

Tartalom

Vezetői összefoglaló.....	3
Előzmények.....	4
Az előelemzés eredménye	5
Az összes kérés elemzése 2021.09.17.....	5
Az összes kérés elemzése 2021.09.18.....	36
Kiberbiztonsági elemzés.....	67
A hosting szolgáltató hálózati terhelés kimutatása:	67
Támadási minták.....	70
Az összes konkurens kérés mintázata.....	70
Az SSH bejelentkezési felület támadása	71
A webes admin felület támadási mintázata.....	72
A rendszert, nem szabványos módon elérni kívánó IP címek eloszlása	73
A rendszert nem szabványos módon elérni kívánó IP címek országonkénti eloszlása	74
A rendszer parancssori elérést célzó ip címek eloszlása országonként	75
A szabványos kérések és a támadások eloszlása forrás címekhez viszonyítva.....	76
Terheléses támadás	77
A támadó IP címek attribútumai.....	78
Összefoglalás.....	79

Vezetői összefoglaló

A szeptember 17-i és 18-i előválasztási rendszer leállítását három, egymástól nem elválasztható körülmény eredményezte.

Elsők között olyan konfigurációs hibák említhetőek, hogy az alkalmazást kiszolgáló infrastruktúra alulméretezett, hálózati szempontból védtelen volt, így a megnövekedett forgalom és a rendszert ért támadásokkal szemben nem volt megfelelően védve, így nem volt képes a normális kérések kiszolgálására.

A menedzsment, a számítógépek közötti szinkronizációt és a beérkező kéréseket ugyanazon csatorna volt hivatott kiszolgálni, így a megnövekedett, túlterhelt forgalom blokkolta a számítógépek közötti, valamint az adminisztrátorok és a kiszolgálók közötti kommunikációt.

A problémát a szerverek hálózati kapcsolatának működésképtelensége/túlterhelése okozta

Mindemellett jól ismert támadó hálózatok támadták a kiszolgálókat, de ez adatvesztéssel, az adatok integritásának elvesztésével, jogosulatlan adathozzáféréssel nem járt, a rendelkezésre állás viszont nagyban sérült.

Előzmények

„Szeptember 17-ike 19 és 21 óra között időszakos, majd 18-án 8 órától fokozatosan erősödő anomáliák jelentkeztek egy hazai szolgáltatónál elhelyezett szervereink elérésében, amelyek 10 órától a rendszer teljes elérhetetlenségéhez vezettek. Az informatikusokkal és a szerverszoba-szolgáltatóval történt többszöri egyeztetés után sem sikerült a problémára azonnali megoldást találni, de minden jel az erőforrások (vagy sávszélesség) extrém és indokolatlan túlterhelésére mutatott (amíg volt hálózati kapcsolat, a szerverek nem mutattak extrém processzorhasználati, vagy memória adatokat). (A szerverekhez kapcsolódó Cloudflare védelmi rendszer a legkritikusabb órákban több egyéb fenyegetést is megállított, amelyek kiindulását Kínára és az Egyesült Államokra azonosította, de ennek csak az azonos időzítés miatt lehet jelentősége, nem értek célt.) A szerverszoba szolgáltatójánál a hétfégi személyzet első ránézésre nem tapasztalt hardveres, vagy forgalmi anomáliákat. A szervernaplók túl elsősorban a szerverszoba routerjének naplófájljaira lett volna szükség, amelyet válaszuk szerint nem tárolnak. Eközben az aHang és a pártok informatikusai biztonsági szakértők bevonásával elemezték a helyzetet a rendelkezésre álló információk alapján, és mivel a problémát nem sikerült egyértelműen azonosítani, a teljes rendszer azonnali elköltöztetése mellett döntöttek, amit a csoport rögtön meg is kezdett.

Az OEVB ezt követően az előválasztás hétfőig való felfüggesztéséről döntött.

Délután sikerült elérni felsőbb vezetőt a szerverszoba-szolgáltatónál, aki azt közölte, hogy „mégis van a normálistól eltérő külföldi terhelés egy csatornán, ami reálisan megállíthatta a rendszert”. Kértünk minden lehetséges rendelkezésre álló adatot, de mindössze grafikonokat kaptunk meg, amelyen ugyan jól látszik az érintett időszávokban érkezett extrém terhelés, de nem derült ki, hogy ez milyen csatornán, honnan jött, hogyan és pontosan mire irányult (ezeket a részleteket továbbra is próbáljuk kideríteni). (forrás:aHang)

Az előelemzés eredménye

Az elérhető információk azonnali elemzése a 2021, szeptember 17. és 2021 szeptember 18-i logog alapján az alábbi képet mutatta:

Az összes kérés elemzése 2021.09.17.

UNIQUE VISITORS PER DAY - INCLUDING SPIDERS
 HITS HAVING THE SAME IP, DATE AND AGENT ARE A UNIQUE VISIT.

Panel Options

17/Sep/20210.089k180k270k350k440k530k620k710k800k0.09.0k18k27k36k45k54k63k72k81kHitsVisitorsHitsVisitors

#	HITS	VISITORS	TX. AMOUNT	DATA
MIN.	886 437 (100.00%)	90 068 (100.00%)	10.76 GiB (100.00%)	
MAX.	886 437 (100.00%)	90 068 (100.00%)	10.76 GiB (100.00%)	
AVG.	886 437 (100.00%)	90 068 (100.00%)	10.76 GiB (100.00%)	
1	886 437 (100.00%)	90 068 (100.00%)	10.76 GiB (100.00%)	17/Sep/2021
TOT.	886 437	90 068	10.76 GiB	1

-
-
-
-

REQUESTED FILES (URLS)
 TOP REQUESTS SORTED BY HITS [,AVGTS,CUMITS,MAXTS,MTHD,PROTO]

Panel Options

POST /idopont/elovalasztas2021 HTTP/1.1 GET /idopont/elovalasztas2021?utm_source=Email&utm_medium=Newsletter&utm_campaign=PR-1_44452 HTTP/1.1 GET /jeloltek/377 HTTP/1.1 GET /jeloltek/368 HTTP/1.1 GET /api/tszHelper/getOevk?zipcode=8000 HTTP/1.1 POST /api/v4/users/ids?since=1631879346533 HTTP/1.1 GET /api/v4/system/notices/75td34dzfyaxddjdicboa81a?client=web&clientVersion=5.36.1 HTTP/1.1 GET /wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1 HTTP/2 GET /appversions/update/obfuscated HTTP/1.1 GET /api/tszHelper/getOevk?zipcode=1138 HTTP/20.04.1k8.1k12k16k20k24k28k32k37k0.01.8k3.6k5.3k7.1k8.9k11k12k14k16kHitsVisitorsHitsVisitors

#	HITS	VISITORS	TX. AMOUNT	METHOD	PROTOCOL	DATA
MIN.	1 (0.00%)	1 (0.00%)	—	—	—	—
MAX.	40 558 (7.45%)	17 744 (7.22%)	376.95 MiB (11.08%)	—	—	—
AVG.	5 (0.00%)	2 (0.00%)	34.49 KiB (0.00%)	—	—	—
1	40 558 (4.58%)	6 864 (7.62%)	212.58 MiB (1.93%)	POST	HTTP/1.1	/idopont/elovalasztas2021
2	33 869 (3.82%)	13 624 (15.13%)	376.95 MiB (3.42%)	GET	HTTP/2	/
3	31 829 (3.59%)	12 175 (13.52%)	195.44 MiB (1.77%)	GET	HTTP/1.1	/idopont/elovalasztas2021
4	30 789 (3.47%)	7 199 (7.99%)	1.27 MiB (0.01%)	GET	HTTP/1.1	/queue
5	26 221 (2.96%)	17 744 (19.70%)	57.75 MiB (0.52%)	GET	HTTP/2	/oevk-finder
6	17 289 (1.95%)	5 851 (6.50%)	13.69 MiB (0.12%)	GET	HTTP/1.1	/slots/timetable/elovalasztas2021

#	HITS	VISITORS	TX. AMOUNT	METHOD	PROTOCOL	DATA
MIN.	1 (0.00%)	1 (0.00%)	—	—	—	—
MAX.	40 558 (7.45%)	17 744 (7.22%)	376.95 MiB (11.08%)	—	—	—
AVG.	5 (0.00%)	2 (0.00%)	34.49 KiB (0.00%)	—	—	—
7	13 544 (1.53%)	384 (0.43%)	9.76 MiB (0.09%)	POST	HTTP/1.1	/api/v4/users/status/ids
8	9 932 (1.12%)	3 704 (4.11%)	10.48 MiB (0.10%)	GET	HTTP/1.1	/slots/sendlink/obfuscated
9	7 550 (0.85%)	3 444 (3.82%)	5.75 MiB (0.05%)	POST	HTTP/1.1	/slots/sendlink/obfuscated
10	6 498 (0.73%)	15 (0.02%)	317.29 KiB (0.00%)	POST	HTTP/1.1	/slots/recover
11	5 818 (0.66%)	277 (0.31%)	7.06 MiB (0.06%)	GET	HTTP/1.1	/api/v4/users/me/teams/75td34dzjfyaxddjdicboa81a/channels/members
12	5 515 (0.62%)	160 (0.18%)	14.13 MiB (0.13%)	GET	HTTP/1.1	/api/v4/users/me/teams/75td34dzjfyaxddjdicboa81a/channels?include_deleted=true
13	5 506 (0.62%)	288 (0.32%)	409.38 KiB (0.00%)	POST	HTTP/1.1	/api/v4/channels/members/me/view
14	5 215 (0.59%)	163 (0.18%)	1005.73 KiB (0.01%)	POST	HTTP/1.1	/users/login

#	HITS	VISITORS	TX. AMOUNT	METHOD	PROTOCOL	DATA
MIN.	1 (0.00%)	1 (0.00%)	—	—	—	—
MAX.	40 558 (7.45%)	17 744 (7.22%)	376.95 MiB (11.08%)	—	—	—
AVG.	5 (0.00%)	2 (0.00%)	34.49 KiB (0.00%)	—	—	—
15	5 200 (0.59%)	158 (0.18%)	117.73 MiB (1.07%)	GET	HTTP/1.1	/elections/coredata/26
16	4 979 (0.56%)	2 680 (2.98%)	40.8 MiB (0.37%)	GET	HTTP/1.1	/_next/image?url=/logo-1215x215.png&w=1080&q=75
17	4 726 (0.53%)	272 (0.30%)	560.38 KiB (0.00%)	GET	HTTP/1.1	/api/v4/users/me/teams/unread
18	4 655 (0.53%)	963 (1.07%)	13.21 MiB (0.12%)	GET	HTTP/1.1	/_next/image?url=/logo-1215x215.png&w=384&q=75
19	4 619 (0.52%)	2 544 (2.82%)	47.71 MiB (0.43%)	GET	HTTP/2	/?
20	4 342 (0.49%)	161 (0.18%)	4.94 MiB (0.04%)	GET	HTTP/1.1	/api/v4/plugins/webapp
21	3 896 (0.44%)	1 689 (1.88%)	18.77 MiB (0.17%)	GET	HTTP/1.1	/_next/image?url=/logo-1215x215.png&w=640&q=75
22	3 245 (0.37%)	190 (0.21%)	48.49 MiB (0.44%)	GET	HTTP/1.1	/users

#	HITS	VISITORS	TX. AMOUNT	METHOD	PROTOCOL	DATA
MIN.	1 (0.00%)	1 (0.00%)	—	—	—	
MAX.	40 558 (7.45%)	17 744 (7.22%)	376.95 MiB (11.08%)	—	—	
AVG.	5 (0.00%)	2 (0.00%)	34.49 KiB (0.00%)	—	—	
23	3 055 (0.34%)	1 377 (1.53%)	65.81 MiB (0.60%)	GET	HTTP/1.1	/
24	2 504 (0.28%)	988 (1.10%)	3.5 MiB (0.03%)	GET	HTTP/1.1	/presences/onlinevote/26
TOT.	544 149	245 909	3.32 GiB	—	—	101 058

-
-
-
-

STATICREQUESTS

TOP STATIC REQUESTS SORTED BY HITS[, AVGTS, CUMTTS, MAXTS, MTHD, PROTO]

Panel Options

GET /_next/static/chunks/6b7d6a5cd9e9e7f1ca56102c1924426761ff9fc3.fac4a36e54a002ab79c5.js HTTP/2GET /img/barion-card-strip-intl.svg HTTP/2GET /assets/img/elni-hivlak-1920x1080.png HTTP/2GET /_next/static/chunks/pages/id-capture-3ea0229577b51e2cc8a6.js HTTP/1.1GET /js/popper.min.js HTTP/1.1GET /_next/static/chunks/pages/oevk-finder-f04545eaeaf61ce2b36a.js HTTP/1.1GET /wp-content/uploads/2019/09/New-Google.png HTTP/2GET /assets/img/hero/hero-1-overly.png HTTP/2GET /apple-touch-icon-120x120-precomposed.png HTTP/2GET /wp-content/themes/wao2018/img/wao-logo_2_hu.png HTTP/1.10.01.8k3.6k5.3k7.1k8.9k11k12k14k16k0.01.7k3.4k5.1k6.8k8.5k10k12k14k15kHitsVisitorsHitsVisitors

