Trap method in ensuring data security

D A Shkirdov[1], E S Sagatov[1] and P S Dmitrenko[2]

[1]Samara National Research University, Moskovskoe Shosse, 34A, Samara, Russia, 443086
[2]V.I. Vernadsky Crimean Federal University, Prospekt Vernadskogo, 4, Simferopol, Russia, 295007

e-mail: sagatov@ya.ru

Abstract. This paper presents the results of data analysis from a geographically distributed honeypot network. Such honeypot servers were deployed in Samara, Rostov on Don, Crimea and the USA two years ago. Methods for processing statistics are discussed in detail for secure remote access SSH. Lists of attacking addresses are highlighted, and their geographical affiliation is determined. Rank distributions were used as the basis for statistical analysis. The intensity of requests to each of the 10 installed services was then calculated.

1. Introduction

Today network and information technologies determine largely both the current standard of living and the possibilities for the future development of society. Unfortunately, modern telecommunications are inseparable from the attempts of intruders to disrupt their stable operation. These attempts have long been undertaken not by individual criminals, but by well-organised groups of hackers. In recent years, accusations of destructive actions are increasingly heard against states.

Under these conditions, the protection of telecommunications and information infrastructure becomes the most important task for both public services and private companies. For the needs of protection, a special infrastructure is created. This paper will focus on creating one of the types of such an infrastructure, known as a network of honeypot servers.

Network attacks can be divided into two large classes [1]:

• Attacks aimed at disabling the telecommunications infrastructure due to the increased load associated with a large number of calls. Overflow can concern both communication channels and the number of requests to a service. These are the so-called denial of service (DoS) attacks.

• Attacks aimed at intercepting telecommunications and information infrastructure management. These attacks are characterised by penetration into the software of the control system with a subsequent acquisition of superuser rights. It should be emphasised that all attempts to take control are carried out exclusively through network requests.

This classification suggests a way to deal with network threats. In order to successfully counter intrusions aimed at denial of service due to the increased load on the network, it is necessary to uncover the sources of the attack and block them.

To combat control interception, it is necessary to create an infrastructure that allows for recording attacking network requests and analysing them. This is necessary to fully understand the mechanism of attack. In turn, attacking requests can come in two forms. The first type is based on the human

factor. This may be the appointment of a simple password for a standard login. The human factor includes a banal betrayal associated with the transfer of information about the features of the protective infrastructure and password system, etc.

Sometimes software failures are used to intercept control, including specially opened backdoors, which are left at the insistence of special services [2]. Attacking requests of this type also need to be studied and classified.

To detect attacking requests, a special approach was proposed known as the honeypot method [3].

A lot of requests are made to the usual resources on the Internet, both legal and malicious. It is simply impossible to recognise attacking requests in the general stream. However, we can make such a resource [4], to which an ordinary user will not be accessed because there will be no content on this server. In addition, this server should not be offered to search engines for scanning. In this case, all requests can be considered suspicious.

After highlighting information about attacking requests and their sources, we can build a defensive infrastructure. First, the most vulnerable network services will be allocated based on data on the number of requests to them. Secondly, the mechanisms and frequency of using any software vulnerabilities that attackers use will become known. Thirdly, databases of attacking addresses will be formed, which will simplify their blocking. Fourthly, it will be possible to carry out active measures to investigate botnets by artificially infecting a honeypot server and tracking the further actions of intruders [5].

Finally, data on the intrusion model will allow for the formulation of relevant rules for conducting an audit of network security [6]. Moreover, these rules will be updated as data is updated from the honeypot servers. Based on the rules for auditing, appropriate software should be developed that could work in local networks and conduct preliminary testing of the most important network resources.

2. Honeypot device and measuring infrastructure

Measuring infrastructure is required for primary data collection. This infrastructure should include geographically dispersed servers. This is necessary to further verify the data and exclude random calls from the general list of attacking requests. The probability of accidental access to two or more geographically separated honeypot [7] servers is extremely small. In addition, installing multiple honeypot servers allows you to increase the database, as attacking requests, and their sources.

