Analysis of Cyber Threats at the Level of a Distributed Network

Constantin-Alin COPACI, Adelaida STĂNCIULESCU, Ioan C. BACIVAROV
Faculty of Electronics, Telecommunications and Information Technology,
National University of Science and Technology POLITEHNICA Bucharest, Romania
constantin.copaci@stud.etti.upb.ro, adelaida.deatcu@stud.etti.upb.ro, ioan.bacivarov@upb.ro

Abstract

Ensuring a high level of security of the networks and IT systems that underpin the delivery of an organization's essential services has become a necessity that involves integrated, comprehensive approaches, the adoption of new and permanent cyber security strategies, significant financial investments and rapid organizational adaptations and ambitious. This article aims to provide a comprehensive analysis of the cyber security of a distributed computer network within an organization. In this context, the article promotes the implementation of proactive tools to strengthen cyber security at the institutional level.

Index terms: cyber security, vulnerability, cyber threats, monitoring, distributed network

1. Introduction

In this article we aim to highlight the diversity of cyber threats facing the organization, as well as draw attention to the importance of active, continuous monitoring and protection against them. Also, the article aims to sensitize users about the associated risks and encourage the implementation of proactive measures to prevent and combat cyber threats.

By being aware of and understanding cyber risks, the organization can take appropriate measures to effectively protect itself and reduce the potential impact of a cyber attack. The analysis of cyber-attacks of the last period revealed a series of significant cyber attacks and events at the global level:

DDoS attacks on Russian banks: At the end of July 2024, several banks in Russia, such as VTB, Gazprombank and Alfa Bank, were targeted by distributed denial-of-service (DDoS) attacks. The attacks were claimed by Ukraine's military intelligence services (HUR) and led to temporary disruptions to bank applications and websites, as well as major telecom operators such as Beeline and Rostelecom. This was one of the largest cyber attack campaigns in the region, reflecting the escalation of cyber conflicts between the two countries [1].

Attacks on the gaming industry: The mobile game "Hamster Kombat", which has more than 250 million players, has been the target of malware attacks targeting users with fake software for Android and Windows. Hackers were able to install spyware and information-stealing programs on players' devices.[2].

Virgin Media cyber attack: In July, Virgin Media was hit by a phishing attack that compromised the data of around 20,000 of the company's users. This was a demonstration of vulnerabilities in the protection systems of telecommunications companies, having consequences on the services offered [3].

Emergence of new ransomware groups: Several ransomware groups emerged during this period, such as "Volcano Demon" and "Eldorado". These groups have carried out attacks on companies in the real estate, education and healthcare sectors using advanced encryption and extortion techniques. "Eldorado" was notable for using ransomware variants adapted for VMware ESXi and Windows [4] [5].

2. Electronic services with Internet access vulnerable to cyber attacks

In general, any service connected to the Internet is exposed to security risks, and vulnerabilities can arise from various causes, such as misconfigurations, outdated software, or the lack of adequate protection measures.

Types of vulnerable electronic services with Internet access commonly found in an organization [6]:

- *Servers and databases*

Common vulnerabilities: Weak or default passwords, unauthorized access, wrong permission settings, outdated software.

Risks: Attackers can gain access to sensitive information such as users' personal data or confidential company files.

- *Online payment systems (e.g. e-commerce)*

Common vulnerabilities: Interception of payment data (if not properly encrypted), man-in-the-middle attacks, insecure storage of payment data.

Risks: Online fraud, theft of users' financial information (e.g. credit cards).

- *Email services*

Common vulnerabilities: Phishing, spoofing attacks, lack of encryption (e.g. TLS), use of weak passwords.

Risks: Theft of confidential information, spread of malware or viruses through infected emails, social typing attacks on users.

- *Cloud services*

Common vulnerabilities: Misconfiguration of permissions, lack of encryption of stored data, unauthorized access to sensitive files.

Risks: Compromise of data stored in the cloud, access and theft of sensitive information (e.g. documents or financial data), unauthorized deletion of files.

- *Websites and web applications*

Common vulnerabilities: Cross-Site Scripting (XSS), SQL Injection, authentication vulnerabilities, lack of encryption (SSL/TLS), lack of security updates.

Risks: Hackers can exploit vulnerabilities to access sensitive data, modify website content, intercept user data, or infect visitors with malware.

- *Virtual Private Networks (VPNs)*

Common vulnerabilities: Insecure VPN protocols, use of compromised VPN servers, weak encryption.

Risks: Exposure of personal data and browsing history, identification and location of users, possibility of being tracked or intercepted data transmitted.