#	HITS	VISITORS	TX. AMOUNT	METHOD	PROTOCOL	DATA
MIN.	1 (0.00%)	1 (0.00%)	—	—	—	
MAX.	17 818 (5.29%)	17 001 (5.53%)	2.09 GiB (28.31%)	—	—	
AVG.	93 (0.03%)	85 (0.03%)	2.1 MiB (0.03%)	—	—	
1	17 818 (2.01%)	16 991 (18.86%)	2.09 GiB (19.45%)	GET	HTTP/2	/_next/static/chunks/6b7d6a5cd9e9e7f1ca56102c1924426761ff9fc3.fac4a36e54a002ab79c5.js
2	17 803 (2.01%)	17 001 (18.88%)	1.4 GiB (12.98%)	GET	HTTP/2	/_next/static/chunks/4dbb12635a627dcd0960f648091e077e847b268e.f5d8f9b6e2e5d67efa16.js
3	17 380 (1.96%)	16 486 (18.30%)	1.09 GiB (10.14%)	GET	HTTP/2	/_next/static/css/8bf75869.f97d1e43.chunk.css
4	17 247 (1.95%)	16 456 (18.27%)	187.23 MiB (1.70%)	GET	HTTP/2	/_next/static/chunks/e59a682365ab2f2de7f8de9f2fd50c497923cacc.f3c3d5155526e4a2120.js
5	17 247 (1.95%)	16 445 (18.26%)	286.01 MiB (2.60%)	GET	HTTP/2	/_next/static/chunks/pages/_app-2d8979f5242eb4b40296.js
6	17 225 (1.94%)	16 405 (18.21%)	683.24 MiB (6.20%)	GET	HTTP/2	/_next/static/chunks/framework.ced6e340f70acef0a47b.js
7	17 091 (1.93%)	16 243 (18.03%)	1.12 MiB (0.01%)	GET	HTTP/2	/_next/static/chunks/8bf75869.c3c33dcc23d96beb9452.js
8	17 089 (1.93%)	16 237 (18.03%)	5.32 MiB (0.05%)	GET	HTTP/2	/_next/static/css/styles.992800d0.chunk.css

#	HITS	VISITORS	TX. AMOUNT	METHOD	PROTOCOL	DATA
MIN.	1 (0.00%)	1 (0.00%)	—	—	—	
MAX.	17 818 (5.29%)	17 001 (5.53%)	2.09 GiB (28.31%)	—	—	
AVG.	93 (0.03%)	85 (0.03%)	2.1 MiB (0.03%)	—	—	
9	17 089 (1.93%)	16 225 (18.01%)	1.85 MiB (0.02%)	GET	HTTP/2	/_next/static/chunks/styles.350173a13ad454915e37.js
10	17 026 (1.92%)	16 241 (18.03%)	39.55 MiB (0.36%)	GET	HTTP/2	/_next/static/chunks/4ab9fad2a792c959f6dbadd80e7a97df4866337a.0a836e232ed405b93873.js
11	17 010 (1.92%)	16 193 (17.98%)	147.28 MiB (1.34%)	GET	HTTP/2	/_next/static/chunks/be280f052055141bfd42d205d7fbbfc89d7c18bb.49ff25905e868cd0a5bc.js
12	17 009 (1.92%)	16 189 (17.97%)	117.37 MiB (1.06%)	GET	HTTP/2	/_next/static/chunks/main-6937bb7abbe4219bd650.js
13	16 905 (1.91%)	16 101 (17.88%)	12 MiB (0.11%)	GET	HTTP/2	/_next/static/chunks/webpack-d7b2fb72fb7257504a38.js
14	16 456 (1.86%)	15 690 (17.42%)	1.2 MiB (0.01%)	GET	HTTP/2	/_next/static/7Th_7xghNyv-tf7p6zZQa/_ssgManifest.js
15	16 453 (1.86%)	15 689 (17.42%)	9.84 MiB (0.09%)	GET	HTTP/2	/_next/static/7Th_7xghNyv-tf7p6zZQa/_buildManifest.js
16	16 449 (1.86%)	15 715 (17.45%)	26.68 MiB (0.24%)	GET	HTTP/2	/_next/static/chunks/pages/oevk-finder-afbf8a56fe52fe403808.js

#	HITS	VISITORS	TX. AMOUNT	METHOD	PROTOCOL	DATA
MIN.	1 (0.00%)	1 (0.00%)	—	—	—	
MAX.	17 818 (5.29%)	17 001 (5.53%)	2.09 GiB (28.31%)	—	—	
AVG.	93 (0.03%)	85 (0.03%)	2.1 MiB (0.03%)	—	—	
17	4 872 (0.55%)	2 067 (2.29%)	6.26 MiB (0.06%)	GET	HTTP/1.1	/favicon-196x196.png
18	4 493 (0.51%)	1 165 (1.29%)	556.97 KiB (0.00%)	GET	HTTP/1.1	/favicon-32x32.png
19	3 406 (0.38%)	773 (0.86%)	597.46 KiB (0.01%)	GET	HTTP/1.1	/ringing.mp3
20	1 941 (0.22%)	859 (0.95%)	16.64 KiB (0.00%)	GET	HTTP/1.1	/favicon-16x16.png
21	1 765 (0.20%)	1 113 (1.24%)	169.89 KiB (0.00%)	GET	HTTP/1.1	/apple-touch-icon-152x152.png
22	1 557 (0.18%)	841 (0.93%)	111.74 KiB (0.00%)	GET	HTTP/1.1	/favicon-128x128.png
23	1 413 (0.16%)	784 (0.87%)	147.99 KiB (0.00%)	GET	HTTP/1.1	/favicon-96x96.png
24	1 272 (0.14%)	1 244 (1.38%)	3.6 MiB (0.03%)	GET	HTTP/2	/css/style.css

#	HITS	VISITORS	TX. AMOUNT	METHOD	PROTOCOL	DATA
MIN.	1 (0.00%)	1 (0.00%)	—	—	—	—
MAX.	17 818 (5.29%)	17 001 (5.53%)	2.09 GiB (28.31%)	—	—	—
AVG.	93 (0.03%)	85 (0.03%)	2.1 MiB (0.03%)	—	—	—
TOT.	336 908	307 465	7.39 GiB	—	—	3 612

-
-
-
-

NOT FOUND URLS (404s)

TOP NOT FOUND URLS SORTED BY HITS[,AVGTS,CUMTS,MAXTS,MTHD,PROTO]

Panel Options

GET /robots.txt HTTP/1.1 GET /idopont/el HTTP/1.1 GET /hu/kampanyaink/img/headerbg_white.png HTTP/2 GET /userfiles/ANNEX 1 SWAN membership form WORD sample EN 2018_09_14(1).pdf HTTP/1.1 GET /en/comment/reply/6402 HTTP/1.1 GET /ru/print/1059 HTTP/1.1 GET /ru/print/4050?page=13 HTTP/1.1 GET /ru/printmail/67 HTTP/1.1 GET /en/comment/reply/6470 HTTP/1.1 GET /galeria/esemenyek/csaladi-delelott-szaloky-agival/P1050283.JPG/view?searchterm=None HTTP/1.1 10.04488130180220260310350400HitsVisitorsHitsVisitors

#	HITS	VISITORS	TX. AMOUNT	METHOD	PROTOCOL	DATA
MIN.	1 (0.02%)	—	—	—	—	—
MAX.	431 (8.01%)	—	199.93 KiB (0.42%)	—	—	—
AVG.	1 (0.02%)	—	16.28 KiB (0.03%)	—	—	—
1	431 (0.05%)	0 (0.00%)	199.93 KiB (0.00%)	GET	HTTP/1.1	/robots.txt
2	247 (0.03%)	0 (0.00%)	126.88 KiB (0.00%)	GET	HTTP/1.1	/idopont/elovalasztas2021□
3	164 (0.02%)	0 (0.00%)	118.57 KiB (0.00%)	GET	HTTP/1.1	/apple-touch-icon.png
4	128 (0.01%)	0 (0.00%)	84.51 KiB (0.00%)	GET	HTTP/1.1	/apple-touch-icon-precomposed.png
5	88 (0.01%)	0 (0.00%)	16.26 KiB (0.00%)	GET	HTTP/1.1	/profiles/deanjorgensen/activity
6	86 (0.01%)	0 (0.00%)	12.8 KiB (0.00%)	GET	HTTP/2	/favicon.ico
7	38 (0.00%)	0 (0.00%)	20.12 KiB (0.00%)	GET	HTTP/1.1	/presences/sendlink/obfuscated
8	35 (0.00%)	0 (0.00%)	11.32 KiB (0.00%)	GET	HTTP/2	/robots.txt

#	HITS	VISITORS	TX. AMOUNT	METHOD	PROTOCOL	DATA
MIN.	1 (0.02%)	—	—	—	—	—
MAX.	431 (8.01%)	—	199.93 KiB (0.42%)	—	—	—
AVG.	1 (0.02%)	—	16.28 KiB (0.03%)	—	—	—
9	34 (0.00%)	0 (0.00%)	17.53 KiB (0.00%)	GET	HTTP/1.1	/idopont/elovalasztas2021🔒
10	33 (0.00%)	0 (0.00%)	5.03 KiB (0.00%)	GET	HTTP/1.1	/favicon.ico
11	22 (0.00%)	0 (0.00%)	24.46 KiB (0.00%)	GET	HTTP/1.1	/id
12	21 (0.00%)	0 (0.00%)	8.41 KiB (0.00%)	GET	HTTP/1.0	/robots.txt
13	19 (0.00%)	0 (0.00%)	361 B (0.00%)	GET	HTTP/1.1	/static/main.ecb2bd8cff7ad3980df1.worker.js
14	18 (0.00%)	0 (0.00%)	15.83 KiB (0.00%)	GET	HTTP/1.1	/apple-touch-icon-120x120-precomposed.png
15	17 (0.00%)	0 (0.00%)	8.47 KiB (0.00%)	GET	HTTP/1.1	/idopont/elovalasztas
16	17 (0.00%)	0 (0.00%)	8.73 KiB (0.00%)	GET	HTTP/1.1	/idopont/elovalasztas2021inkabb

#	HITS	VISITORS	TX. AMOUNT	METHOD	PROTOCOL	DATA
MIN.	1 (0.02%)	—	—	—	—	—
MAX.	431 (8.01%)	—	199.93 KiB (0.42%)	—	—	—
AVG.	1 (0.02%)	—	16.28 KiB (0.03%)	—	—	—
17	16 (0.00%)	0 (0.00%)	5.28 KiB (0.00%)	GET	HTTP/1.1	/app-ads.txt
18	16 (0.00%)	0 (0.00%)	2.46 KiB (0.00%)	GET	HTTP/1.1	/
19	16 (0.00%)	0 (0.00%)	7.7 KiB (0.00%)	GET	HTTP/1.1	/koordinátor
20	16 (0.00%)	0 (0.00%)	2.48 KiB (0.00%)	GET	HTTP/1.1	/api/v4/emoji/name/exploding_head
21	15 (0.00%)	0 (0.00%)	7.79 KiB (0.00%)	GET	HTTP/1.1	/idopont/elovalasztas2021regisztrációt
22	15 (0.00%)	0 (0.00%)	8.22 KiB (0.00%)	GET	HTTP/1.1	/idopont/elovalasztas2021x22https://www.facebook.com/ungarpeterlmp/posts/1919523874892897
23	15 (0.00%)	0 (0.00%)	2.32 KiB (0.00%)	GET	HTTP/1.1	/api/v4/emoji/name/face_with_rolling_eyes
24	14 (0.00%)	0 (0.00%)	7.18 KiB (0.00%)	GET	HTTP/1.1	/idopont/elovalasztas2021infók

#	HITS	VISITORS	TX. AMOUNT	METHOD	PROTOCOL	DATA
MIN.	1 (0.02%)	—	—	—	—	—
MAX.	431 (8.01%)	—	199.93 KiB (0.42%)	—	—	—
AVG.	1 (0.02%)	—	16.28 KiB (0.03%)	—	—	—
TOT.	5 380	—	46.51 MiB	—	—	2 926

-
-
-
-

VISITOR:HOSTNAMESANDIPS
 TOP VISITOR:HOSTS SORTED BY HITS[,AVGTS,CUMTS,MAXTS]

Panel Options

172.68.226.168172.68.50.26162.158.93.15172.68.50.62198.41.242.94172.68.226.162172.68.226.220162.158.148.242162.158.90.187172.70.130.320.04.2k8.5k13k17k21k25k30k34k38k0.02304606909201.2k1.4k1.6k1.8k2.1kHitsVisitorsHitsVisitors

#	HITS	VISITORS	TX. AMOUNT	COUNTRY	DATA
MIN.	1 (0.00%)	1 (0.00%)	—	—	—
MAX.	42 448 (4.79%)	2 308 (2.56%)	422.34 MiB (3.83%)	—	—
AVG.	34 (0.00%)	3 (0.00%)	434.68 KiB (0.00%)	—	—
1	42 448 (4.79%)	2 308 (2.56%)	146.48 MiB (1.33%)	HU Hungary	172.68.226.168
2	39 082 (4.41%)	2 075 (2.30%)	149.64 MiB (1.36%)	HU Hungary	172.68.226.170
3	38 399 (4.33%)	2 130 (2.36%)	140.82 MiB (1.28%)	HU Hungary	172.68.226.120
4	37 307 (4.21%)	2 048 (2.27%)	146.31 MiB (1.33%)	HU Hungary	172.68.226.218
5	20 626 (2.33%)	1 464 (1.63%)	92.17 MiB (0.84%)	AT Austria	172.68.50.100
6	18 045 (2.04%)	565 (0.63%)	49.29 MiB (0.45%)	HU Hungary	172.68.226.196
7	13 030 (1.47%)	650 (0.72%)	34.9 MiB (0.32%)	AT Austria	172.68.50.80
8	11 549 (1.30%)	1 031 (1.14%)	37.77 MiB (0.34%)	HU Hungary	172.68.226.216

#	HITS	VISITORS	TX. AMOUNT	COUNTRY	DATA
MIN.	1 (0.00%)	1 (0.00%)	—	—	—
MAX.	42 448 (4.79%)	2 308 (2.56%)	422.34 MiB (3.83%)	—	—
AVG.	34 (0.00%)	3 (0.00%)	434.68 KiB (0.00%)	—	—
9	10 113 (1.14%)	81 (0.09%)	26.98 MiB (0.24%)	HU Hungary	172.68.226.118
10	10 012 (1.13%)	776 (0.86%)	52 MiB (0.47%)	AT Austria	172.68.50.234
11	9 901 (1.12%)	1 285 (1.43%)	22.59 MiB (0.21%)	HU Hungary	172.68.226.184
12	8 728 (0.98%)	622 (0.69%)	28.04 MiB (0.25%)	AT Austria	172.68.50.66
13	8 466 (0.96%)	74 (0.08%)	31.34 MiB (0.28%)	HU Hungary	172.68.226.136
14	7 474 (0.84%)	836 (0.93%)	22.29 MiB (0.20%)	AT Austria	172.68.50.28
15	7 176 (0.81%)	643 (0.71%)	30.17 MiB (0.27%)	AT Austria	172.68.50.88
16	5 368 (0.61%)	821 (0.91%)	1.66 MiB (0.02%)	HU Hungary	172.68.226.172