Our network of honeypot servers consists of 4 units. Three of them are in the European part of Russia, while one of the servers is installed on a hosting in the USA. When choosing placements, we were guided by the simplicity of the installation process and low-cost hosting. This choice is due to the fact that the data of this study was intended to create protective mechanisms in the Russian segment of the Internet. In addition to coverage, our research also distinguishes a rather long time of collecting statistics, which was more than two years.

The choice of applications installed on the honeypot server was determined by their popularity with users. All honeypot servers have the GNU Debian/Linux operating system installed. A list of protocols, services, associated software, types of attacks, and log files with their location is given in Table 1.

Table 1. Basic parameters of the honeypot server.

№	Network protocol or service	Installed software	Possible attack types	Path to the data file
1	VoIP SIP, Internet telephony	Asterisk	Password selection Incoming call to search for existing number	/var/log/asterisk/messages
2	HTTP, web service	Apache, Nginx	Attempt to find admin panel phpmyadmin, CMS WP, Joomla Attempt to access node	/var/log/nginx/*
3	POP3, IMAP, email	Dovecot, exim	Password selection	/var/log/mail.log

4	MySQL, database management system	MySQL	Password selection	/var/log/MySQL/*
5	SMB, universal service to access network resources	Samba	Password selection	/var/log/Samba/*
6	Proxy, reseller server with redundancy	Squid	Password selection	/var/log/squid3/access.log
7	SSH, secure remote access	OpenSSH	Password selection	/var/log/auth.log
8	FTP, File Transfer Protocol	vsftpd	Password selection	/var/log/vsftpd.log
9	DNS, domain name service	Bind9	DNS vulnerabilities	/var/log/named.log
10	Firewall	iptables	Port scan	/var/log/iptables

Standard ports were used to configure network protocols and services. A list of all active ports open on each of the honeypot servers is given in Table 2. The netstat command was used to output data.

Table 2. List of open ports on a honeypot server.

List of open TCP IPv4 ports on a honeypot server.

```
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN      532/vsftpd
tcp        0      0 91.222.129.204:53       0.0.0.0:*               LISTEN      478/named
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN      478/named
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      480/SSHd
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN      478/named
tcp        0      0 0.0.0.0:58201           0.0.0.0:*               LISTEN      463/rpc.statd
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      1127/smbd
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN      1035/mysqld
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      1127/smbd
tcp        0      0 127.0.0.1:5038          0.0.0.0:*               LISTEN      1422/asterisk
tcp        0      0 0.0.0.0:110             0.0.0.0:*               LISTEN      494/dovecot
tcp        0      0 0.0.0.0:143             0.0.0.0:*               LISTEN      1/init
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      453/rpcbind
tcp        0      0 0.0.0.0:2000            0.0.0.0:*               LISTEN      1422/asterisk
tcp        0      0 0.0.0.0:8080            0.0.0.0:*               LISTEN      660/apache2
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      577/nginx -g daemon
```

List of open TCP IPv6 ports on a honeypot server.

```
tcp6       0      0 :::22                   :::*                    LISTEN      480/SSHd
tcp6       0      0 :::3128                 :::*                    LISTEN      618/(squid-1)
tcp6       0      0 :::57115                :::*                    LISTEN      463/rpc.statd
tcp6       0      0 :::445                  :::*                    LISTEN      1127/smbd
tcp6       0      0 :::139                  :::*                    LISTEN      1127/smbd
tcp6       0      0 :::110                  :::*                    LISTEN      494/dovecot
tcp6       0      0 :::143                  :::*                    LISTEN      1/init
tcp6       0      0 :::111                  :::*                    LISTEN      453/rpcbind
```