3. Web traffic monitoring

Internet traffic monitoring was carried out to assess how the Internet is used within the organization and to identify potential security issues. Data traffic analysis is essential to understand user behavior and proactively implement appropriate security measures.

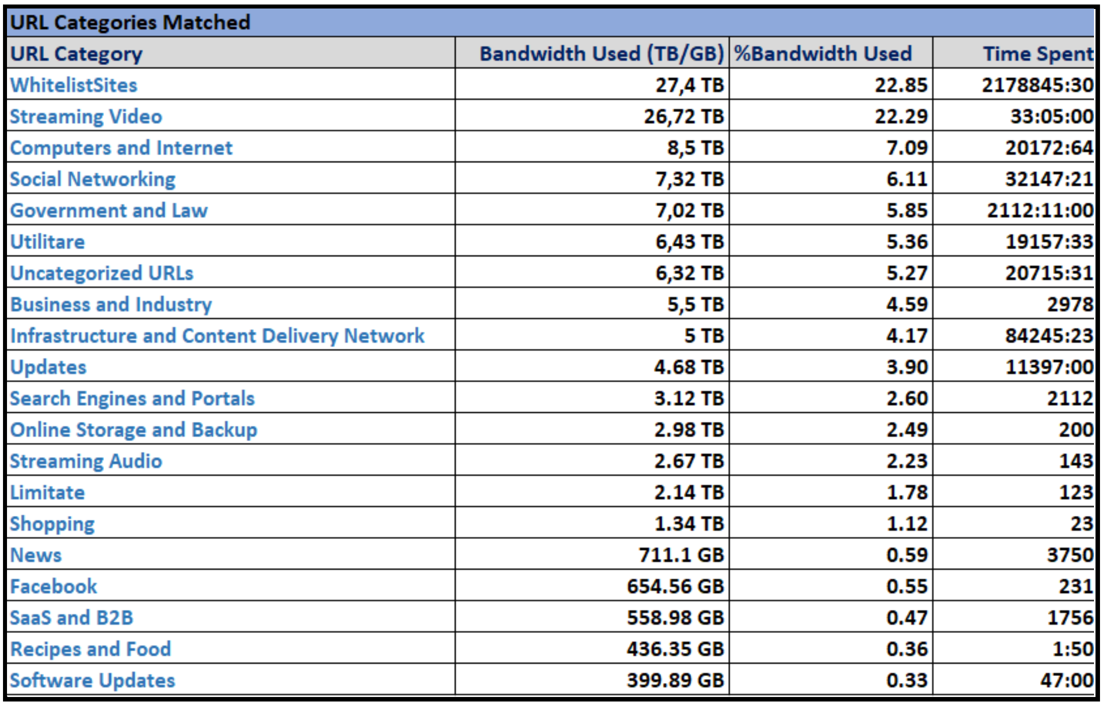
Traffic monitoring was carried out on two levels:

a. Analysis of data traffic between networks (LAN, WAN, Internet) – performed at the router level;
b. Using a Squid proxy log analyzer configured at the proxy server level.

3.1. Analysis of data traffic between networks (LAN, WAN, Internet) – performed at the router level

Monitoring network equipment is critical to ensuring optimal performance, detecting and preventing network problems, and maintaining security.

At the level of the organization under analysis, the top 20 positions in descending order, from the point of view of generated traffic, look like this (Figure 1):



URL Categories Matched			
URL Category	Bandwidth Used (TB/GB)	%Bandwidth Used	Time Spent
WhitelistSites	27,4 TB	22.85	2178845:30
Streaming Video	26,72 TB	22.29	33:05:00
Computers and Internet	8,5 TB	7.09	20172:64
Social Networking	7,32 TB	6.11	32147:21
Government and Law	7,02 TB	5.85	2112:11:00
Utilitare	6,43 TB	5.36	19157:33
Uncategorized URLs	6,32 TB	5.27	20715:31
Business and Industry	5,5 TB	4.59	2978
Infrastructure and Content Delivery Network	5 TB	4.17	84245:23
Updates	4.68 TB	3.90	11397:00
Search Engines and Portals	3.12 TB	2.60	2112
Online Storage and Backup	2.98 TB	2.49	200
Streaming Audio	2.67 TB	2.23	143
Limitate	2.14 TB	1.78	123
Shopping	1.34 TB	1.12	23
News	711.1 GB	0.59	3750
Facebook	654.56 GB	0.55	231
SaaS and B2B	558.98 GB	0.47	1756
Recipes and Food	436.35 GB	0.36	1:50
Software Updates	399.89 GB	0.33	47:00