#	HITS	VISITORS	TX. AMOUNT	COUNTRY	DATA
MIN.	1 (0.00%)	1 (0.00%)	—	—	—
MAX.	42 448 (4.79%)	2 308 (2.56%)	422.34 MiB (3.83%)	—	—
AVG.	34 (0.00%)	3 (0.00%)	434.68 KiB (0.00%)	—	—
17	5 063 (0.57%)	536 (0.60%)	22.86 MiB (0.21%)	HU Hungary	172.68.226.156
18	4 875 (0.55%)	549 (0.61%)	23.39 MiB (0.21%)	HU Hungary	172.68.226.206
19	4 782 (0.54%)	848 (0.94%)	1.26 MiB (0.01%)	HU Hungary	172.68.226.150
20	4 545 (0.51%)	810 (0.90%)	1.33 MiB (0.01%)	HU Hungary	172.68.226.164
21	3 773 (0.43%)	1 (0.00%)	398.17 KiB (0.00%)	IE Ireland	52.50.49.59
22	3 391 (0.38%)	11 (0.01%)	3.71 MiB (0.03%)	DE Germany	162.158.94.120
23	3 011 (0.34%)	743 (0.82%)	2.37 MiB (0.02%)	AT Austria	172.68.50.246
24	2 976 (0.34%)	337 (0.37%)	8.19 MiB (0.07%)	AT Austria	172.68.50.84

#	HITS	VISITORS	TX. AMOUNT	COUNTRY	DATA
MIN.	1 (0.00%)	1 (0.00%)	—	—	—
MAX.	42 448 (4.79%)	2 308 (2.56%)	422.34 MiB (3.83%)	—	—
AVG.	34 (0.00%)	3 (0.00%)	434.68 KiB (0.00%)	—	—
TOT.	886 437	90 068	10.76 GiB	—	25 964

-
-
-
-

OPERATING SYSTEMS
 TOP OPERATING SYSTEMS SORTED BY HITS [,AVGTS,CUMTS,MAXTS]

Panel Options

WindowsAndroidiOSMacintoshUnknownLinuxUnix-likeChrome OSOthers0.041k82k120k160k210k250k290k330k370k0.04.7k9.5k14k19k24k28k33k38k43kHitsVisitorsHitsVisitors

#	HITS	VISITORS	TX. AMOUNT	DATA
MIN.	1 (0.00%)	1 (0.00%)	—	
MAX.	363 225 (40.98%)	15 914 (17.67%)	3.49 GiB (32.41%)	
AVG.	4 616 (0.52%)	469 (0.52%)	57.4 MiB (0.52%)	
1	410 295 (46.29%)	20 564 (22.83%)	4.05 GiB (37.63%)	Windows
2	258 616 (29.17%)	47 242 (52.45%)	3.3 GiB (30.62%)	Android
3	96 321 (10.87%)	12 416 (13.79%)	1.27 GiB (11.83%)	iOS
4	53 486 (6.03%)	5 230 (5.81%)	495.21 MiB (4.49%)	Macintosh
5	49 797 (5.62%)	1 979 (2.20%)	1.38 GiB (12.83%)	Unknown
6	17 061 (1.92%)	2 428 (2.70%)	231.93 MiB (2.10%)	Linux
7	438 (0.05%)	158 (0.18%)	18.72 MiB (0.17%)	Unix-like
8	286 (0.03%)	42 (0.05%)	4.94 MiB (0.04%)	Chrome OS

#	HITS	VISITORS	TX. AMOUNT	DATA
MIN.	1 (0.00%)	1 (0.00%)	—	
MAX.	363 225 (40.98%)	15 914 (17.67%)	3.49 GiB (32.41%)	
AVG.	4 616 (0.52%)	469 (0.52%)	57.4 MiB (0.52%)	
9	137 (0.02%)	9 (0.01%)	30.31 MiB (0.27%)	Others
TOT.	886 437	90 068	10.76 GiB	192

-
-
-
-

BROWSERS
 TOP BROWSERS SORTED BY HITS [, AVGTS, CUMTS, MAXTS]

Panel Options

ChromeFirefoxSafariOthersEdgeUnknownCrawlersOperaMSIE0.056k110k170k220k280k340k390k450k500k0.05.8k12k17k23k29k35k40k46k52kHitsVisitorsHitsVisitors

#	HITS	VISITORS	TX. AMOUNT	DATA
MIN.	1 (0.00%)	1 (0.00%)	—	
MAX.	360 846 (40.71%)	28 620 (31.78%)	3.78 GiB (35.15%)	
AVG.	1 057 (0.12%)	107 (0.12%)	13.15 MiB (0.12%)	
1	559 074 (63.07%)	57 494 (63.83%)	6.04 GiB (56.09%)	Chrome
2	86 337 (9.74%)	6 307 (7.00%)	1003.62 MiB (9.11%)	Firefox
3	83 857 (9.46%)	8 409 (9.34%)	1.09 GiB (10.14%)	Safari
4	57 542 (6.49%)	9 698 (10.77%)	784.4 MiB (7.12%)	Others
5	33 246 (3.75%)	2 078 (2.31%)	343.83 MiB (3.12%)	Edge
6	22 886 (2.58%)	398 (0.44%)	81.19 MiB (0.74%)	Unknown
7	19 639 (2.22%)	1 849 (2.05%)	1.18 GiB (10.92%)	Crawlers
8	17 867 (2.02%)	1 671 (1.86%)	194.58 MiB (1.77%)	Opera

#	HITS	VISITORS	TX. AMOUNT	DATA
MIN.	1 (0.00%)	1 (0.00%)	—	
MAX.	360 846 (40.71%)	28 620 (31.78%)	3.78 GiB (35.15%)	
AVG.	1 057 (0.12%)	107 (0.12%)	13.15 MiB (0.12%)	
9	1 217 (0.14%)	281 (0.31%)	31.15 MiB (0.28%)	MSIE
TOT.	886 437	90 068	10.76 GiB	838

-
-
-
-

TIME DISTRIBUTION
 DATA SORTED BY HOUR [,AVGTS,CUMTS,MAXTS]

Panel Options

00030609121518210.011k21k32k42k53k64k74k85k95k0.01.3k2.6k3.9k5.2k6.5k7.7k9.0k10k12kHitsVisitorsHitsVisitors

#	HITS	VISITORS	TX. AMOUNT	DATA
MIN.	2 632 (0.30%)	555 (0.43%)	44.57 MiB (0.40%)	
MAX.	106 024 (11.96%)	12 909 (9.93%)	1.22 GiB (11.31%)	
AVG.	36 934 (4.17%)	5 414 (4.17%)	459.23 MiB (4.17%)	
1	7 828 (0.88%)	1 513 (1.68%)	101.24 MiB (0.92%)	00
2	4 024 (0.45%)	822 (0.91%)	54.93 MiB (0.50%)	01
3	3 674 (0.41%)	847 (0.94%)	50.66 MiB (0.46%)	02
4	2 632 (0.30%)	555 (0.62%)	44.57 MiB (0.40%)	03
5	3 503 (0.40%)	770 (0.85%)	58.81 MiB (0.53%)	04
6	4 757 (0.54%)	969 (1.08%)	75.66 MiB (0.69%)	05
7	12 520 (1.41%)	2 432 (2.70%)	186.46 MiB (1.69%)	06
8	22 387 (2.53%)	3 425 (3.80%)	309.08 MiB (2.80%)	07

#	HITS	VISITORS	TX. AMOUNT	DATA
MIN.	2 632 (0.30%)	555 (0.43%)	44.57 MiB (0.40%)	
MAX.	106 024 (11.96%)	12 909 (9.93%)	1.22 GiB (11.31%)	
AVG.	36 934 (4.17%)	5 414 (4.17%)	459.23 MiB (4.17%)	
9	33 243 (3.75%)	4 625 (5.14%)	468.72 MiB (4.25%)	08
10	46 489 (5.24%)	6 073 (6.74%)	648.8 MiB (5.89%)	09
11	51 753 (5.84%)	7 636 (8.48%)	862.62 MiB (7.83%)	10
12	53 261 (6.01%)	7 311 (8.12%)	709.13 MiB (6.43%)	11
13	54 648 (6.16%)	7 375 (8.19%)	1001.19 MiB (9.08%)	12
14	53 084 (5.99%)	7 473 (8.30%)	524.1 MiB (4.76%)	13
15	65 909 (7.44%)	10 467 (11.62%)	717.71 MiB (6.51%)	14
16	66 911 (7.55%)	9 601 (10.66%)	694.79 MiB (6.30%)	15

#	HITS	VISITORS	TX. AMOUNT	DATA
MIN.	2 632 (0.30%)	555 (0.43%)	44.57 MiB (0.40%)	
MAX.	106 024 (11.96%)	12 909 (9.93%)	1.22 GiB (11.31%)	
AVG.	36 934 (4.17%)	5 414 (4.17%)	459.23 MiB (4.17%)	
17	79 287 (8.94%)	9 959 (11.06%)	829.92 MiB (7.53%)	16
18	86 117 (9.71%)	10 683 (11.86%)	967.27 MiB (8.78%)	17
19	106 024 (11.96%)	12 909 (14.33%)	1.22 GiB (11.31%)	18
20	68 087 (7.68%)	9 244 (10.26%)	844.96 MiB (7.67%)	19
21	31 196 (3.52%)	5 929 (6.58%)	377.74 MiB (3.43%)	20
22	6 184 (0.70%)	2 810 (3.12%)	64.02 MiB (0.58%)	21
23	11 177 (1.26%)	3 693 (4.10%)	77.2 MiB (0.70%)	22
24	11 742 (1.32%)	2 830 (3.14%)	104.82 MiB (0.95%)	23

#	HITS	VISITORS	TX. AMOUNT	DATA
MIN.	2 632 (0.30%)	555 (0.43%)	44.57 MiB (0.40%)	
MAX.	106 024 (11.96%)	12 909 (9.93%)	1.22 GiB (11.31%)	
AVG.	36 934 (4.17%)	5 414 (4.17%)	459.23 MiB (4.17%)	
TOT.	886 437	129 951	10.76 GiB	24

-
-
-
-

REFERRING SITES
 TOP REFERRING SITES SORTED BY HITS[, AVGT, CUMTS, MAXTS]

Panel Options

dev.szavazas.eleve.huchat.eleve.huwww.reddit.comt.coxn--elvaszts-21af05k.humyactivity.google.comferencjozsef.ezalenyeg.huszolnok.ezalenyeg.huhirsztar.huwww.penzcentrum.hu0.032k64k96k130k160k190k220k260k290k0.03.2k6.4k9.6k13k16k19k22k26k29kHitsVisitorsHitsVisit
 ors

#	HITS	VISITORS	TX. AMOUNT	DATA
MIN.	1 (0.00%)	1 (0.00%)	—	
MAX.	321 338 (57.42%)	31 923 (33.37%)	6.28 GiB (75.01%)	
AVG.	1 929 (0.34%)	329 (0.34%)	29.55 MiB (0.34%)	
1	321 338 (36.25%)	22 753 (25.26%)	6.28 GiB (58.32%)	dev.szavazas.eleve.hu
2	69 811 (7.88%)	642 (0.71%)	169.33 MiB (1.54%)	eleve.hu
3	59 069 (6.66%)	31 923 (35.44%)	477.42 MiB (4.33%)	elovalasztas.hu
4	40 846 (4.61%)	12 432 (13.80%)	119.83 MiB (1.09%)	szavazas.eleve.hu
5	17 945 (2.02%)	7 929 (8.80%)	137.69 MiB (1.25%)	elovalasztas2021.hu
6	9 943 (1.12%)	161 (0.18%)	251.13 MiB (2.28%)	nyitottakvagyunk.hu
7	7 434 (0.84%)	1 252 (1.39%)	379.07 MiB (3.44%)	tamogass.ahang.hu
8	5 963 (0.67%)	4 789 (5.32%)	40.05 MiB (0.36%)	m.facebook.com

#	HITS	VISITORS	TX. AMOUNT	DATA
MIN.	1 (0.00%)	1 (0.00%)	—	
MAX.	321 338 (57.42%)	31 923 (33.37%)	6.28 GiB (75.01%)	
AVG.	1 929 (0.34%)	329 (0.34%)	29.55 MiB (0.34%)	
9	3 343 (0.38%)	1 350 (1.50%)	23.96 MiB (0.22%)	l.facebook.com
10	3 189 (0.36%)	2 230 (2.48%)	65.23 MiB (0.59%)	www.google.com
11	2 828 (0.32%)	2 449 (2.72%)	19.89 MiB (0.18%)	lm.facebook.com
12	2 605 (0.29%)	141 (0.16%)	9.7 MiB (0.09%)	sator.eleve.hu
13	1 724 (0.19%)	1 291 (1.43%)	9.1 MiB (0.08%)	com.google.android.gm
14	1 586 (0.18%)	85 (0.09%)	229.36 MiB (2.08%)	nohastudio.hu
15	1 189 (0.13%)	94 (0.10%)	79.5 MiB (0.72%)	swannet.org
16	995 (0.11%)	694 (0.77%)	10.35 MiB (0.09%)	momentum.hu