List of open UDP IPv4 ports on a honeypot server.

```
udp        0      0 0.0.0.0:4520            0.0.0.0:*                           1422/asterisk
udp        0      0 0.0.0.0:4569            0.0.0.0:*                           1422/asterisk
```

```
udp        0      0 0.0.0.0:16892           0.0.0.0:*                           1422/asterisk
udp        0      0 0.0.0.0:16893           0.0.0.0:*                           1422/asterisk
udp        0      0 0.0.0.0:625             0.0.0.0:*                           453/rpcbind
udp        0      0 127.0.0.1:639           0.0.0.0:*                           463/rpc.statd
udp        0      0 0.0.0.0:5000            0.0.0.0:*                           1422/asterisk
udp        0      0 0.0.0.0:5060            0.0.0.0:*                           1422/asterisk
udp        0      0 0.0.0.0:13254           0.0.0.0:*                           1422/asterisk
udp        0      0 0.0.0.0:13255           0.0.0.0:*                           1422/asterisk
udp        0      0 0.0.0.0:42003           0.0.0.0:*                           618/(squid-1)
udp        0      0 0.0.0.0:12030           0.0.0.0:*                           1422/asterisk
udp        0      0 0.0.0.0:12031           0.0.0.0:*                           1422/asterisk
udp        0      0 0.0.0.0:53099           0.0.0.0:*                           463/rpc.statd
udp        0      0 91.222.129.204:53       0.0.0.0:*                           478/named
udp        0      0 127.0.0.1:53            0.0.0.0:*                           478/named
udp        0      0 0.0.0.0:111             0.0.0.0:*                           453/rpcbind
udp        0      0 0.0.0.0:10368           0.0.0.0:*                           1422/asterisk
udp        0      0 0.0.0.0:10369           0.0.0.0:*                           1422/asterisk
udp        0      0 91.222.129.255:137      0.0.0.0:*                           1104/nmbd
udp        0      0 91.222.129.204:137      0.0.0.0:*                           1104/nmbd
udp        0      0 0.0.0.0:137             0.0.0.0:*                           1104/nmbd
udp        0      0 91.222.129.255:138      0.0.0.0:*                           1104/nmbd
udp        0      0 91.222.129.204:138      0.0.0.0:*                           1104/nmbd
udp        0      0 0.0.0.0:138             0.0.0.0:*                           1104/nmbd
udp        0      0 0.0.0.0:18630           0.0.0.0:*                           1422/asterisk
udp        0      0 0.0.0.0:18631           0.0.0.0:*                           1422/asterisk
udp        0      0 0.0.0.0:10442           0.0.0.0:*                           1422/asterisk
udp        0      0 0.0.0.0:10443           0.0.0.0:*                           1422/asterisk
udp        0      0 0.0.0.0:14582           0.0.0.0:*                           1422/asterisk
udp        0      0 0.0.0.0:14583           0.0.0.0:*                           1422/asterisk
```

List of open UDP IPv6 ports on a honeypot server.

```
udp6       0      0 :::625                  :::*                                453/rpcbind
udp6       0      0 :::38513                :::*                                618/(squid-1)
udp6       0      0 :::111                  :::*                                453/rpcbind
udp6       0      0 :::57514                :::*                                463/rpc.statd
```

3. General statistics on ports

To process the primary data from log files with statistics, special scripts were written that operated with regular expressions and extracted the data we needed.

First, we present the data on traffic by ports, which was obtained by analysing NetFlow data for the month. The data on the most loaded ports, depending on the type of protocols, is summarised in the following Table 3.

It should be noted that Table 3 shows data only for the first 10 ports for each type of protocol. The number of flows in the column shows the number of completed flows that transmitted data on a given port. A stream can be viewed as a single connection between devices with fixed IP addresses and ports.

It should be noted that requests were made to all TCP ports without exception, and the number of requests to the most unpopular port exceeded 10 in one month. Requests on the UDP protocol were fixed only to 16743 ports, and 74.5% of UDP ports were not used.

The collected statistics allow us to rank the popularity of attacks for various types of Internet services, which were discussed in Section 3. Table 4 highlights the top ten of the most popular services for hacking.

Here, Winbox is an application for managing MikroTik RouterOS, and rpcbind is a remote procedure call service.