Fig. 1. Top 20 positions in descending order, in terms of traffic generated

As percentages, these data are represented in the following graph (Figure 2):

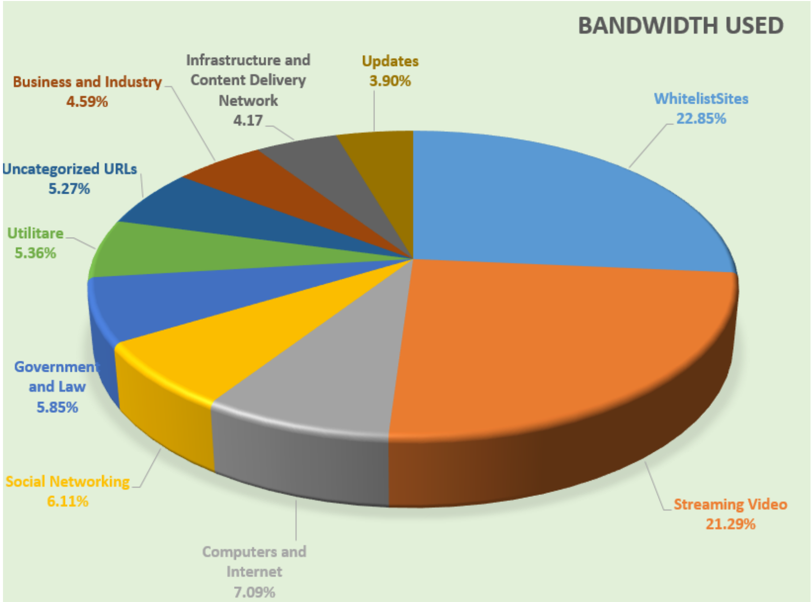


Fig. 2. Graphic representation of the values regarding the generated traffic

The conducted study revealed the following trends in the use of the Internet by users:

- Professional Activities: Access to information relevant to the performance of work duties.
- Media Content Consumption: Watching videos, participating in video conferences or listening to music.
- Accessing government websites and legislation.
- Social Media Interaction: Navigating social media platforms for communication and interaction.
- Email Management: Checking and replying to emails.
- Searching for Personal Information and Online Shopping: Using the Internet to search for information of personal interest or to make online purchases.

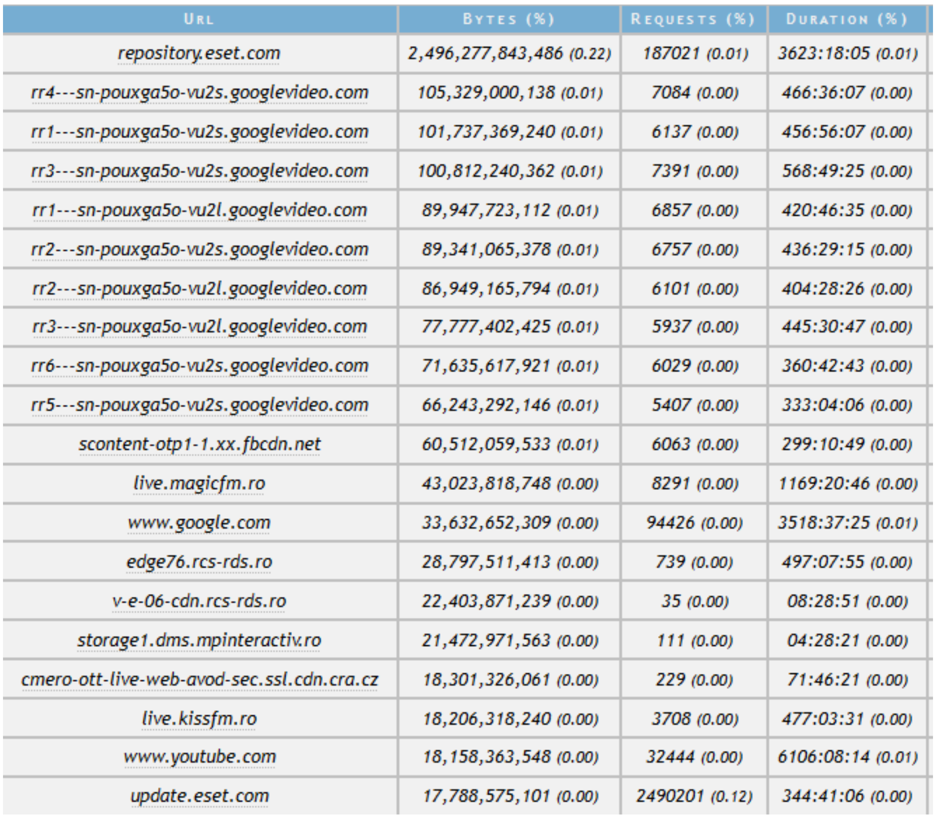
3.2. At the proxy server level

At the organization level a proxy server is configured and a network **cache (Squid)** is used to handle HTTP, HTTPS and FTP traffic, used to improve network performance and improve security. Squid is also used for **traffic filtering purposes, access monitoring** and **temporary storage of frequently accessed resources** (cache), to reduce latencies and network load.