#	HITS	VISITORS	TX. AMOUNT	DATA
MIN.	1 (0.00%)	1 (0.00%)	—	
MAX.	321 338 (57.42%)	31 923 (33.37%)	6.28 GiB (75.01%)	
AVG.	1 929 (0.34%)	329 (0.34%)	29.55 MiB (0.34%)	
17	955 (0.11%)	27 (0.03%)	40.12 MiB (0.36%)	ma-puppetry.eu
18	889 (0.10%)	700 (0.78%)	3.96 MiB (0.04%)	ahang.hu
19	713 (0.08%)	137 (0.15%)	2.77 MiB (0.03%)	terkep.eleve.hu
20	584 (0.07%)	377 (0.42%)	6.11 MiB (0.06%)	www.google.hu
21	494 (0.06%)	3 (0.00%)	10.75 MiB (0.10%)	korbe.hu
22	423 (0.05%)	5 (0.01%)	2.28 MiB (0.02%)	metabase.tamogass.ahang.hu
23	391 (0.04%)	305 (0.34%)	3.64 MiB (0.03%)	www.youtube.com
24	338 (0.04%)	311 (0.35%)	3.35 MiB (0.03%)	youtube.com

#	HITS	VISITORS	TX. AMOUNT	DATA
MIN.	1 (0.00%)	1 (0.00%)	—	
MAX.	321 338 (57.42%)	31 923 (33.37%)	6.28 GiB (75.01%)	
AVG.	1 929 (0.34%)	329 (0.34%)	29.55 MiB (0.34%)	
TOT.	559 607	95 662	8.37 GiB	290

-
-
-
-

HTTPSTATUSCODES
 TOP HTTP STATUS CODES SORTED BY HITS [,AVGTS,CUMTS,MAXTS]

Panel Options

2xx Success3xx Redirection1xx Informational4xx Client Errors5xx Server Errors0.077k150k230k310k390k460k540k620k690k0.07.2k14k22k29k36k43k51k58k65kHitsVisitorsHitsVisitors

#	HITS	VISITORS	TX. AMOUNT	DATA
MIN.	1 (0.00%)	1 (0.00%)	—	
MAX.	770 492 (86.92%)	72 228 (69.84%)	10.57 GiB (98.22%)	
AVG.	36 934 (4.17%)	4 309 (4.17%)	459.23 MiB (4.17%)	
1	771 181 (87.00%)	72 368 (80.35%)	10.57 GiB (98.24%)	2xx Success
2	72 871 (8.22%)	27 435 (30.46%)	1.96 MiB (0.02%)	3xx Redirection
3	25 425 (2.87%)	2 980 (3.31%)	142.93 MiB (1.30%)	1xx Informational
4	14 636 (1.65%)	0 (0.00%)	47.95 MiB (0.44%)	4xx Client Errors
5	2 324 (0.26%)	634 (0.70%)	1.21 MiB (0.01%)	5xx Server Errors
TOT.	886 437	103 417	10.76 GiB	24

-
-
-
-

GEO LOCATION

CONTINENT>COUNTRY SORTED BY UNIQUE HITS [,AVGTS,CUMTS,MAXTS]

Panel Options

EU EuropeNA North AmericaAS AsiaAF AfricaOC OceaniaSA South America0.086k170k260k340k430k520k600k690k780k0.08.3k17k25k33k42k50k58k67k75kHitsVisitorsHitsVisitors

#	HITS	VISITORS	TX. AMOUNT	DATA
MIN.	1 (0.00%)	1 (0.00%)	166 B (0.00%)	
MAX.	589 611 (66.51%)	36 473 (40.50%)	7.49 GiB (69.59%)	
AVG.	8 207 (0.93%)	833 (0.92%)	102.05 MiB (0.93%)	
1	861 199 (97.15%)	83 283 (92.47%)	9.72 GiB (90.32%)	EU Europe
2	18 281 (2.06%)	4 896 (5.44%)	812.61 MiB (7.37%)	NA North America
3	4 293 (0.48%)	1 439 (1.60%)	191.62 MiB (1.74%)	AS Asia
4	1 616 (0.18%)	84 (0.09%)	38.62 MiB (0.35%)	AF Africa
5	681 (0.08%)	287 (0.32%)	10.74 MiB (0.10%)	OC Oceania
6	367 (0.04%)	78 (0.09%)	13.2 MiB (0.12%)	SA South America
TOT.	886 437	90 067	10.76 GiB	108

Az összes kérés elemzése 2021.09.18.

UNIQUE VISITORS PER DAY - INCLUDING SPIDERS
HITS HAVING THE SAME IP, DATE AND AGENT ARE A UNIQUE VISIT.

Panel Options

18/Sep/2021 0.03.1k6.2k9.2k12k15k18k22k25k28k0.04108201.2k1.6k2.0k2.4k2.9k3.3k3.7k HitsVisitorsHitsVisitors

#	HITS	VISITORS	TX. AMOUNT	DATA
MIN.	30 780 (100.00%)	4 075 (100.00%)	1.67 GiB (100.00%)	
MAX.	30 780 (100.00%)	4 075 (100.00%)	1.67 GiB (100.00%)	
AVG.	30 780 (100.00%)	4 075 (100.00%)	1.67 GiB (100.00%)	
1	30 780 (100.00%)	4 075 (100.00%)	1.67 GiB (100.00%)	18/Sep/2021
TOT.	30 780	4 075	1.67 GiB	1

-
-
-
-

REQUESTED FILES (URLS)
TOP REQUESTS SORTED BY HITS [, AVGTS, CUMTS, MAXTS, MTHD, PROTO]

Panel Options

POST /wp-login.php HTTP/1.1 GET /wp-content/plugins/elementor/assets/lib/font-awesome/css/fontawesome.min.css?ver=5.12.0 HTTP/2 GET /js/resources/css/textboxio.css?version=2.3.0.46 HTTP/2 GET /wp-content/plugins/elementor/assets/lib/font-awesome/css/fontawesome.min.css?ver=5.9.0 HTTP/2 GET /.well-known/acme-challenge/kA6iQdfZmEzKbsTzJNDZZ-gINDh3Y7kndnVgwMCQiw HTTP/1.1 POST /process-

payment?paymentId=29ab796a1318ec119988001dd8b71cf3 HTTP/1.1GET /process-payment?paymentId=24ab796a1318ec119988001dd8b71cf3 HTTP/1.1GET /process-payment?paymentId=6e3e317d1318ec119988001dd8b71cf3 HTTP/1.1GET /api/collection/root HTTP/2POST /api/card/79/query HTTP/20.0851702603404305106006807700.071140210280360430500570640HitsVisitorsHitsVisitors

#	HITS	VISITORS	TX. AMOUNT	METHOD	PROTOCOL	DATA
MIN.	1 (0.01%)	1 (0.01%)	—	—	—	—
MAX.	844 (5.02%)	704 (5.72%)	42.18 MiB (4.27%)	—	—	—
AVG.	3 (0.02%)	2 (0.02%)	200.02 KiB (0.02%)	—	—	—
1	844 (2.74%)	704 (17.28%)	1.79 MiB (0.10%)	POST	HTTP/1.1	/wp-login.php
2	715 (2.32%)	584 (14.33%)	2.69 MiB (0.16%)	GET	HTTP/2	/elovalasztas?utm_medium=iframe&utm_source=elovalasztas-hu&utm_campaign=landingpage
3	683 (2.22%)	643 (15.78%)	3.67 MiB (0.21%)	GET	HTTP/2	?utm_source=ahang&utm_medium=email&utm_campaign=blast2021-09-18
4	644 (2.09%)	324 (7.95%)	38.76 MiB (2.26%)	GET	HTTP/1.1	/
5	464 (1.51%)	9 (0.22%)	10.14 MiB (0.59%)	GET	HTTP/1.1	/ru/опубликован-список-терминов-о-лидерс/
6	366 (1.19%)	252 (6.18%)	925.56 KiB (0.05%)	GET	HTTP/1.1	/wp-login.php
7	289 (0.94%)	258 (6.33%)	1.98 MiB (0.12%)	POST	HTTP/2	/start

#	HITS	VISITORS	TX. AMOUNT	METHOD	PROTOCOL	DATA
MIN.	1 (0.01%)	1 (0.01%)	—	—	—	
MAX.	844 (5.02%)	704 (5.72%)	42.18 MiB (4.27%)	—	—	
AVG.	3 (0.02%)	2 (0.02%)	200.02 KiB (0.02%)	—	—	
8	284 (0.92%)	173 (4.25%)	112.57 KiB (0.01%)	POST	HTTP/1.1	/xmlrpc.php
9	164 (0.53%)	119 (2.92%)	25.66 MiB (1.50%)	GET	HTTP/2	/
10	146 (0.47%)	146 (3.58%)	3.71 KiB (0.00%)	GET	HTTP/2	/cookie-accepted
11	127 (0.41%)	1 (0.02%)	186 B (0.00%)	POST	HTTP/1.1	/hooks/jen86md3o7fjb8wmi58769tm3c
12	111 (0.36%)	5 (0.12%)	2.42 MiB (0.14%)	GET	HTTP/1.1	/ru/опубликован-список-терминов-о-лидерс/?>
13	94 (0.31%)	3 (0.07%)	220.02 KiB (0.01%)	GET	HTTP/1.1	/hu/kozosseg-tagok/
14	91 (0.30%)	40 (0.98%)	1.56 MiB (0.09%)	GET	HTTP/1.1	/en/
15	88 (0.29%)	5 (0.12%)	1.58 MiB (0.09%)	GET	HTTP/1.1	/news/

#	HITS	VISITORS	TX. AMOUNT	METHOD	PROTOCOL	DATA
MIN.	1 (0.01%)	1 (0.01%)	—	—	—	—
MAX.	844 (5.02%)	704 (5.72%)	42.18 MiB (4.27%)	—	—	—
AVG.	3 (0.02%)	2 (0.02%)	200.02 KiB (0.02%)	—	—	—
16	82 (0.27%)	76 (1.87%)	941.24 KiB (0.05%)	GET	HTTP/2	/wp-content/plugins/elementor/assets/lib/waypoints/waypoints.min.js?ver=4.0.2
17	70 (0.23%)	64 (1.57%)	13.34 MiB (0.78%)	GET	HTTP/2	/wp-content/plugins/elementor-pro/assets/css/frontend.min.css?ver=2.8.5
18	69 (0.22%)	64 (1.57%)	1.05 MiB (0.06%)	GET	HTTP/2	/wp-content/plugins/elementor/assets/lib/eicons/css/elementor-icons.min.css?ver=5.6.2
19	66 (0.21%)	62 (1.52%)	7.81 MiB (0.46%)	GET	HTTP/2	/wp-content/plugins/elementor-pro/assets/js/frontend.min.js?ver=2.8.5
20	66 (0.21%)	62 (1.52%)	8.76 MiB (0.51%)	GET	HTTP/2	/wp-content/plugins/elementor/assets/lib/swiper/swiper.min.js?ver=5.3.6
21	65 (0.21%)	64 (1.57%)	33.32 KiB (0.00%)	GET	HTTP/1.1	/profiles/deanjorgensen/activity
22	63 (0.20%)	60 (1.47%)	405.75 KiB (0.02%)	GET	HTTP/2	/wp-content/plugins/elementor-pro/assets/lib/sticky/jquery.sticky.min.js?ver=2.8.5
23	62 (0.20%)	59 (1.45%)	647.55 KiB (0.04%)	GET	HTTP/2	/wp-content/plugins/elementor/assets/lib/dialog/dialog.min.js?ver=4.7.6

#	HITS	VISITORS	TX. AMOUNT	METHOD	PROTOCOL	DATA
MIN.	1 (0.01%)	1 (0.01%)	—	—	—	—
MAX.	844 (5.02%)	704 (5.72%)	42.18 MiB (4.27%)	—	—	—
AVG.	3 (0.02%)	2 (0.02%)	200.02 KiB (0.02%)	—	—	—
24	61 (0.20%)	61 (1.50%)	5.54 MiB (0.32%)	GET	HTTP/2	/wp-includes/js/jquery/jquery.js?ver=1.12.4-wp
TOT.	16 810	12 299	986.84 MiB	—	—	5 052

-
-
-
-

STATICREQUESTS
TOP STATICREQUESTS SORTED BY HITS[,AVGTS,CUMITS,MAXTS,MTHD,PROTO]

Panel Options

GET /css/style.css HTTP/2GET /css/fonts.css HTTP/2GET /wp-content/uploads/2020/09/swan-slider.jpg HTTP/2GET /files/swannet/ версия на русском_0.pdf HTTP/1.1GET /kepek/image_7364136331131557862570442.jpeg HTTP/2GET /wp-content/uploads/2019/09/New-Espell.png HTTP/2GET /kepek/image_8471418052661580403192826.jpeg HTTP/1.1GET /images/resource/modul_alap.jpg HTTP/2GET /vue.js HTTP/2GET /apple-icon-72x72.png HTTP/1.10.01302704005406708009401.1k1.2k0.01302603905206507709001.0k1.2kHitsVisitorsHitsVisitors

#	HITS	VISITORS	TX. AMOUNT	METHOD	PROTOCOL	DATA
MIN.	1 (0.01%)	1 (0.01%)	—	—	—	
MAX.	1 337 (12.08%)	1 287 (12.24%)	195.97 MiB (28.95%)	—	—	
AVG.	12 (0.11%)	12 (0.11%)	807.8 KiB (0.12%)	—	—	
1	1 337 (4.34%)	1 287 (31.58%)	2.59 MiB (0.15%)	GET	HTTP/2	/css/style.css
2	1 337 (4.34%)	1 287 (31.58%)	195.97 MiB (11.43%)	GET	HTTP/2	/css/bootstrap.min.css
3	1 312 (4.26%)	1 281 (31.44%)	86.09 MiB (5.02%)	GET	HTTP/2	/js/jquery-3.3.1.slim.min.js
4	1 307 (4.25%)	1 277 (31.34%)	71.09 MiB (4.15%)	GET	HTTP/2	/js/bootstrap.min.js
5	1 299 (4.22%)	1 268 (31.12%)	25.37 MiB (1.48%)	GET	HTTP/2	/js/popper.min.js
6	1 289 (4.19%)	1 251 (30.70%)	29.83 MiB (1.74%)	GET	HTTP/2	/img/barion-card-strip-intl.svg
7	233 (0.76%)	138 (3.39%)	90.88 KiB (0.01%)	GET	HTTP/1.1	/robots.txt
8	92 (0.30%)	76 (1.87%)	1.07 MiB (0.06%)	GET	HTTP/1.1	/wp-content/uploads/2019/09/New-AMC.png