4. Statistics processing rules on the example of SSH service

In this section, the paper will present the basic data obtained after processing statistics from the honeypot servers. We emphasise once again that the data in this section is based on the log files of the installed services. Log files in turn contain only the response of the service to external requests. In this

section, we attempt to classify threats based on these responses. The full content of the request in most cases remains unknown to us.

Table 3. Data on the number of requests by ports.

№	TCP		UDP		ICMP	
	Port number	Number of flows	Port number	Number of flows	Request type	Number of flows
1	22	284 452	5060	280 161	8.0	23 829
2	80	84 934	137	45 550	3.3	11 989
3	23	43 213	111	4 509	3.10	1 797
4	75	32 984	523	2 397	3.2	1 121
5	3306	32 738	0	2 262	11.0	787
6	8291	32 473	53413	1 400		
7	139	13 504	1900	1 065		
8	21	11 277	123	643		
9	8080	10 798	53	596		
10	111	10 676	11211	406		

Table 4. List of popularity of services.

№	Service type	Ports
1	SSH	22
2	SIP	5060
3	HTTP	80
4	Samba	137, 139
5	Telnet	23
6	MySQL	3306
7	Winbox	8291
8	FTP	21
9	Alternate HTTP	8080, 8088, 8888, 8081, etc
10	rpcbind	111

At the beginning of the section, we will show how data is processed using the SSH server as an example. This is a remote-control service of the operating system, each session of which is protected using encryption, including the transfer of a password for user identification. Data was collected during 2017-2019, with the total period exceeding one year. Information about the size of the collected data is available in Table 5.

Table 5. Sizes of collected data.

Crimea	Rostov on Don	Samara	USA
1.20 Gb	0.46 Gb	1.15 Gb	2.53 Gb

Since the data on the honeypot server was not announced in any way (either through DNS, or registration in a search engine, or in IP telephony, etc.), all requests to the specified IP address can be considered suspicious. More suspicious are calls to the SSH server installed as part of the honeypot.

Attacking requests can be divided into two categories. The first of these should include requests for the selection of a pair: username and password. If the password is the simplest, then there is a chance to get access to the system management via a small search. The second category of attacking requests attempts to exploit the identified vulnerabilities of software implementing the server-side of the SSH protocol. It should be noted that such requests are quite difficult to identify using the analysis of log files, since this one contains only system responses.

Table 6 contains data on the number of unique addresses that sent requests to the honeypot server.

A comparison of the data in Tables 6 and 7 shows that IP addresses are sending requests unevenly. Among them are random devices that send requests by mistake, and they should be removed from the

final blacklist. In order to understand how irregularly the various devices perform requests, we constructed a rank distribution. Using specially written scripts, we will determine how many times n_i requests were sent from one IP address or another during the statistics collection period. Then we arrange these addresses in descending order of the number of requests n_i before enumerating these addresses according to the resulting queue. The dependence of the number of requests n_i on the place in the ordered list i is the rank distribution. Usually it is depicted on a graph with logarithmic axes $\lg(n_i)$ and $\lg(i)$. The resulting graph can be found in Figure 1.

Table 6. The number of IP addresses involved in requests to the SSH server.

	Crimea	Rostov on Don	Samara	USA
Total	15 970	15 527	16 486	15 909

Table 7 contains data on the total number of requests.

Table 7. Number of requests to the SSH server.

	Crimea	Rostov on Don	Samara	USA
Total	10 352 958	3 221 026	9 002 497	21 875 655

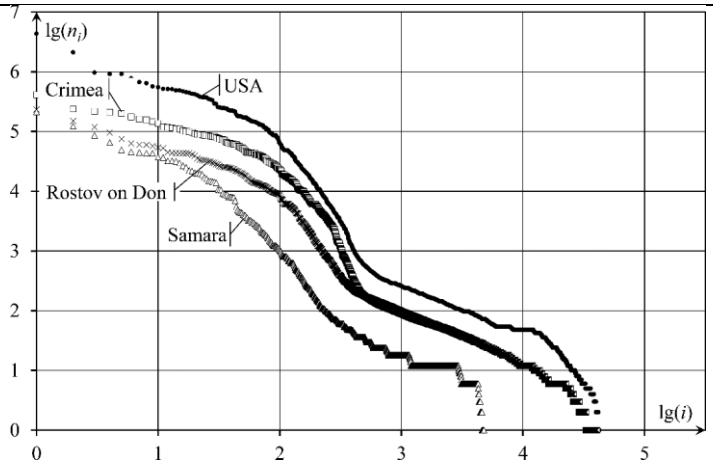

Figure 1. Rank distribution for the number of requests for SSH.