Traffic monitoring was done by using the SquidAnalyzer software [7], installed on the proxy server within the organization. This software is a Squid proxy log analyzer and report generator with statistics on times, hits, bytes, users, networks, URLs and domains. Statistical reports are geared towards user and bandwidth control.

SquidAnalyzer uses flat files to store data and does not require SQL, SQL Lite or Berkeley databases. This log parser is incremental.

The analysis of network traffic generated at the level of the organization (August-October 2024) was carried out from the perspective *of relevance and use of network resources.* The top 20 most accessed web addresses in terms of traffic (total amount of data transferred) are shown in Figure 3.



URL	BYTES (%)	REQUESTS (%)	DURATION (%)
repository.eset.com	2,496,277,843,486 (0.22)	187021 (0.01)	3623:18:05 (0.01)
rr4---sn-pouxga5o-vu2s.googlevideo.com	105,329,000,138 (0.01)	7084 (0.00)	466:36:07 (0.00)
rr1---sn-pouxga5o-vu2s.googlevideo.com	101,737,369,240 (0.01)	6137 (0.00)	456:56:07 (0.00)
rr3---sn-pouxga5o-vu2s.googlevideo.com	100,812,240,362 (0.01)	7391 (0.00)	568:49:25 (0.00)
rr1---sn-pouxga5o-vu2l.googlevideo.com	89,947,723,112 (0.01)	6857 (0.00)	420:46:35 (0.00)
rr2---sn-pouxga5o-vu2s.googlevideo.com	89,341,065,378 (0.01)	6757 (0.00)	436:29:15 (0.00)
rr2---sn-pouxga5o-vu2l.googlevideo.com	86,949,165,794 (0.01)	6101 (0.00)	404:28:26 (0.00)
rr3---sn-pouxga5o-vu2l.googlevideo.com	77,777,402,425 (0.01)	5937 (0.00)	445:30:47 (0.00)
rr6---sn-pouxga5o-vu2s.googlevideo.com	71,635,617,921 (0.01)	6029 (0.00)	360:42:43 (0.00)
rr5---sn-pouxga5o-vu2s.googlevideo.com	66,243,292,146 (0.01)	5407 (0.00)	333:04:06 (0.00)
scontent-otp1-1.xx.fbcdn.net	60,512,059,533 (0.01)	6063 (0.00)	299:10:49 (0.00)
live.magicfm.ro	43,023,818,748 (0.00)	8291 (0.00)	1169:20:46 (0.00)
www.google.com	33,632,652,309 (0.00)	94426 (0.00)	3518:37:25 (0.01)
edge76.rcs-rds.ro	28,797,511,413 (0.00)	739 (0.00)	497:07:55 (0.00)
v-e-06-cdn.rcs-rds.ro	22,403,871,239 (0.00)	35 (0.00)	08:28:51 (0.00)
storage1.dms.mpinteractiv.ro	21,472,971,563 (0.00)	111 (0.00)	04:28:21 (0.00)
cmero-ott-live-web-avod-sec.ssl.cdn.cra.cz	18,301,326,061 (0.00)	229 (0.00)	71:46:21 (0.00)
live.kissfm.ro	18,206,318,240 (0.00)	3708 (0.00)	477:03:31 (0.00)
www.youtube.com	18,158,363,548 (0.00)	32444 (0.00)	6106:08:14 (0.01)
update.eset.com	17,788,575,101 (0.00)	2490201 (0.12)	344:41:06 (0.00)

Fig. 3. The top 20 most accessed web addresses in terms of traffic

The total amount of bytes transferred for each URL (web page) was analyzed. As you can see, the first place is the updates of the antivirus solution (Eset). During the analyzed period, the traffic that the antivirus solution updates generate is approximately 2.5 TB, being approximately 24 times higher than that of the next accessed page (Figure 4).