#	HITS	VISITORS	TX. AMOUNT	METHOD	PROTOCOL	DATA
MIN.	1 (0.01%)	1 (0.01%)	—	—	—	
MAX.	1 337 (12.08%)	1 287 (12.24%)	195.97 MiB (28.95%)	—	—	
AVG.	12 (0.11%)	12 (0.11%)	807.8 KiB (0.12%)	—	—	
9	60 (0.19%)	53 (1.30%)	704.31 KiB (0.04%)	GET	HTTP/2	/wp-content/uploads/2019/09/New-AMC.png
10	52 (0.17%)	50 (1.23%)	3.63 MiB (0.21%)	GET	HTTP/2	/wp-content/plugins/elementor/assets/lib/font-awesome/webfonts/fa-solid-900.woff2
11	42 (0.14%)	40 (0.98%)	253.63 KiB (0.01%)	GET	HTTP/2	/wp-content/themes/wao2018/img/wao-logo_2_en.png
12	42 (0.14%)	35 (0.86%)	1.61 MiB (0.09%)	GET	HTTP/2	/wp-content/uploads/2019/09/hero_image_09.20-01-1600x604.jpg
13	40 (0.13%)	39 (0.96%)	712.27 KiB (0.04%)	GET	HTTP/2	/wp-content/themes/wao2018/img/wao-logo_2_hu.png
14	40 (0.13%)	39 (0.96%)	499.84 KiB (0.03%)	GET	HTTP/2	/wp-content/themes/wao2018/SwissBold.woff2
15	40 (0.13%)	38 (0.93%)	16.63 KiB (0.00%)	GET	HTTP/2	/wp-content/themes/wao2018/img/fb.svg
16	40 (0.13%)	40 (0.98%)	8.08 MiB (0.47%)	GET	HTTP/2	/wp-content/uploads/2019/06/hero_image_3.2-01-2.jpg

#	HITS	VISITORS	TX. AMOUNT	METHOD	PROTOCOL	DATA
MIN.	1 (0.01%)	1 (0.01%)	—	—	—	
MAX.	1 337 (12.08%)	1 287 (12.24%)	195.97 MiB (28.95%)	—	—	
AVG.	12 (0.11%)	12 (0.11%)	807.8 KiB (0.12%)	—	—	
17	39 (0.13%)	37 (0.91%)	128.06 KiB (0.01%)	GET	HTTP/2	/wp-content/themes/wao2018/img/in.png
18	39 (0.13%)	37 (0.91%)	446.13 KiB (0.03%)	GET	HTTP/2	/wp-content/themes/wao2018/img/insta.png
19	38 (0.12%)	36 (0.88%)	1.7 KiB (0.00%)	GET	HTTP/2	/wp-content/plugins/a3-lazy-load/assets/images/lazy_placeholder.gif
20	34 (0.11%)	33 (0.81%)	5.4 KiB (0.00%)	GET	HTTP/2	/wp-content/themes/wao2018/img/headerbg.png
21	33 (0.11%)	33 (0.81%)	424.44 KiB (0.02%)	GET	HTTP/2	/wp-content/plugins/elementor/assets/lib/font-awesome/webfonts/fa-regular-400.woff2
22	33 (0.11%)	33 (0.81%)	27.4 KiB (0.00%)	GET	HTTP/2	/wp-content/themes/wao2018/img/headerbg_white.png
23	33 (0.11%)	33 (0.81%)	1.79 MiB (0.10%)	GET	HTTP/1.1	/js/bootstrap.min.js
24	33 (0.11%)	26 (0.64%)	343.94 KiB (0.02%)	GET	HTTP/2	/favicon.ico

#	HITS	VISITORS	TX. AMOUNT	METHOD	PROTOCOL	DATA
MIN.	1 (0.01%)	1 (0.01%)	—	—	—	—
MAX.	1 337 (12.08%)	1 287 (12.24%)	195.97 MiB (28.95%)	—	—	—
AVG.	12 (0.11%)	12 (0.11%)	807.8 KiB (0.12%)	—	—	—
TOT.	11 072	10 517	676.85 MiB	—	—	858

-
-
-
-

NOT FOUND URLS (404S)
TOP NOT FOUND URLS SORTED BY HITS[, AVGTS, CUMTS, MAXTS, MTHD, PROTO]

Panel Options

GET /robots.txt HTTP/1.1GET /ru/comment/reply/6339 HTTP/1.1GET /en/node/1695 HTTP/1.1GET /ru/node/1859 HTTP/1.1GET /ru/taxonomy/term/255/all/feed HTTP/1.1GET /en/content/swan-vacancy-advocacy-officer HTTP/1.1GET /ru/Члены/фонд-здоровья-и-общественного-развития HTTP/1.1GET /ru/taxonomy/term/98/<?> HTTP/1.1GET /ru/node/6245 HTTP/1.1GET /ru/node/634 HTTP/1.10.023466992120140160180210HitsVisitorsHitsVisitors

#	HITS	VISITORS	TX. AMOUNT	METHOD	PROTOCOL	DATA
MIN.	1 (0.03%)	—	—	—	—	—
MAX.	229 (7.90%)	—	739.76 KiB (1.43%)	—	—	—
AVG.	1 (0.03%)	—	27.62 KiB (0.05%)	—	—	—
1	229 (0.74%)	0 (0.00%)	154.44 KiB (0.01%)	GET	HTTP/1.1	/robots.txt
2	52 (0.17%)	0 (0.00%)	7.48 KiB (0.00%)	GET	HTTP/2	/favicon.ico
3	29 (0.09%)	0 (0.00%)	5.47 KiB (0.00%)	GET	HTTP/1.1	/profiles/deanjorgensen/activity
4	28 (0.09%)	0 (0.00%)	127.84 KiB (0.01%)	GET	HTTP/2	/robots.txt
5	25 (0.08%)	0 (0.00%)	168.56 KiB (0.01%)	GET	HTTP/1.1	/.env
6	24 (0.08%)	0 (0.00%)	3.83 KiB (0.00%)	GET	HTTP/1.0	/robots.txt
7	19 (0.06%)	0 (0.00%)	2.52 KiB (0.00%)	GET	HTTP/1.1	/wp-content/
8	14 (0.05%)	0 (0.00%)	2.12 KiB (0.00%)	GET	HTTP/1.1	/favicon.ico

#	HITS	VISITORS	TX. AMOUNT	METHOD	PROTOCOL	DATA
MIN.	1 (0.03%)	—	—	—	—	—
MAX.	229 (7.90%)	—	739.76 KiB (1.43%)	—	—	—
AVG.	1 (0.03%)	—	27.62 KiB (0.05%)	—	—	—
9	7 (0.02%)	0 (0.00%)	2.31 KiB (0.00%)	GET	HTTP/2	/apple-touch-icon-precomposed.png
10	6 (0.02%)	0 (0.00%)	75.98 KiB (0.00%)	GET	HTTP/1.1	/wp-content/plugins/wp-automatic/wp-pinterest-automatic
11	6 (0.02%)	0 (0.00%)	642 B (0.00%)	GET	HTTP/2	/apple-touch-icon.png
12	6 (0.02%)	0 (0.00%)	106.04 KiB (0.01%)	GET	HTTP/1.1	/ru/taxonomy/term/231/<?>
13	6 (0.02%)	0 (0.00%)	106.04 KiB (0.01%)	GET	HTTP/1.1	/ru/taxonomy/term/88/<?>
14	6 (0.02%)	0 (0.00%)	30.05 KiB (0.00%)	GET	HTTP/1.1	/process-payment?paymentId=6cd0f51dc318ec119988001dd8b71cf3
15	5 (0.02%)	0 (0.00%)	1.45 KiB (0.00%)	GET	HTTP/1.1	/wp-login.php
16	5 (0.02%)	0 (0.00%)	680 B (0.00%)	GET	HTTP/1.1	/config/getuser?index=0

#	HITS	VISITORS	TX. AMOUNT	METHOD	PROTOCOL	DATA
MIN.	1 (0.03%)	—	—	—	—	—
MAX.	229 (7.90%)	—	739.76 KiB (1.43%)	—	—	—
AVG.	1 (0.03%)	—	27.62 KiB (0.05%)	—	—	—
17	5 (0.02%)	0 (0.00%)	88.36 KiB (0.01%)	GET	HTTP/1.1	/ru/taxonomy/term/89/<?>
18	4 (0.01%)	0 (0.00%)	66.67 KiB (0.00%)	GET	HTTP/1.1	/node/1379
19	4 (0.01%)	0 (0.00%)	16.26 KiB (0.00%)	GET	HTTP/1.0	/contact-info/
20	4 (0.01%)	0 (0.00%)	66.67 KiB (0.00%)	GET	HTTP/1.1	/en/content/brothel-“protectors”-were-exposed-department-ukrainian-ministry-interior
21	4 (0.01%)	0 (0.00%)	66.67 KiB (0.00%)	GET	HTTP/1.1	/en/content/lgbti-and-sex-workers-rights-activist-kemal-ördek-was-raped-and-assaulted-their-home
22	4 (0.01%)	0 (0.00%)	66.67 KiB (0.00%)	GET	HTTP/1.1	/en/content/make-or-break-year-hiv-prevention-bulgaria-“goodwill”-campaign
23	4 (0.01%)	0 (0.00%)	70.69 KiB (0.00%)	GET	HTTP/1.1	/ru/Члены/са-одиссей
24	4 (0.01%)	0 (0.00%)	70.69 KiB (0.00%)	GET	HTTP/1.1	/ru/Члены/всеукраинская-лига-«легалайф»

#	HITS	VISITORS	TX. AMOUNT	METHOD	PROTOCOL	DATA
MIN.	1 (0.03%)	—	—	—	—	—
MAX.	229 (7.90%)	—	739.76 KiB (1.43%)	—	—	—
AVG.	1 (0.03%)	—	27.62 KiB (0.05%)	—	—	—
TOT.	2 898	—	50.63 MiB	—	—	1 877

-
-
-
-

VISITOR HOSTNAMES AND IPS

TOP VISITOR HOSTS SORTED BY [HITS, AVGTS, CUMTS, MAXTS]

Panel Options

52.169.80.5537.76.82.109134.255.105.140193.148.19.3923.228.109.14766.249.69.22566.249.88.252185.191.171.3891.104.210.24884.225.182.880.01402804205607108509901.1k1.3k0.02.04.06.08.010HitsVisitors
HitsVisitors

#	HITS	VISITORS	TX. AMOUNT	COUNTRY	DATA
MIN.	1 (0.00%)	1 (0.02%)	—		—
MAX.	1 407 (4.57%)	11 (0.27%)	487.08 MiB (28.41%)		—
AVG.	8 (0.03%)	1 (0.02%)	462.82 KiB (0.03%)		—
1	1 407 (4.57%)	1 (0.02%)	2.7 MiB (0.16%)	IE Ireland	52.169.80.55
2	712 (2.31%)	1 (0.02%)	10.16 MiB (0.59%)	DE Germany	95.91.42.9
3	657 (2.13%)	1 (0.02%)	5.92 MiB (0.35%)	DE Germany	164.68.111.45
4	632 (2.05%)	1 (0.02%)	4.98 MiB (0.29%)	CA Canada	192.99.160.200
5	601 (1.95%)	1 (0.02%)	5.23 MiB (0.30%)	CA Canada	192.99.161.45
6	578 (1.88%)	1 (0.02%)	5.14 MiB (0.30%)	DE Germany	5.9.156.20
7	496 (1.61%)	1 (0.02%)	3.34 MiB (0.19%)	CA Canada	167.114.101.65
8	305 (0.99%)	1 (0.02%)	2.87 MiB (0.17%)	DE Germany	207.180.245.134

#	HITS	VISITORS	TX. AMOUNT	COUNTRY	DATA
MIN.	1 (0.00%)	1 (0.02%)	—		—
MAX.	1 407 (4.57%)	11 (0.27%)	487.08 MiB (28.41%)		—
AVG.	8 (0.03%)	1 (0.02%)	462.82 KiB (0.03%)		—
9	301 (0.98%)	1 (0.02%)	487.08 MiB (28.41%)	DE Germany	148.251.9.145
10	257 (0.83%)	3 (0.07%)	2.07 MiB (0.12%)	HU Hungary	5.204.83.177
11	240 (0.78%)	1 (0.02%)	1.51 MiB (0.09%)	CA Canada	167.114.211.237
12	221 (0.72%)	1 (0.02%)	2.78 MiB (0.16%)	DE Germany	148.251.244.137
13	200 (0.65%)	1 (0.02%)	1.37 MiB (0.08%)	DE Germany	144.76.40.222
14	179 (0.58%)	1 (0.02%)	6.31 MiB (0.37%)	US United States	216.244.66.250
15	153 (0.50%)	1 (0.02%)	4.46 MiB (0.26%)	DE Germany	5.9.154.68
16	152 (0.49%)	1 (0.02%)	4.19 MiB (0.24%)	HU Hungary	94.44.243.74

#	HITS	VISITORS	TX. AMOUNT	COUNTRY	DATA
MIN.	1 (0.00%)	1 (0.02%)	—		—
MAX.	1 407 (4.57%)	11 (0.27%)	487.08 MiB (28.41%)		—
AVG.	8 (0.03%)	1 (0.02%)	462.82 KiB (0.03%)		—
17	144 (0.47%)	1 (0.02%)	14.66 MiB (0.86%)	US United States	98.26.13.104
18	143 (0.46%)	1 (0.02%)	3.71 MiB (0.22%)	HU Hungary	91.82.213.25
19	129 (0.42%)	2 (0.05%)	7.31 MiB (0.43%)	CN China	180.163.220.68
20	127 (0.41%)	1 (0.02%)	186 B (0.00%)	Unknown	10.0.0.129
21	122 (0.40%)	1 (0.02%)	1.22 MiB (0.07%)	DE Germany	144.76.137.254
22	122 (0.40%)	0 (0.00%)	67.2 KiB (0.00%)	ID Indonesia	114.7.131.90
23	104 (0.34%)	2 (0.05%)	53.58 KiB (0.00%)	HU Hungary	134.255.66.179
24	102 (0.33%)	5 (0.12%)	2.18 MiB (0.13%)	HU Hungary	188.36.223.207