The most active IP addresses managed to send about a million requests to the SSH server. At the same time, a significant part of the addresses turned out once.

The next part of the analysis is devoted to the coincidence of attacking nodes for a geographically distributed network of honeypot servers.

Table 8 shows data on the number of matched IP addresses sending requests to SSH for each pair of honeypot servers.

Table 8. The number of matched IP for two servers.

	Crimea	Rostov on Don	Samara	USA
Crimea	15 970	17%	16%	15%
Rostov on Don	4560	15 527	16%	15%
Samara	4414	4373	16 486	14%
USA	4201	4099	4051	15 909

The total number of unique addresses that sent requests to this honeypot is on the diagonal. The number of matching IP addresses for the two honeypot servers is indicated in the cell below the diagonal. Above the diagonal is the corresponding percentage.

Table 9 shows data on the number of addresses from which requests were sent to three and four traps.

Table 9. The number of matched IP addresses for three or more traps.

Crimea, Rostov on Don, Samara	3 079
Crimea, Rostov on Don, USA	2 874
Crimea, Samara, USA	2 793
Rostov on Don, Samara, USA	2 717
Crimea, Rostov on Don, Samara, USA	2 235

However, the graph from Figure 1 shows that the number of requests from a single IP address can vary greatly. We need to understand how this number is distributed and how many requests are the same for two, three and four honeypots. Table 10 shows the pairwise matching of requests for honeypot servers.

Comparing the data in Tables 8 and 9 shows that matching requests originate from IP addresses from the top of the rank distribution. That is, the same attacking servers make the selection of the password, while the addresses from the tail of the rank distribution most likely accessed only one honeypot server, and only then by chance.

Table 10. The number of matching requests.

	Crimea	Rostov on Don	Samara	USA
Crimea	10 352 958	61%	56%	40%
Rostov on Don	8 277 703	3 221 026	57%	38%
Samara	10 856 564	6 978 442	9 002 497	46%
USA	13 021 228	9 485 649	14 235 002	21 875 655

Table 11 contains data on the number of matching requests for 3 and 4 honeypot servers. The greatest correlation between attacking requests is observed on Russian honeypots.

Table 11. Matching requests for 3 and 4 honeypot servers.

	Request number	The ratio of the total number of requests
Crimea, Rostov on Don, Samara	11 854 523	53%
Crimea, Rostov on Don, USA	13 383 641	38%
Crimea, Samara, USA	15 314 147	37%
Rostov on Don, Samara, USA	12 295 278	36%
Crimea, Rostov on Don, Samara, USA	15 832 904	36%

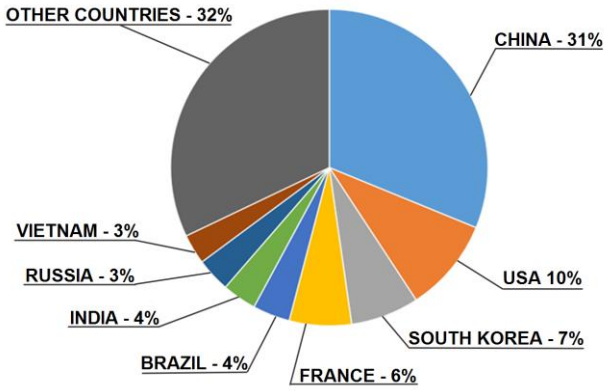

Figure 2. Distribution of IP Addresses by Country.