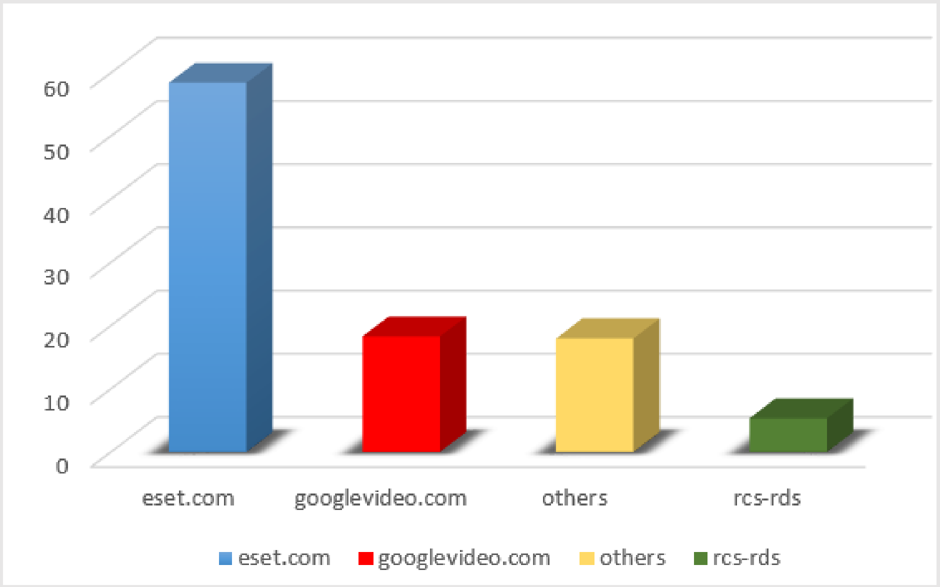
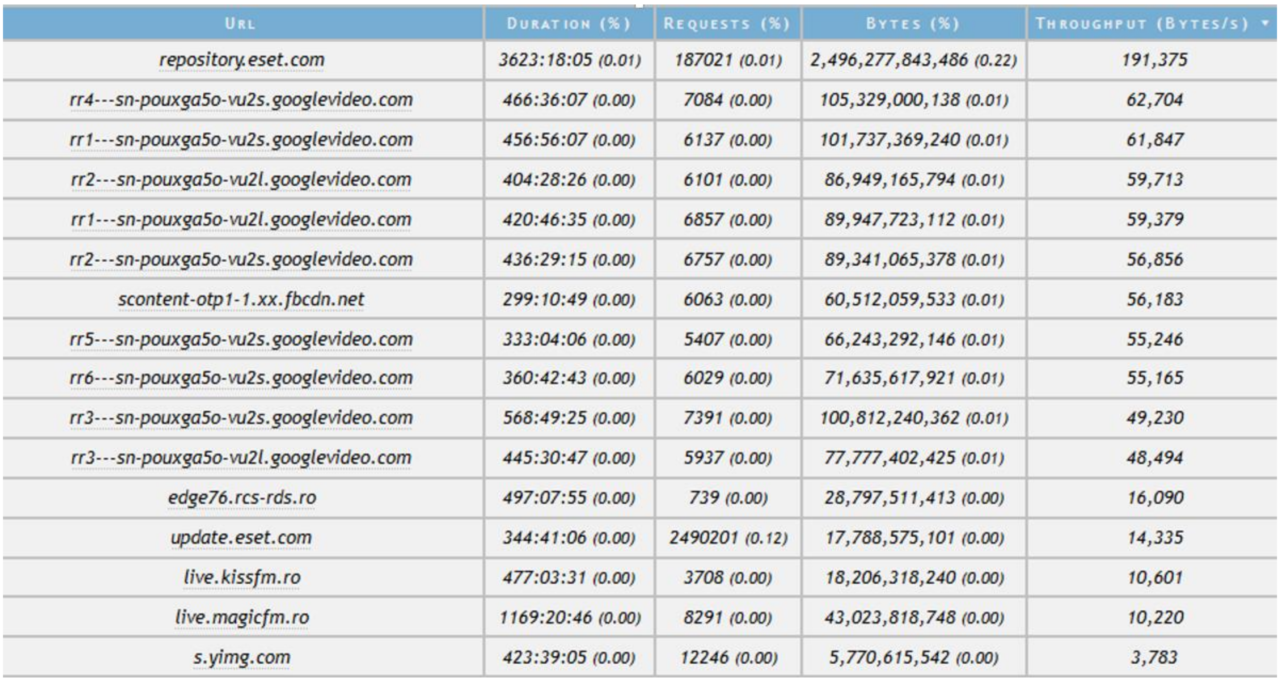


Fig. 4. Total amount of bytes transferred for each URL

Time spent by users on web pages:

The sites on which users spent the most time were identified by analyzing URLs with high throughput, indicating sites of high interest or abnormal activity (Figure 5).