#	HITS	VISITORS	TX. AMOUNT	COUNTRY	DATA
MIN.	1 (0.00%)	1 (0.02%)	—	—	—
MAX.	1 407 (4.57%)	11 (0.27%)	487.08 MiB (28.41%)	—	—
AVG.	8 (0.03%)	1 (0.02%)	462.82 KiB (0.03%)	—	—
TOT.	30 780	4 075	1.67 GiB	—	3 793

-
-
-
-

OPERATING SYSTEMS

TOP OPERATING SYSTEMS SORTED BY HITS [, AVGTS, CUMTS, MAXTS]

Panel Options

UnknownAndroidWindowsiOSLinuxMacintoshUnix-likeChrome OSDarwin0.09501.9k2.9k3.8k4.8k5.7k6.7k7.6k8.6k0.01503004506007508901.0k1.2k1.3kHitsVisitorsHitsVisitors

#	HITS	VISITORS	TX. AMOUNT	DATA
MIN.	1 (0.00%)	1 (0.02%)	5 B (0.00%)	
MAX.	9 499 (30.86%)	823 (20.20%)	791.88 MiB (46.19%)	
AVG.	362 (1.18%)	47 (1.15%)	20.17 MiB (1.18%)	
1	9 499 (30.86%)	704 (17.28%)	791.88 MiB (46.19%)	Unknown
2	8 573 (27.85%)	897 (22.01%)	380.34 MiB (22.19%)	Android
3	7 269 (23.62%)	1 482 (36.37%)	305.59 MiB (17.83%)	Windows
4	2 250 (7.31%)	238 (5.84%)	127.4 MiB (7.43%)	iOS
5	1 648 (5.35%)	422 (10.36%)	36.17 MiB (2.11%)	Linux
6	1 330 (4.32%)	241 (5.91%)	57.74 MiB (3.37%)	Macintosh
7	198 (0.64%)	89 (2.18%)	14.86 MiB (0.87%)	Unix-like
8	11 (0.04%)	1 (0.02%)	340.36 KiB (0.02%)	Chrome OS

#	HITS	VISITORS	TX. AMOUNT	DATA
MIN.	1 (0.00%)	1 (0.02%)	5 B (0.00%)	
MAX.	9 499 (30.86%)	823 (20.20%)	791.88 MiB (46.19%)	
AVG.	362 (1.18%)	47 (1.15%)	20.17 MiB (1.18%)	
9	2 (0.01%)	1 (0.02%)	5 B (0.00%)	Darwin
TOT.	30 780	4 075	1.67 GiB	85

-
-
-
-

BROWSERS
TOP BROWSERS SORTED BY HITS [, AVGTS, CUMITS, MAXTS]

Panel Options

ChromeCrawlersFirefoxSafariUnknownOthersEdgeOperaMSIEYandex.Brows0.01.2k2.4k3.6k4.7k5.9k7.1k8.3k9.5k11k0.01903805807709601.2k1.3k1.5k1.7kHitsVisitorsHitsVisitors

#	HITS	VISITORS	TX. AMOUNT	DATA
MIN.	1 (0.00%)	1 (0.02%)	—	
MAX.	6 091 (19.79%)	679 (16.66%)	676.77 MiB (39.48%)	
AVG.	77 (0.25%)	10 (0.25%)	4.31 MiB (0.25%)	
1	11 855 (38.52%)	1 917 (47.04%)	556.9 MiB (32.49%)	Chrome
2	9 034 (29.35%)	719 (17.64%)	826.76 MiB (48.23%)	Crawlers
3	2 822 (9.17%)	531 (13.03%)	74.22 MiB (4.33%)	Firefox
4	2 331 (7.57%)	307 (7.53%)	134.17 MiB (7.83%)	Safari
5	1 820 (5.91%)	113 (2.77%)	15.34 MiB (0.89%)	Unknown
6	1 597 (5.19%)	267 (6.55%)	68.57 MiB (4.00%)	Others
7	590 (1.92%)	91 (2.23%)	22.24 MiB (1.30%)	Edge
8	508 (1.65%)	60 (1.47%)	12.63 MiB (0.74%)	Opera

#	HITS	VISITORS	TX. AMOUNT	DATA
MIN.	1 (0.00%)	1 (0.02%)	—	
MAX.	6 091 (19.79%)	679 (16.66%)	676.77 MiB (39.48%)	
AVG.	77 (0.25%)	10 (0.25%)	4.31 MiB (0.25%)	
9	185 (0.60%)	37 (0.91%)	2.67 MiB (0.16%)	MSIE
10	6 (0.02%)	4 (0.10%)	11.8 KiB (0.00%)	Yandex.Brows
TOT.	30 780	4 075	1.67 GiB	398

-
-
-
-

TIME DISTRIBUTION
DATA SORTED BY HOUR [,AVGTS,CUMTS,MAXTS]

Panel Options
 00030609141720230.03306601.0k1.3k1.7k2.0k2.3k2.7k3.0k0.050100150200250300350400450HitsVisitorsHitsVisitors

#	HITS	VISITORS	TX. AMOUNT	DATA
MIN.	72 (0.23%)	24 (0.46%)	2.12 MiB (0.12%)	
MAX.	3 312 (10.76%)	495 (9.42%)	612.1 MiB (35.71%)	
AVG.	1 399 (4.55%)	238 (4.53%)	77.92 MiB (4.55%)	
1	1 120 (3.64%)	159 (3.90%)	19.51 MiB (1.14%)	00
2	720 (2.34%)	153 (3.75%)	24.11 MiB (1.41%)	01
3	1 199 (3.90%)	128 (3.14%)	15.16 MiB (0.88%)	02
4	380 (1.23%)	162 (3.98%)	33.03 MiB (1.93%)	03
5	585 (1.90%)	181 (4.44%)	19.12 MiB (1.12%)	04
6	617 (2.00%)	194 (4.76%)	20.4 MiB (1.19%)	05
7	1 709 (5.55%)	202 (4.96%)	55.7 MiB (3.25%)	06
8	1 971 (6.40%)	250 (6.13%)	55.94 MiB (3.26%)	07

#	HITS	VISITORS	TX. AMOUNT	DATA
MIN.	72 (0.23%)	24 (0.46%)	2.12 MiB (0.12%)	
MAX.	3 312 (10.76%)	495 (9.42%)	612.1 MiB (35.71%)	
AVG.	1 399 (4.55%)	238 (4.53%)	77.92 MiB (4.55%)	
9	1 665 (5.41%)	267 (6.55%)	57.42 MiB (3.35%)	08
10	453 (1.47%)	94 (2.31%)	13.24 MiB (0.77%)	09
11	96 (0.31%)	28 (0.69%)	4.6 MiB (0.27%)	10
12	72 (0.23%)	24 (0.59%)	2.12 MiB (0.12%)	11
13	365 (1.19%)	112 (2.75%)	20.49 MiB (1.20%)	14
14	1 744 (5.67%)	335 (8.22%)	91.67 MiB (5.35%)	15
15	1 460 (4.74%)	294 (7.21%)	122.96 MiB (7.17%)	16
16	2 351 (7.64%)	401 (9.84%)	612.1 MiB (35.71%)	17

#	HITS	VISITORS	TX. AMOUNT	DATA
MIN.	72 (0.23%)	24 (0.46%)	2.12 MiB (0.12%)	
MAX.	3 312 (10.76%)	495 (9.42%)	612.1 MiB (35.71%)	
AVG.	1 399 (4.55%)	238 (4.53%)	77.92 MiB (4.55%)	
17	2 843 (9.24%)	495 (12.15%)	100.9 MiB (5.89%)	18
18	2 888 (9.38%)	469 (11.51%)	120.85 MiB (7.05%)	19
19	3 312 (10.76%)	439 (10.77%)	95.92 MiB (5.60%)	20
20	2 411 (7.83%)	394 (9.67%)	113.13 MiB (6.60%)	21
21	1 150 (3.74%)	249 (6.11%)	48.66 MiB (2.84%)	22
22	1 669 (5.42%)	227 (5.57%)	67.26 MiB (3.92%)	23
TOT.	30 780	5 257	1.67 GiB	22

•
•
•

•

REFERRING SITES

TOP REFERRING SITES SORTED BY HITS [,AVGTS,CUMTS,MAXTS]

Panel Options

tamogass.ahang.hukorbe.huwww.swannet.orgsimplesite.comstat.linkensphere.comSwannet.orgwebtechsurvey.comgoogle.comnyitottakvagyunk.orgwww.kornyvéd.hu0.08501.7k2.6k3.4k4.3k5.1k6.0k6.8k7.7k0.014
02704105506908209601.1k1.2kHitsVisitorsHitsVisitors

#	HITS	VISITORS	TX. AMOUNT	DATA
MIN.	1 (0.01%)	1 (0.04%)	—	
MAX.	8 511 (52.29%)	1 370 (48.22%)	420.26 MiB (53.57%)	
AVG.	208 (1.28%)	36 (1.27%)	10.06 MiB (1.28%)	
1	8 511 (27.65%)	1 370 (33.62%)	420.26 MiB (24.51%)	tamogass.ahang.hu
2	2 853 (9.27%)	81 (1.99%)	83.87 MiB (4.89%)	nyitottakvagyunk.hu
3	1 230 (4.00%)	84 (2.06%)	94.25 MiB (5.50%)	swannet.org
4	867 (2.82%)	29 (0.71%)	35.18 MiB (2.05%)	ma-puppetry.eu
5	682 (2.22%)	43 (1.06%)	117.35 MiB (6.85%)	nohastudio.hu

#	HITS	VISITORS	TX. AMOUNT	DATA
MIN.	1 (0.01%)	1 (0.04%)	—	
MAX.	8 511 (52.29%)	1 370 (48.22%)	420.26 MiB (53.57%)	
AVG.	208 (1.28%)	36 (1.27%)	10.06 MiB (1.28%)	
6	625 (2.03%)	501 (12.29%)	2.35 MiB (0.14%)	ahang.hu
7	307 (1.00%)	5 (0.12%)	2.06 MiB (0.12%)	metabase.tamogass.ahang.hu
8	165 (0.54%)	70 (1.72%)	54.74 KiB (0.00%)	decidim.ahang.hu
9	159 (0.52%)	15 (0.37%)	9.47 MiB (0.55%)	korbe.hu
10	142 (0.46%)	136 (3.34%)	760.62 KiB (0.04%)	com.google.android.gm
11	129 (0.42%)	119 (2.92%)	530.25 KiB (0.03%)	elovalasztas.hu
12	111 (0.36%)	81 (1.99%)	422.76 KiB (0.02%)	terjed.ahang.hu
13	69 (0.22%)	69 (1.69%)	279.22 KiB (0.02%)	szabad.ahang.hu

#	HITS	VISITORS	TX. AMOUNT	DATA
MIN.	1 (0.01%)	1 (0.04%)	—	
MAX.	8 511 (52.29%)	1 370 (48.22%)	420.26 MiB (53.57%)	
AVG.	208 (1.28%)	36 (1.27%)	10.06 MiB (1.28%)	
14	48 (0.16%)	37 (0.91%)	7.52 MiB (0.44%)	www.google.com
15	45 (0.15%)	3 (0.07%)	3.6 MiB (0.21%)	193.32.232.143
16	40 (0.13%)	12 (0.29%)	77.71 KiB (0.00%)	dev.ahang.hu
17	30 (0.10%)	15 (0.37%)	276.08 KiB (0.02%)	www.swannet.org
18	23 (0.07%)	10 (0.25%)	247.17 KiB (0.01%)	baidu.com
19	19 (0.06%)	17 (0.42%)	153.06 KiB (0.01%)	m.facebook.com
20	19 (0.06%)	18 (0.44%)	103.42 KiB (0.01%)	freemail.hu
21	17 (0.06%)	15 (0.37%)	141.88 KiB (0.01%)	lm.facebook.com

#	HITS	VISITORS	TX. AMOUNT	DATA
MIN.	1 (0.01%)	1 (0.04%)	—	
MAX.	8 511 (52.29%)	1 370 (48.22%)	420.26 MiB (53.57%)	
AVG.	208 (1.28%)	36 (1.27%)	10.06 MiB (1.28%)	
22	16 (0.05%)	1 (0.02%)	368.25 KiB (0.02%)	dev.szavazas.eleve.hu
23	13 (0.04%)	8 (0.20%)	149.3 KiB (0.01%)	youtube.com
24	9 (0.03%)	7 (0.17%)	505.57 KiB (0.03%)	www.google.hu
TOT.	16 276	2 841	784.56 MiB	78

-
-
-
-

HTTP STATUS CODES

TOP HTTP STATUS CODES SORTED BY HITS [, AVGTS, CUMTS, MAXTS]

Panel Options

2xx Success3xx Redirection4xx Client Errors5xx Server Errors1xx Informational0.02.1k4.2k6.3k8.4k10k13k15k17k19k0.03607101.1k1.4k1.8k2.1k2.5k2.9k3.2kHitsVisitorsHitsVisitors

#	HITS	VISITORS	TX. AMOUNT	DATA
MIN.	3 (0.01%)	3 (0.06%)	—	
MAX.	20 823 (67.65%)	3 554 (71.32%)	1.62 GiB (96.75%)	
AVG.	1 923 (6.25%)	311 (6.24%)	107.14 MiB (6.25%)	
1	20 969 (68.13%)	3 570 (87.61%)	1.62 GiB (96.85%)	2xx Success
2	5 534 (17.98%)	1 247 (30.60%)	2.57 MiB (0.15%)	3xx Redirection
3	3 577 (11.62%)	0 (0.00%)	50.68 MiB (2.96%)	4xx Client Errors
4	697 (2.26%)	163 (4.00%)	745.02 KiB (0.04%)	5xx Server Errors
5	3 (0.01%)	3 (0.07%)	46 B (0.00%)	1xx Informational
TOT.	30 780	4 983	1.67 GiB	16



GEOLOCATION

CONTINENT > COUNTRY SORTED BY UNIQUE HITS [, AVGTS, CUMTS, MAXTS]

