrical Engineering and Informatics, vol. 7, no. 4, Dec. 2018.

[13] NCSC, Alert: Targeted ransomware attacks on the UK education sector by cyber criminals, available at https://www.ncsc.gov.uk/news/alert-targeted-ransomware-attacks-on-uk-educatio n-sector, accessed: December 14, 2020.

[14] PONEMON INSTITUTE and IBM, Cost of a Data Breach Report, available at: https://www.ibm.com/security/digital-assets/cost-data-breach-report, accessed: January 9, 2021.

[15] ROSSOW, C., DIETRICH, C. and BOS, H., Large-Scale Analysis of Malware Downloaders, in: Flegel U., Markatos E., Robertson W. (eds) Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA 2012. Lecture Notes in Computer Science, vol 7591. Springer, Berlin, Heidelberg 2013.

[16] SHAHZAD, A., et al. Effects of COVID-19 in E-learning on higher education institution students: the group comparison between male and female, in: Quality & Quantity. 2020.

[17] VMWare, VMware Cyber Security Report, available at: https://www.qassociates.co.uk/wp-content/uploads/2016/06/36300-VMware-Cyber-Security-Report.pdf, accessed: December 10, 2020.

[18] WANG, J., et al., Research Article Phishing Susceptibility: An Investigation into the Processing of a Targeted Spear Phishing Email, in: IEEE Transactions on Professional Communication, 55(4). 2012.

[19] YILMAZ, SEYHMUS & ZAVRAK and SULTAN, Adware: A Review, in: International Journal of Computer Science and Information Technologies, 6. 2015.

[20] ZLOMISLIĆ, V., FERTALJ, K. and SRUK, V., Denial of service attacks, defenses and research challenges, in: Cluster Computing, 20(1). 2017.