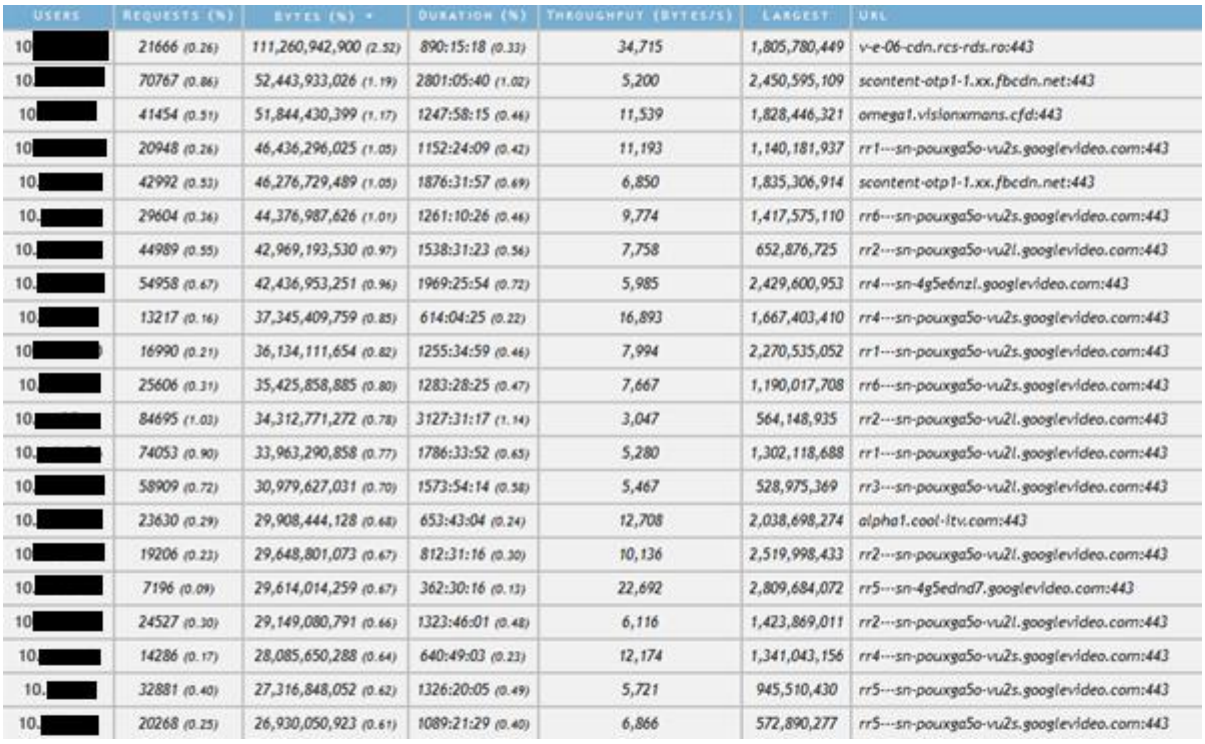
Url	Duration (%)	Requests (%)	Bytes (%)	Throughput (Bytes/s) ▾
repository.eset.com	3623:18:05 (0.01)	187021 (0.01)	2,496,277,843,486 (0.22)	191,375
rr4---sn-pouxga5o-vu2s.googlevideo.com	466:36:07 (0.00)	7084 (0.00)	105,329,000,138 (0.01)	62,704
rr1---sn-pouxga5o-vu2s.googlevideo.com	456:56:07 (0.00)	6137 (0.00)	101,737,369,240 (0.01)	61,847
rr2---sn-pouxga5o-vu2l.googlevideo.com	404:28:26 (0.00)	6101 (0.00)	86,949,165,794 (0.01)	59,713
rr1---sn-pouxga5o-vu2l.googlevideo.com	420:46:35 (0.00)	6857 (0.00)	89,947,723,112 (0.01)	59,379
rr2---sn-pouxga5o-vu2s.googlevideo.com	436:29:15 (0.00)	6757 (0.00)	89,341,065,378 (0.01)	56,856
scontent-otp1-1.xx.fbcdn.net	299:10:49 (0.00)	6063 (0.00)	60,512,059,533 (0.01)	56,183
rr5---sn-pouxga5o-vu2s.googlevideo.com	333:04:06 (0.00)	5407 (0.00)	66,243,292,146 (0.01)	55,246
rr6---sn-pouxga5o-vu2s.googlevideo.com	360:42:43 (0.00)	6029 (0.00)	71,635,617,921 (0.01)	55,165
rr3---sn-pouxga5o-vu2s.googlevideo.com	568:49:25 (0.00)	7391 (0.00)	100,812,240,362 (0.01)	49,230
rr3---sn-pouxga5o-vu2l.googlevideo.com	445:30:47 (0.00)	5937 (0.00)	77,777,402,425 (0.01)	48,494
edge76.rcs-rds.ro	497:07:55 (0.00)	739 (0.00)	28,797,511,413 (0.00)	16,090
update.eset.com	344:41:06 (0.00)	2490201 (0.12)	17,788,575,101 (0.00)	14,335
live.kissfm.ro	477:03:31 (0.00)	3708 (0.00)	18,206,318,240 (0.00)	10,601
live.magicfm.ro	1169:20:46 (0.00)	8291 (0.00)	43,023,818,748 (0.00)	10,220
s.yimg.com	423:39:05 (0.00)	12246 (0.00)	5,770,615,542 (0.00)	3,783