Panel Options

EU Europe NA North America AS Asia SA South America AF Africa OC Oceania 0.02.3k4.5k6.8k9.0k11k14k16k18k20k0.02605307901.1k1.3k1.6k1.8k2.1k2.4k Hits Visitors Hits Visitors

#	HITS	VISITORS	TX. AMOUNT	DATA
MIN.	1 (0.00%)	1 (0.02%)	166 B (0.00%)	
MAX.	13 872 (45.07%)	1 482 (36.37%)	627.84 MiB (36.62%)	
AVG.	349 (1.13%)	46 (1.13%)	19.48 MiB (1.14%)	
1	22 586 (73.38%)	2 622 (64.34%)	1.32 GiB (78.70%)	EU Europe
2	5 333 (17.33%)	956 (23.46%)	272.88 MiB (15.92%)	NA North America
3	2 460 (7.99%)	446 (10.94%)	69.06 MiB (4.03%)	AS Asia
4	204 (0.66%)	23 (0.56%)	6.57 MiB (0.38%)	SA South America
5	126 (0.41%)	20 (0.49%)	10.03 MiB (0.58%)	AF Africa
6	71 (0.23%)	8 (0.20%)	6.7 MiB (0.39%)	OC Oceania

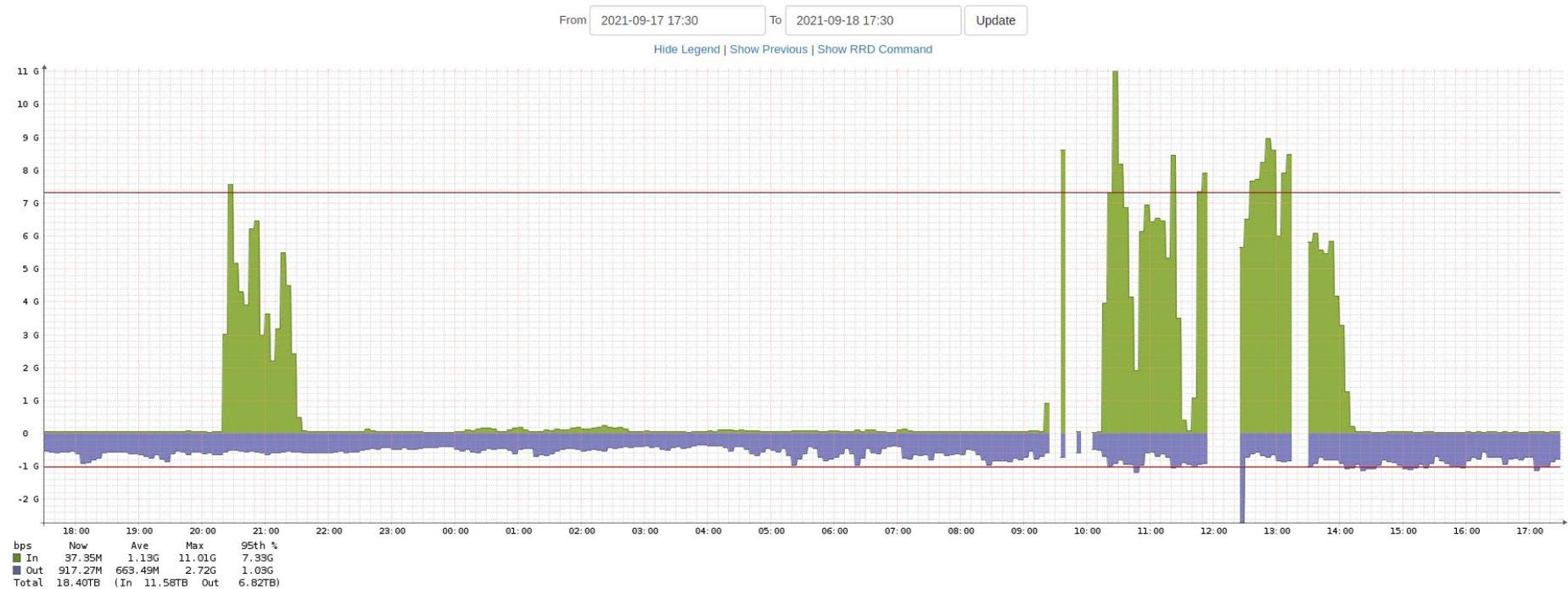
#	HITS	VISITORS	TX. AMOUNT	DATA
MIN.	1 (0.00%)	1 (0.02%)	166 B (0.00%)	
MAX.	13 872 (45.07%)	1 482 (36.37%)	627.84 MiB (36.62%)	
AVG.	349 (1.13%)	46 (1.13%)	19.48 MiB (1.14%)	
TOT.	30 780	4 075	1.67 GiB	88

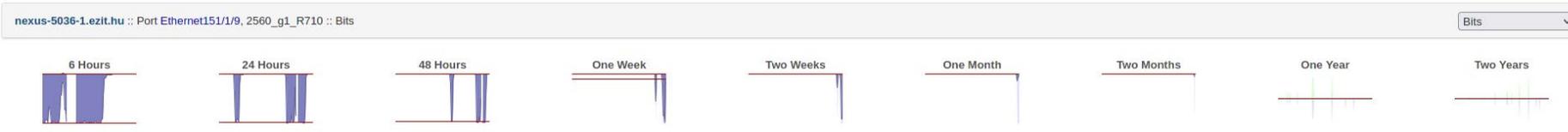
Kiberbiztonsági elemzés

A kiberbiztonsági incidens kivizsgálása a 2021.08.18-i eseményekre fókuszál. A grafikonból jól látszik, hogy a szerverek hálózati befogadó képességének a többszöröse, mintegy 8-szoros forgalom érintette a szervereket.

A hosting szolgáltató hálózati terhelés kimutatása:

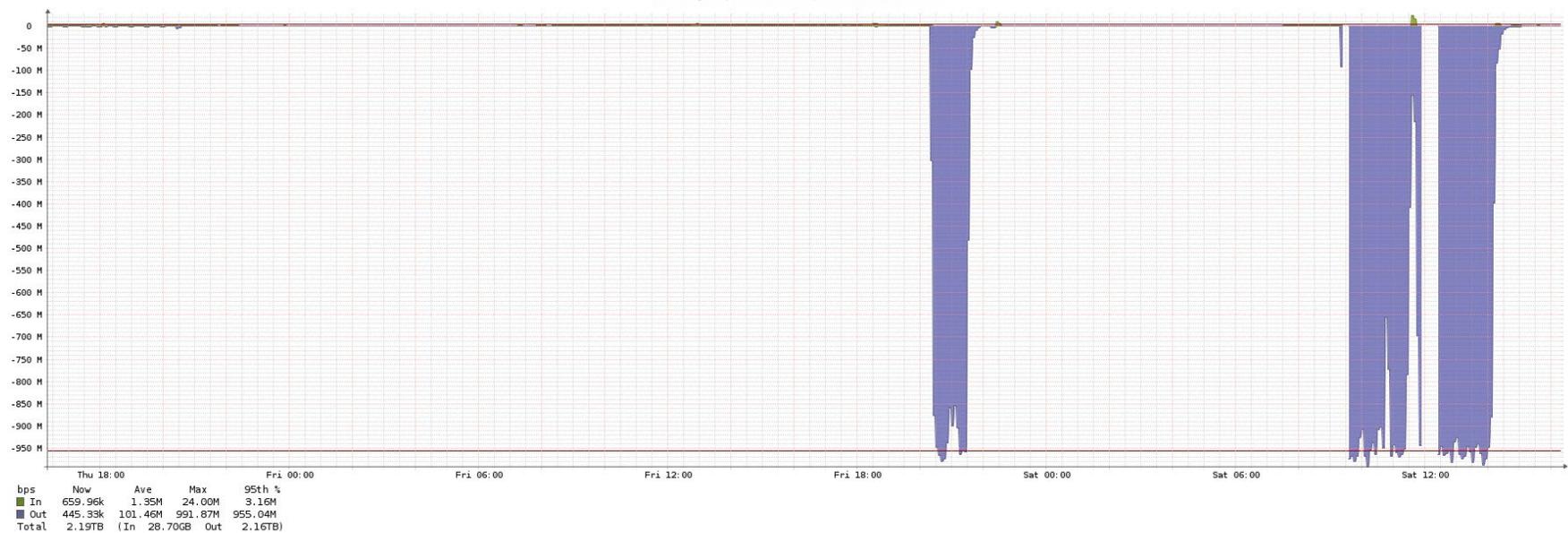
xy

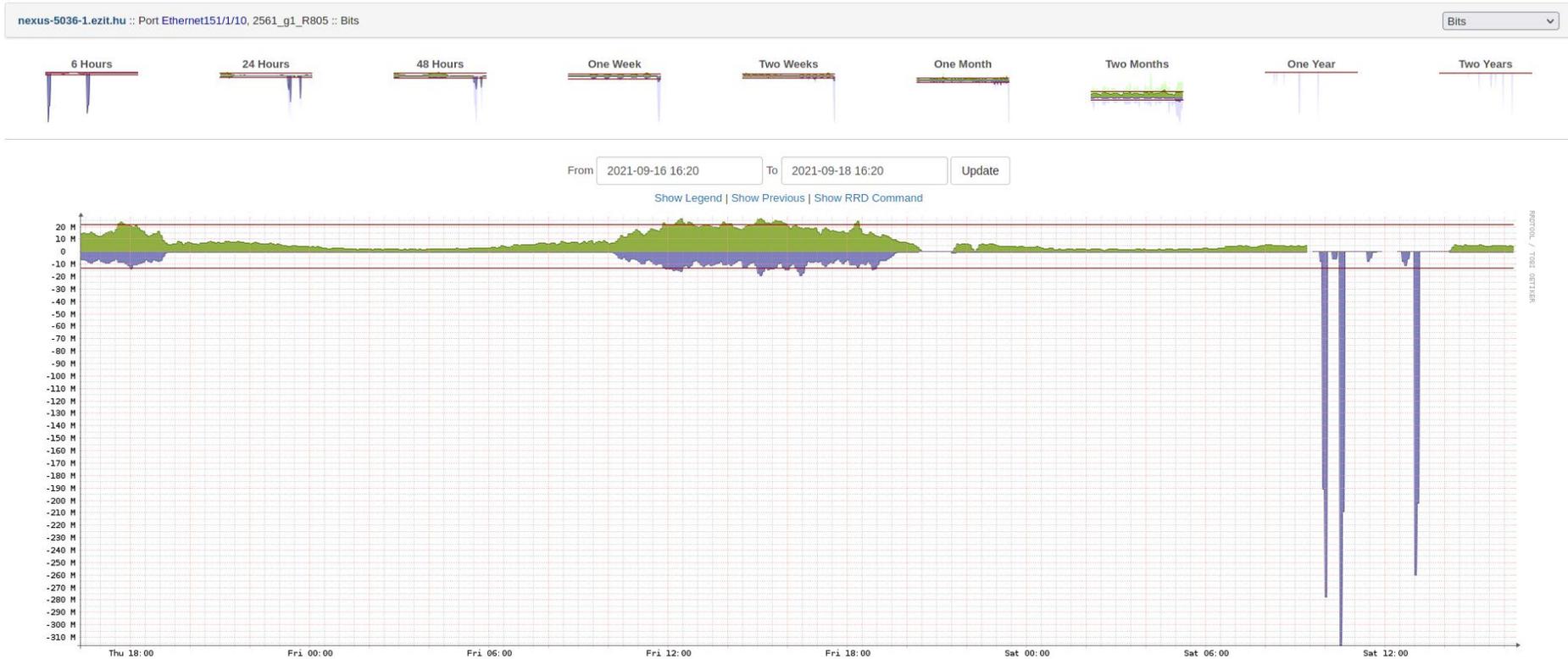




From 2021-09-16 16:20 To 2021-09-18 16:20 Update

[Hide Legend](#) | [Show Previous](#) | [Show RRD Command](#)



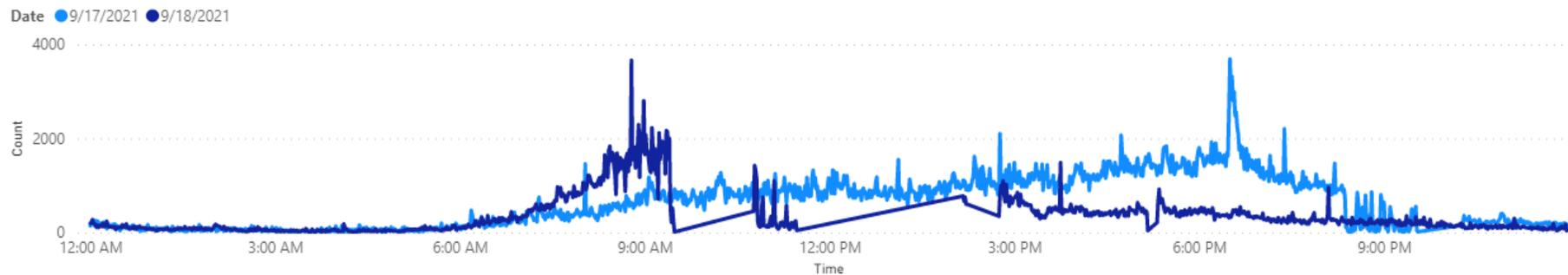


A fenti grafikonokból kiderül, hogy a rendszer alulméretezett volt. A hálózati kapcsolat megszűnt, a szinkronizáció nem volt lehetséges, így a szerver menedzser szoftver lezárta a kapcsolatokat, mivel nem tudta elérni a többi kiszolgálót.

Támadási minták

Az összes konkurens kérés mintázata

Web requests time series



Látható, hogy a kiszolgálók mindkét időpontban elérték a terhelés csúcsát, egymást már nem érték el, így omlott össze a szinkron működés közöttük, ezért az adatintegritás megőrzése miatt a vezérlés az össze szerver elérhetőségét blokkolta.

