

BGP Ranking

Scoring ASNs based on their potential maliciousness



CIRCL

Computer Incident
Response Center
Luxembourg

Team CIRCL - *TLP:WHITE*

info@circl.lu

July 25, 2013

Daily top - <http://bgpranking.circl.lu/>

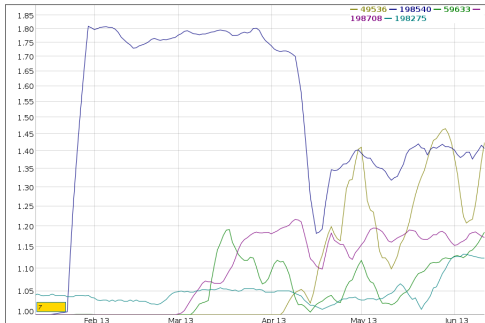
ASN	Description	Rank	Source(s)
49536	DENTA-AS DENTAGLOBAL SYS	1.51759765625	Allenvault, Malc0de, BlocklistDeBots
198540	ELAN-AS Przedsiębiorstwo Usług Specjalistycznych ELAN mgr inż. Andrzej Niechciał	1.398828125	BlocklistDeStrong, DshieldDaily, BlocklistDeBots
59633	UANETWORKING-AS UA-NETWORKING LTD	1.2138671875	BlocklistDeBots
198708	VYMPELSTROY-AS VympelSstroy ltd.	1.155078125	DshieldDaily, BlocklistDeBots
198275	NLNK-AS LLC NEWLINK	1.1454296875	Allenvault, Shunlist, SshbBase, BlocklistDeSsh, EmergingThreatsCompromized, DshieldDaily
3192	FREESTYLE-AS Freestyle Ltd.	1.13671875	BlocklistDeBots
58049	TECHSUPPORT-AS Telecom Tekhpodderzhika Ltd	1.129375	Allenvault, SshbBase, DshieldDaily, BlocklistDeBots
20649	ASFIBERSUNUCU Fibersunucu internet Hizmetleri	1.118359375	DshieldDaily, BlocklistDeBots
51743	HOSTPARK-AS PE Teran Marina Vas'evna	1.08421875	Allenvault, SshbBase, ZeustrackerIpBlockList
199646	ASEPIOHOST EPIOHOST Ltd.	1.0793359375	Allenvault, Malc0de, DshieldDaily
18981	SUPREME-TELECOM - Supreme Telecom Systems, Inc.	1.0658270474	BlocklistDeApache, Allenvault, BlocklistDeMal, BlocklistDeStrong, DshieldDaily, BlocklistDeBots
39022	DEEPMEDIA-AS Deep Media	1.05859375	CleanMXPhishing, CleanMXMalwares
57954	ASBUDKO FOP Budko Dmistro Pavlovuch	1.05284179687	Allenvault, DshieldDaily, BlocklistDeStrong, BlocklistDeBots
47583	HOSTINGER-AS Hostinger International Limited	1.04642950149	CleanMXPhishing, Allenvault, DshieldTopIPs, CleanMXMalwares, CleanMXPortals, Malc0de, DshieldDaily
47918	GIGABASE Gigabase ltd	1.04582682292	Allenvault, CleanMXPhishing, Malc0de, CleanMXMalwares
48239	IT-TV-AS Science-Production Association Information Technologies Ltd	1.042578125	BlocklistDeApache, DshieldDaily, BlocklistDeBots
4905	FA-LAX-1 - Future Ads LLC	1.039609375	Allenvault, Malc0de
49960	SCI-THE-WALL SCI The Wall	1.0391015625	Allenvault, SshbBase, EmergingThreatsCompromized
21702	HADDAD - The Haddad Organization Ltd.	1.0391015625	Allenvault, SshbBase, EmergingThreatsCompromized
49468	MAG-BROSS-AS SC Mag Bross Web Services SRL	1.0390625	CleanMXPhishing, CleanMXPortals
35001	MYOWN-AS MyOwn sprl	1.0390625	Malc0de, CleanMXMalwares
197992	PORT-MIX-AS PortMiks LLC	1.0390625	CleanMXMalwares, CleanMXPortals
197595	OBENETWORK Obenetwork AB	1.03882226562	Allenvault, BlocklistDeBots, BlocklistDeMal, DshieldDaily, BlocklistDeApache
43449	DIMLINE-AS Dimline Ltd.	1.0332421875	Allenvault, SshbBase, ZeustrackerIpBlockList, EmergingThreatsCompromized
45037	HISPAWEB-NETWORK Propeln Consulting S.L.U.	1.03300048828	Allenvault, CleanMXMalwares, Malc0de, CleanMXPortals
46179	MEDIAFIRE - MediaFire, LLC	1.03059570312	Allenvault, Malc0de, CleanMXMalwares
59711	FORTUNIX-AS Fortunix Networks L.P.	1.02970703125	Allenvault, Malc0de, DshieldDaily, CleanMXMalwares
43059	TALKACTIVE-AS Talk Active Aps	1.0293359375	Allenvault, Malc0de, CleanMXMalwares

- Rank: IPs present in lists divided by announced IPs
- Each source list has a weight
- Over 10000 ASNs a day

ASN Comparison - <http://bgpranking.circl.lu/comparator>

List of ASNs, separated with a blank:

