

# BGP Ranking

Scoring ASNs based on their potential maliciousness



**CIRCL**

Computer Incident  
Response Center  
Luxembourg

Team CIRCL - *TLP:WHITE*

[info@circl.lu](mailto:info@circl.lu)

July 25, 2013

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

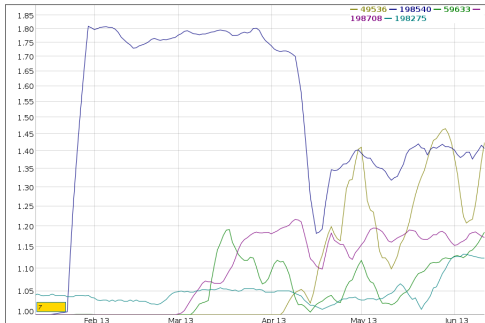
ASN	Description	Rank	Source(s)
<a href="#">49536</a>	DENTA-AS DENTAGLOBAL SYS	1.51759765625	Alienvault, Malc0de, BlocklistDeBots
<a href="#">198540</a>	ELAN-AS Przedsiębiorstwo Usług Specjalistycznych ELAN mgr inż. Andrzej Niechciał	1.398828125	BlocklistDeStrong, DshieldDaily, BlocklistDeBots
<a href="#">59633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

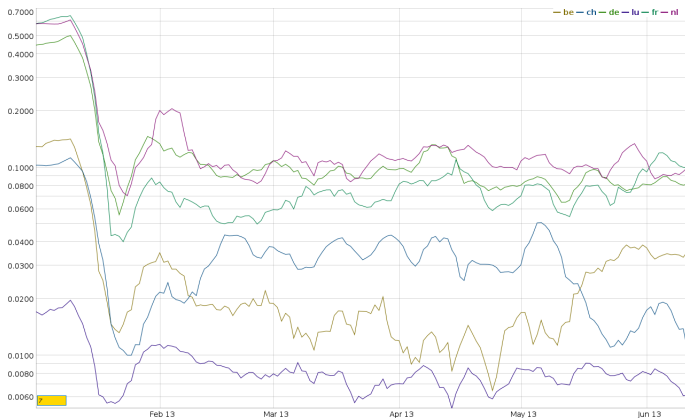
49536 198540 198708 59633 198275



- 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

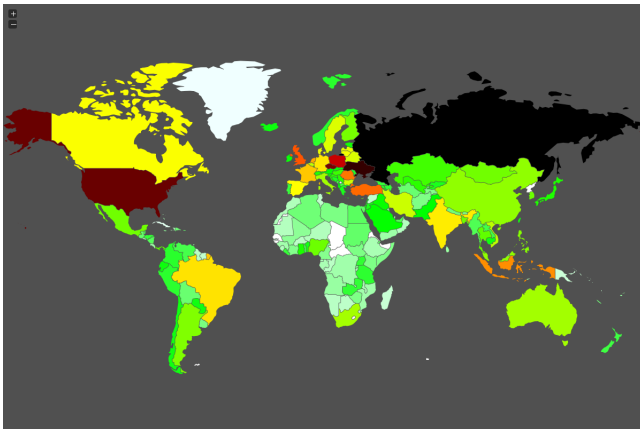
# Country Comparison - [http://bgpranking.circl.lu/trend\\_benelux](http://bgpranking.circl.lu/trend_benelux)



- 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](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