Fig. 5. Sites on which users spent the most time

It is noted that, in this case, the first place is occupied by the web page called by the services that ensure the perimeter protection of users (antivirus server).

Top 20 users with the most activity:

Users with the highest number of requests (total time spent online and URLs accessed) are identified (Figure 6).



USERS	REQUESTS (%)	BYTES (%) •	DURATION (%)	THROUGHPUT (BYTES/S)	LARGEST	URL
10[redacted]	21666 (0.26)	111,260,942,900 (2.52)	890:15:18 (0.33)	34,715	1,805,780,449	v-e-06-cdn.rcs-rds.ro:443
10.[redacted]	70767 (0.86)	52,443,933,026 (1.19)	2801:05:40 (1.02)	5,200	2,450,595,109	scontent-otp1-1.xx.fbcdn.net:443
10[redacted]	41454 (0.51)	51,844,430,399 (1.17)	1247:58:15 (0.46)	11,539	1,828,446,321	omega1.visionxmans.cfd:443
10[redacted]	20948 (0.26)	46,436,296,025 (1.05)	1152:24:09 (0.42)	11,193	1,140,181,937	rr1---sn-pouxga5o-vu2s.googlevideo.com:443
10.[redacted]	42992 (0.53)	46,276,729,489 (1.05)	1876:31:57 (0.69)	6,850	1,835,306,914	scontent-otp1-1.xx.fbcdn.net:443
10.[redacted]	29604 (0.36)	44,376,987,626 (1.01)	1261:10:26 (0.46)	9,774	1,417,575,110	rr6---sn-pouxga5o-vu2s.googlevideo.com:443
10.[redacted]	44989 (0.55)	42,969,193,530 (0.97)	1538:31:23 (0.56)	7,758	652,876,725	rr2---sn-pouxga5o-vu2l.googlevideo.com:443
10.[redacted]	54958 (0.67)	42,436,953,251 (0.96)	1969:25:54 (0.72)	5,985	2,429,600,953	rr4---sn-4g5e6nzl.googlevideo.com:443
10.[redacted]	13217 (0.16)	37,345,409,759 (0.85)	614:04:25 (0.22)	16,893	1,667,403,410	rr4---sn-pouxga5o-vu2s.googlevideo.com:443
10[redacted]	16990 (0.21)	36,134,111,654 (0.82)	1255:34:59 (0.46)	7,994	2,270,535,052	rr1---sn-pouxga5o-vu2s.googlevideo.com:443
10.[redacted]	25606 (0.31)	35,425,858,885 (0.80)	1283:28:25 (0.47)	7,667	1,190,017,708	rr6---sn-pouxga5o-vu2s.googlevideo.com:443
10[redacted]	84695 (1.03)	34,312,771,272 (0.78)	3127:31:17 (1.14)	3,047	564,148,935	rr2---sn-pouxga5o-vu2l.googlevideo.com:443
10.[redacted]	74053 (0.90)	33,963,290,858 (0.77)	1786:33:52 (0.65)	5,280	1,302,118,688	rr1---sn-pouxga5o-vu2l.googlevideo.com:443
10[redacted]	58909 (0.72)	30,979,627,031 (0.70)	1573:54:14 (0.58)	5,467	528,975,369	rr3---sn-pouxga5o-vu2l.googlevideo.com:443
10.[redacted]	23630 (0.29)	29,908,444,128 (0.68)	653:43:04 (0.24)	12,708	2,038,698,274	alpha1.cool-itv.com:443
10[redacted]	19206 (0.23)	29,648,801,073 (0.67)	812:31:16 (0.30)	10,136	2,519,998,433	rr2---sn-pouxga5o-vu2l.googlevideo.com:443
10.[redacted]	7196 (0.09)	29,614,014,259 (0.67)	362:30:16 (0.13)	22,692	2,809,684,072	rr5---sn-4g5ednd7.googlevideo.com:443
10[redacted]	24527 (0.30)	29,149,080,791 (0.66)	1323:46:01 (0.48)	6,116	1,423,869,011	rr2---sn-pouxga5o-vu2l.googlevideo.com:443
10.[redacted]	14286 (0.17)	28,085,650,288 (0.64)	640:49:03 (0.23)	12,174	1,341,043,156	rr4---sn-pouxga5o-vu2s.googlevideo.com:443
10.[redacted]	32881 (0.40)	27,316,848,052 (0.62)	1326:20:05 (0.49)	5,721	945,510,430	rr5---sn-pouxga5o-vu2s.googlevideo.com:443
10.[redacted]	20268 (0.25)	26,930,050,923 (0.61)	1089:21:29 (0.40)	6,866	572,890,277	rr5---sn-pouxga5o-vu2s.googlevideo.com:443