In conclusion, we would like to discuss the question of the criteria for including an address in the blacklist of attacking addresses. Based on these criteria, a blacklist should be made.

The criteria are based on two basic properties: the repeatability of the attacking actions and their geographical distribution. That is, from an IP address listed in the blacklist, attacks must be made at least three times. The target of these attacks should be at least two honeypot servers. As a result of data processing, 7 475 addresses were included in the blacklist.

The diagram in Figure 2 shows the distribution of IP addresses from the blacklist by country.

The diagram in Figure 3 shows the distribution of attacking requests by country.

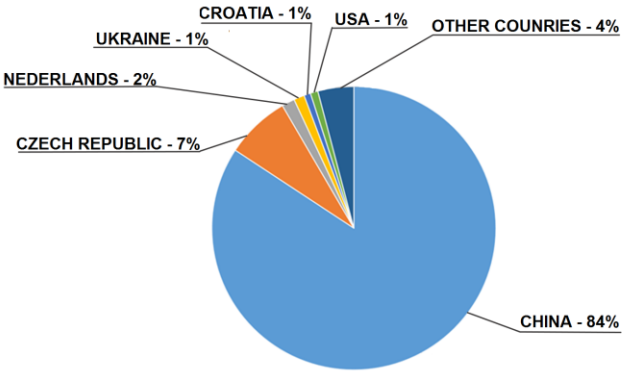

Figure 3. Distribution of attack requests by country.

The ordinate axis delayed the number of requests to the Samba service for the week. Data was taken from a honeypot server located in the USA. The intensity of the attack has increased dramatically since November 2017. Since September 2018, the intensity of the attacks has returned to background values. More than 860 thousand IP addresses sent requests to the American honeypot. In Russia, the intensity of the attacks was an order of magnitude less, and the greatest activity of the attacks was recorded in Rostov on Don.

5. General statistics for Internet services

After the log files for all ten Internet services are processed, we would like to see the comparative tables for the main types of variables that characterise the attacks. The first of these tables should contain data on the number of addresses in the blacklist for each service installed as part of the honeypot.

Table 12. The number of addresses in the blacklist.

№	Service type	The number of addresses in the black list
1	iptables	76 278
2	Samba	66 262
3	Web	7 870
4	SSH	7 475
5	SIP	1 914
6	MySQL	1 039
7	DNS	657
8	Mail	387
9	FTP	360
10	Squid	279

Naturally, the largest list of attacking addresses can be obtained by using a firewall. It detects a request on any ports and types of protocols, and therefore the size of its blacklist is the most complete. It contains the attacking addresses of all network protocols. It is surprising that the second place in the number of attacking addresses is the Samba service, which allows us to access disks and printers from various operating systems.

Another useful type of information on the structure of intrusions is the analysis of countries attacking requests and their IP addresses can be linked back to. Such information is compiled in

Tables 13 and 14. In these tables, the first three countries from the intrusion rating are given for each of the Internet services. Table 14 is based on data by IP addresses, and Table 14 contains data on the number of requests. In each cell, where the country is indicated, data on its percentage contribution to the general structure of attacking requests is also given.

Table 13. Leading Countries by Number of Attacking Addresses.

№	Service type	Countries whose IP addresses are under attack		
1	iptables	China (14%)	USA (14%)	India (7%)
2	Samba	Russia (14%)	Vietnam (12%)	Indonesia (12%)
3	Web	USA (13%)	China (8%)	India (6%)
4	SSH	China (31%)	USA (10%)	Republic of Korea (7%)
5	SIP	France (24%)	USA (22%)	Germany (16%)
6	MySQL	China (82%)	USA (9%)	Brazil (1%)
7	DNS	USA (26%)	China (19%)	Russia (8%)
8	Mail	USA (41%)	France (11%)	Russia (10%)
9	FTP	USA (30%)	France (15%)	Russia (11%)
10	Squid	Russia (18%)	China (17%)	USA (16%)

The data in these tables convincingly indicates from which country the vast majority of attacks are carried out. France, China and the USA can be attributed to the top three of such countries.