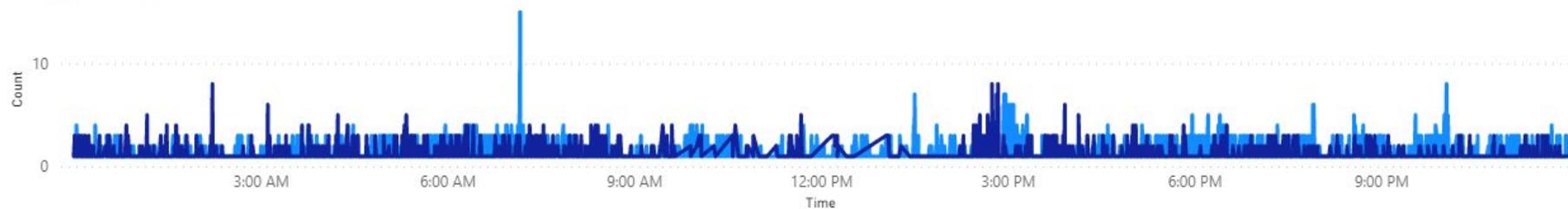
Ezzel megszűnt a szerverek közötti szinkronizáció, ami a rendszer teljes leállításához vezetett.

Az SSH bejelentkezési felület támadása

A grafikonon látható, hogy a távoli bejelentkezés feltörési próbálkozásai botnet tevékenységet mutatnak, a kiugrást az adminisztrátorok bejelentkezési kísérletei okozták. Az eloszlás botnet tevékenység mintázata.

Node1 auth log time series

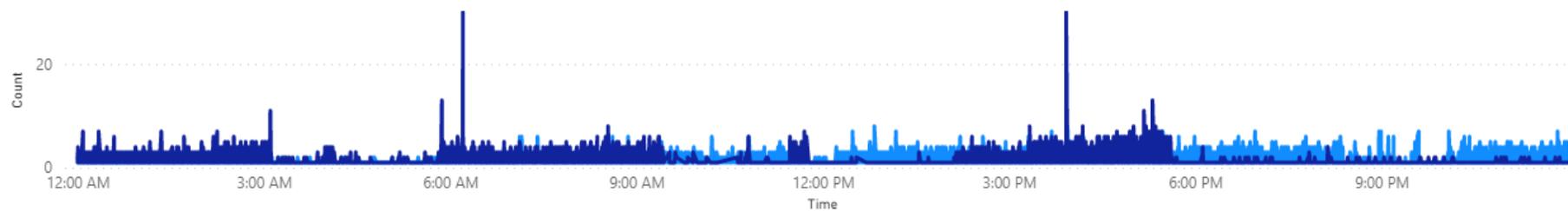
Date ● 9/17/2021 ● 9/18/2021



A webes admin felület támadási mintázata

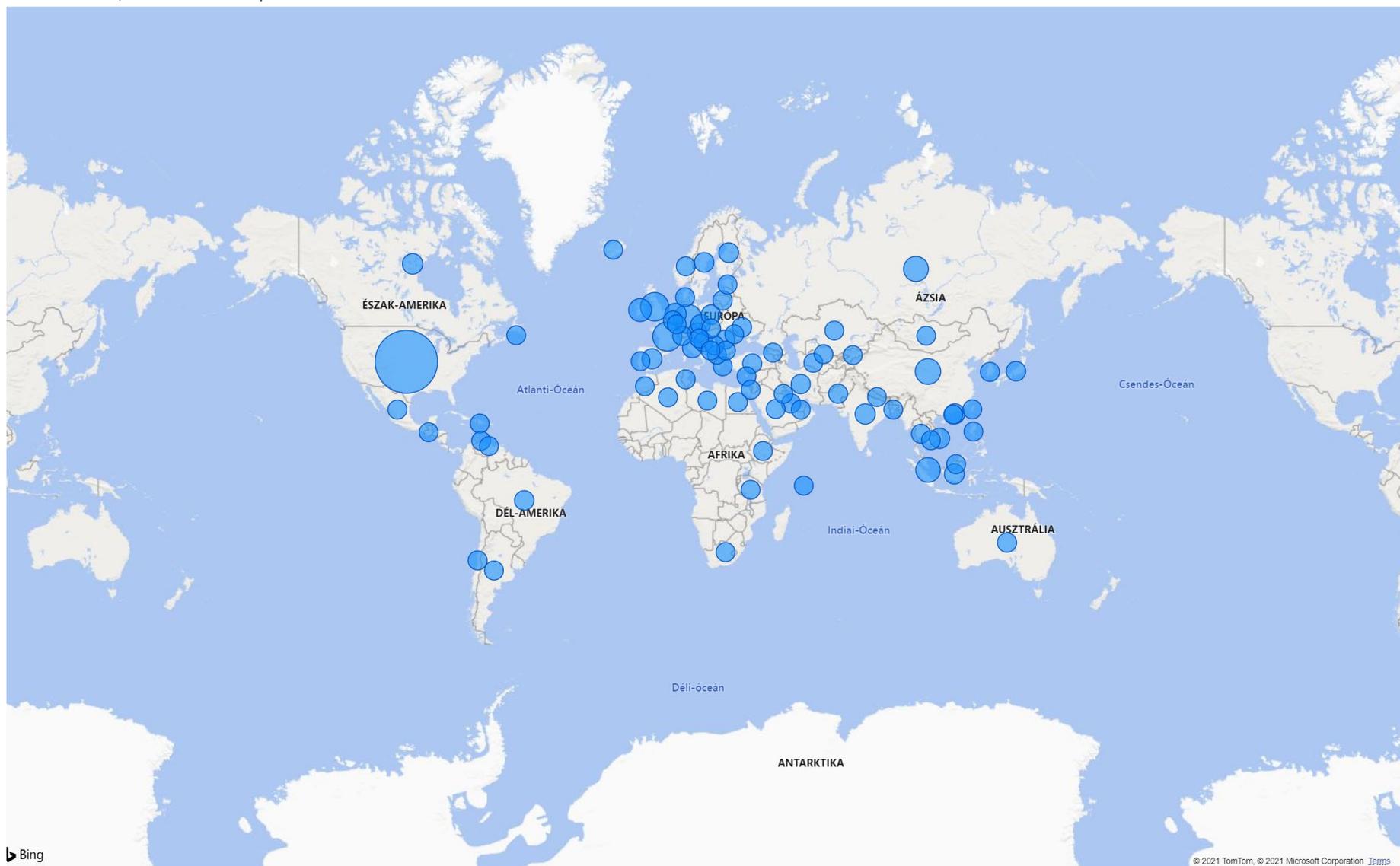
Node1 pveproxy time series

Date ● 9/17/2021 ● 9/18/2021



A rendszer webes adminfelületének elérési, próbálkozási mintázata is követi a terhelési görbe mintáját. Hálózati elérés híján az adminok sem tudtak bejelentkezni a vezérlő felületre.

A rendszert, nem szabványos módon elérni kívánó IP címek eloszlása



A rendszert nem szabványos módon elérni kívánó IP címek országokénti eloszlása

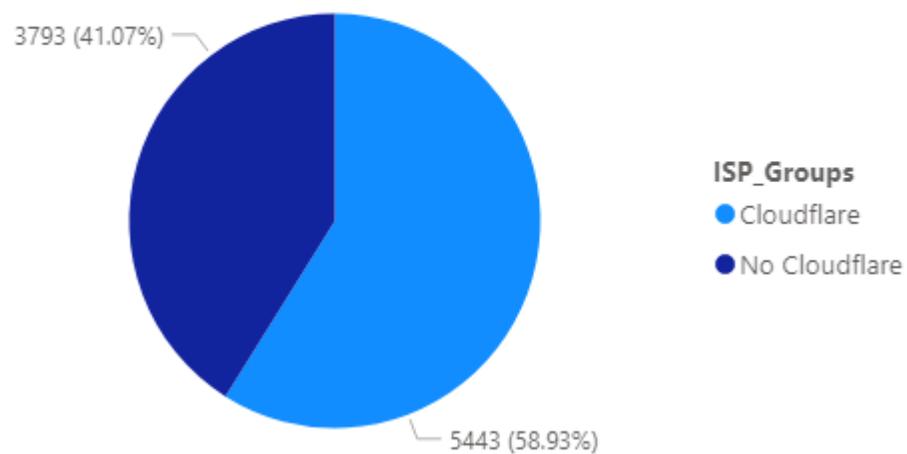
18 Sep - Count of Uniq IPs per country (without CF and Hun IP)



A grafikonon több szabályszerűség is lászik, az egyenlő arányok különböző botnet tevékenységre utalnak.

A szabványos kérések és a támadások eloszlása forrás címekhez viszonyítva

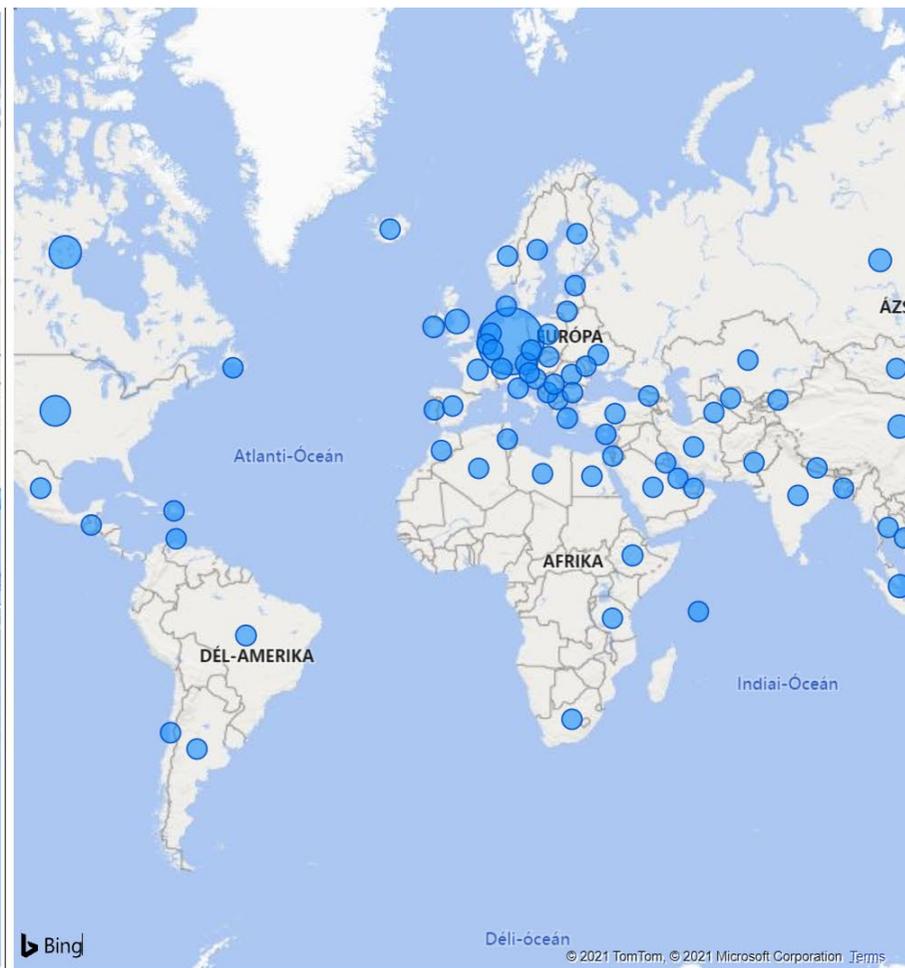
IP-k száma (szept. 18.)



Egyértelműen kimutatható, hogy a normál kéréseket indító forráscímek, valamint a normális kéréseken kívül kérést küldő címek aránya 59%-41%.

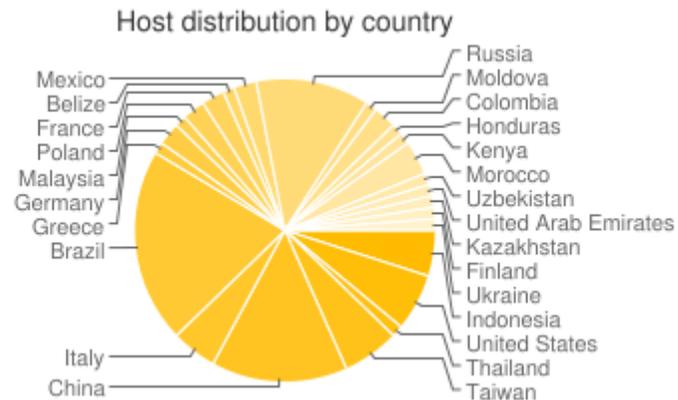
Terheléses támadás

A legtöbb IP az USA-ból, a legnagyobb nem szabványos terhelés viszont Európából érkezett a weboldalra.



A támadó IP címek attribútumai

- Rengeteg kérés a publikus sérülékenység kereső szolgáltatások botnet hálózatához köthető, azaz letapogatás, támadás előkészítésre használt, publikusan elérhető botnet forgalom.
- A legújabb Linux alapú virtualizációs sérülékenységet kereső botnet forgalom is látható a logokban.
- A távoli bejelentkezést célzó bruteforce kérések a jól ismert Cobalt Strike, Trickbot, Locki botnetek forgalma, amik az elmúlt 5 évben szerepet játszottak az amerikai és európai választásokat befolyásoló, valamint a legutóbbi zsaroló vírus támadásokban is.



A legtöbb, a rendszer feltörését célzó támadás a fenti grafikon alapján Braziliából és Kínából érkezett a rendszer ellen. Ezek mindegyike Botnet tevékenységhez és nem célzott, humán támadáshoz köthető.

Összefoglalás

- Kijelenthető, hogy a rendszer a nem tervezett hálózati terhelés miatt nem tudott kiszolgálni.
- Támadási minták tapasztalhatóak a forgalomban, de ezek egyike sem hálózati túlterhelés, sokkal inkább a kiszolgálók és az alkalmazás sérülékenységeit letapogató próbálkozások voltak.
- A megnövekedett forgalom, melynek 41%-a nem rendeltetés szerű volt, valamint a szerverek internet kapcsolatának alul méretezése és a belső szinkronizáció hiányának együttese okozta a leállást.