Fig. 6. Identifying users with the highest number of requests

User level detail:

Table 1. User level detail

No.	Department	Computer IP	Username	The most visited sites
1	Department 1	10. [redacted]	User 1	www.digionline.ro, www.temu.com
2	Department 2	10. [redacted]	User 2	www.youtube.com, www.facebook.com
3	Department 3	10. [redacted]	User 3	live.magicfm.ro, cmero-ott-live-web-avod-sec.ssl.cdn.cra.cz
4	Department 1	10. [redacted]	User 4	www.youtube.com, play.google.com, googlevideo.com
5	Department 1	10. [redacted]	User 5	chat.facebook.com, play.google.com
6	Department 2	10. [redacted]	User 6	www.youtube.com, googlevideo.com
7	Department 3	10. [redacted]	User 7	www.youtube.com
8	Department 3	10. [redacted]	User 8	live.streamtheworld.com, www.youtube.com
9	Department 2	10. [redacted]	User 9	www.youtube.com, play.google.com
10	Department 2	10. [redacted]	User 10	www.youtube.com, play.google.com
11	Department 2	10. [redacted]	User 11	www.youtube.com, play.google.com
12	Department 1	10. [redacted]	User 12	www.youtube.com
13	Department 2	10. [redacted]	User 13	www.youtube.com
14	Department 3	10. [redacted]	User 14	www.youtube.com, cool-eTV.net
15	Department 3	10. [redacted]	User 15	play.discomix.ro, www.youtube.com
16	Department 2	10. [redacted]	User 16	www.youtube.com, play.google.com
17	Department 1	10. [redacted]	User 17	www.youtube.com, play.google.com
18	Department 1	10. [redacted]	User 18	www.youtube.com, play.google.com
19	Department 2	10. [redacted]	User 19	www.youtube.com, facebook.ro
20	Department 2	10. [redacted]	User 20	www.youtube.com

4. Conclusions

Cyber threat analysis within the organization highlights a dynamic and complex cyber security landscape. Amidst the intensification of cyber attacks globally, it is important to adopt proactive and preventive measures to protect the integrity of the IT infrastructure and reduce the potential impact of attacks.

The paper proposed web traffic analysis from the perspective of bandwidth optimization for professional activities. This helps maintain a balance between operational needs and IT security.

Protecting electronic services that access the Internet becomes essential in preventing cyber attacks and protecting personal and organizational data.

Data traffic analysis also proves to be essential to understand user behavior in order to implement appropriate security measures appropriate to the organizational security culture.

References

[1]. https://therecord.media/major-russian-banks-ddos-attack-ukraine

[2]. https://www.bleepingcomputer.com/news/security/hamster-kombats-250-million-players-targeted-in-malware-attacks/

[3]. https://community.virginmedia.com/t5/Security-matters/Latest-Phishing-News-24-07-2024/td-p/5547441

[4]. https://www.bleepingcomputer.com/news/security/new-eldorado-ransomware-targets-windows-vmware-esxi-vms/

[5]. https://therecord.media/ransomware-group-volcano-demon-lukalocker

[6]. https://www.cve.org/

[7]. https://squidanalyzer.darold.net/