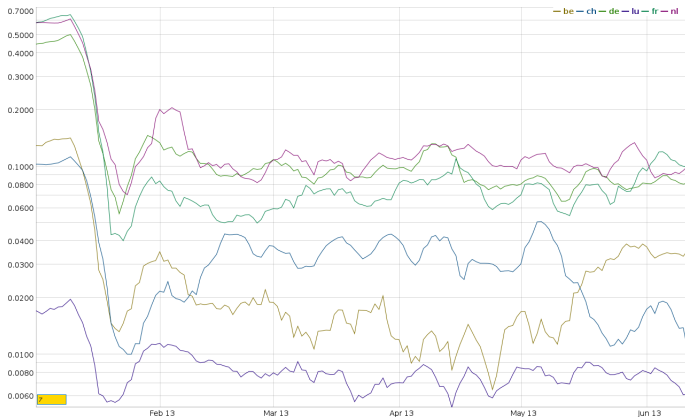
49536 198540 198708 59633 198275



- Merge the graphs of a list of ASNs
- Shows blocks announced by each ASNs

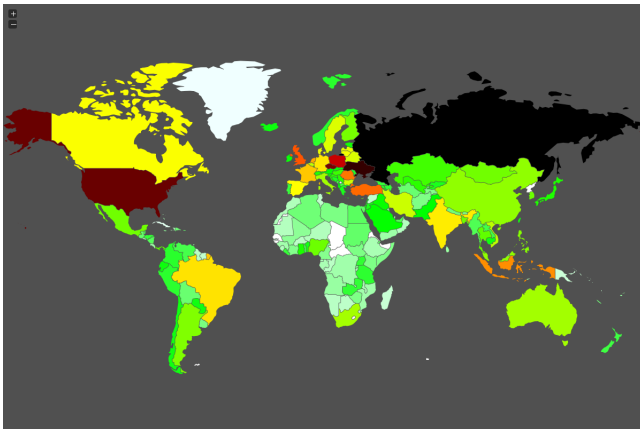
- [49536 \(csv\)](#)
 - [91.207.116.0/23](#)
 - DENTA-AS Dummy description for AS49536: 2013-01-26T01:32:50.591459
 - DENTA-AS DENTAGLOBAL SYS: 2011-05-23T02:36:29.276113
- [198540 \(csv\)](#)
 - [91.236.74.0/23](#)
 - : 2012-05-07T15:05:46.794469
- [59633 \(csv\)](#)
 - [91.210.100.0/22](#)
 - LIANETWORKING-AS Dummy description for AS59633: 2013-01-26T01:44:44.684607
 - LIANETWORKING-AS LIA-NETWORKING LTD: 2012-11-21T02:11:56.629959
- [198708 \(csv\)](#)
 - [91.239.15.0/24](#)
 - : 2013-02-26T01:49:48.755218
- [198275 \(csv\)](#)
 - [91.232.208.0/24](#)
 - : 2012-10-26T14:16:19.054918

Country Comparison - http://bgpranking.circl.lu/trend_benelux



- Comparison between Benelux, Germany, France and Switzerland

Worldmap - <http://bgpranking.circl.lu/map>



- Sum of all the ranks of each ASN, by country

IP Lookup and ASN history - http://bgpranking.circl.lu/ip_lookup

IP to lookup:

217.195.202.10


Submit

- 2013-05-28 - 2013-06-11: [20649](#) - [217.195.202.0/24](#)
 - 2013-06-06: ASFIBERSUNUCU Fibersunucu internet Hizmetleri
 - 2013-06-01: FIBERSUNUCU Fibersunucu internet Hizmetleri
 - 2013-04-07: FIBERSERVER-AS FiberSunucu internet Hizmetleri Ugur Pala
 - 2012-10-08 - 2013-05-27: [42910](#) - [217.195.202.0/24](#)
 - 2013-02-08: SADECEHOSTING-COM Hosting Internet Hizmetleri Ltd Sti
 - 2012-08-12 - 2012-09-02: [20649](#) - [217.195.202.0/24](#)
 - 2013-02-08: TEKLAN-AS FiberSunucu internet Hizmetleri Ugur Pala
 - 2012-08-11 - 2012-08-11: [9121](#) - [217.195.192.0/20](#)
 - 2013-02-08: TTNET Turk Telekomunikasyon Anonim Sirketi
 - 2011-05-17 - 2012-08-10: [20649](#) - [217.195.202.0/24](#)
 - 2013-02-08: TEKLAN-AS FiberSunucu internet Hizmetleri Ugur Pala
-
- Shows the ASNs who announced the IP over time
 - ASN history since 2009-01-01, descriptions since 2013-02-08
 - Why using it instead of Cymru?
 - Historical announces (ASN and prefix)
 - Server/Client/API are availables, you can run it at home.
 - Import bview files, you can use your own

Links

- BGP Ranking and external components
 - Server: <https://github.com/CIRCL/bgp-ranking>
 - API: <https://github.com/CIRCL/bgpranking-redis-api>
 - IP ASN History: <https://github.com/CIRCL/IP-ASN-history>
 - ASN Descriptions:
<https://github.com/CIRCL/ASN-Description-History>

Q&A?



22-24 October 2013 - Luxembourg
9th edition of the infosec conference

"We're not computers, Sebastian, we're physical"
Roy Batty in Blade Runner