Also, the data of Tables 12, 13, 14 allow us to distinguish the main types of intrusions. Password pickup is the greatest threat (a simple password is up to 90% of all hacking incidents). Software flaws are the second most common threat. Data analysis shows that the largest number of holes can be found in the Samba service, but critical vulnerabilities can also occur in web servers, databases and mail servers.

Table 14. Leading Countries by the Number of Attacking Requests.

№	Service type	Countries whose IP addresses are under attack		
1	SIP	France (41%)	Netherlands (24%)	Germany (9%)
2	iptables	France (40%)	Germany (24%)	Russia (14%)
3	SSH	China (83%)	Czech (7%)	Netherlands (2%)
4	Samba	Russia (13%)	Vietnam (11%)	India (8%)
5	DNS	China (90%)	Netherlands (2%)	USA (2%)
6	Web	Ukraine (24%)	USA (20%)	France (18%)
7	MySQL	China (82%)	USA (9%)	Hong Kong (2%)
8	Mail	USA (41%)	France (11%)	Russia (10%)
9	Squid	France (38%)	Russia (12%)	Lithuania (11%)
10	FTP	Lithuania (77%)	France (10%)	USA (8%)

6. Conclusions

In this paper, we presented a series of results that were obtained using the honeypot method. By honeypot we mean a server on which 10 of the most popular Internet services are installed. This server is installed anonymously, without notification and registration, but on a public IP address. Therefore, repeated requests to the honeypot server can be considered suspicious.

Analysis of the log files of the network of honeypots, whose servers are scattered around the world, allow us to make a network intrusion model. This model consists of a number of elements. This paper presents the statistics of calls by ports and protocols and analyses the popularity of installed Internet services.

The processing of the received data is considered in detail using the example of the operating system remote control service SSH. First of all, the rank distribution is constructed for the number of requests to SSH. There is also a correlation between addresses attacking geographically distributed

honeypot servers. The rules for blacklisting the IP addresses of attacking addresses are discussed and fixed.

In addition to statistics for one of the services, data is presented for honeypot servers as a whole. The sizes of blacklists for all 10 services are compared, and the intensity of requests to each of the services is given. Separately, we analysed the geographical affiliation of attacking addresses and requests. For each of the services, the first 3 countries are allocated, the IP addresses of which provide the largest number of attacking requests.

The volume of data obtained is quite large, and in this paper only a small part of the results is given. We expect in the near future to provide new statistics obtained during the processing of the data.

7. References

[1] Gu Y, McCallum A and Towsley D 2005 October Detecting anomalies in network traffic using maximum entropy estimation *Proceedings of the 5th ACM SIGCOMM conference on Internet Measurement* 32-32

[2] Evsyutin O, Kokurina A and Mescheriakov R 2019 A review of methods of embedding information in digital objects for security in the internet of things *Computer Optics* **43(1)** 137-154 DOI: 10.18287/2412-6179-2019-43-1-137-154

[3] Spitzner L 2003 The honeynet project: Trapping the hackers *IEEE Security & Privacy* **99(2)** 15-23

[4] Wang R, Liu Z, Tao M and Zhang L 2015 Identifying Internet background radiation traffic based on traffic source distribution *Journal of High Speed Networks* **21(2)** 107-120

[5] Bhuyan M, Bhattacharyya D and Kalita J 2015 Towards Generating Real-life Datasets for Network Intrusion Detection *IJ Network Security* **17(6)** 683-701

[6] Ryoo J, Rizvi S, Aiken W and Kissell J 2013 Cloud security auditing: challenges and emerging approaches *IEEE Security & Privacy* **12(6)** 68-74

[7] Watson D and Riden J 2008 April The honeynet project: Data collection tools, infrastructure, archives and analysis *Workshop on Information Security Threats Data Collection and Sharing* 24-30

Acknowledgements

The work was done with the financial support of the Ministry of Science and Higher Education of the Russian Federation within the framework of state task No. 2.974.2017/4.6.