WACREN Network: Network and Security management

WACREN Webinar:

Research and Education Networks: Architecture, Routing and Peering

08/12/2020

WACREN NOC

- Monitor availability
  - Nagios
- Monitor Performance
  - Cacti, MRTG
- Monitor Reliability
  - Smokeping
  - PerfSonar
- Traffic Classification
  - Nimbus
- Alert
- Ticketing
- Internet OoB

WACREN NOC

- Deal with Suppliers(Colo and connectivity)
  - Emails and Phones
  - Performance review meetings
- Deal with NRENs
  - **We lost services/No longer received routes from you** ☺
  - **Not passing traffic through WACREN☺**
  - Emails and Phone
    - noc@wacren.net
    - Moving to support@wacren.net
  - **You seem under attack according to traffic seen by WACREN** ☺
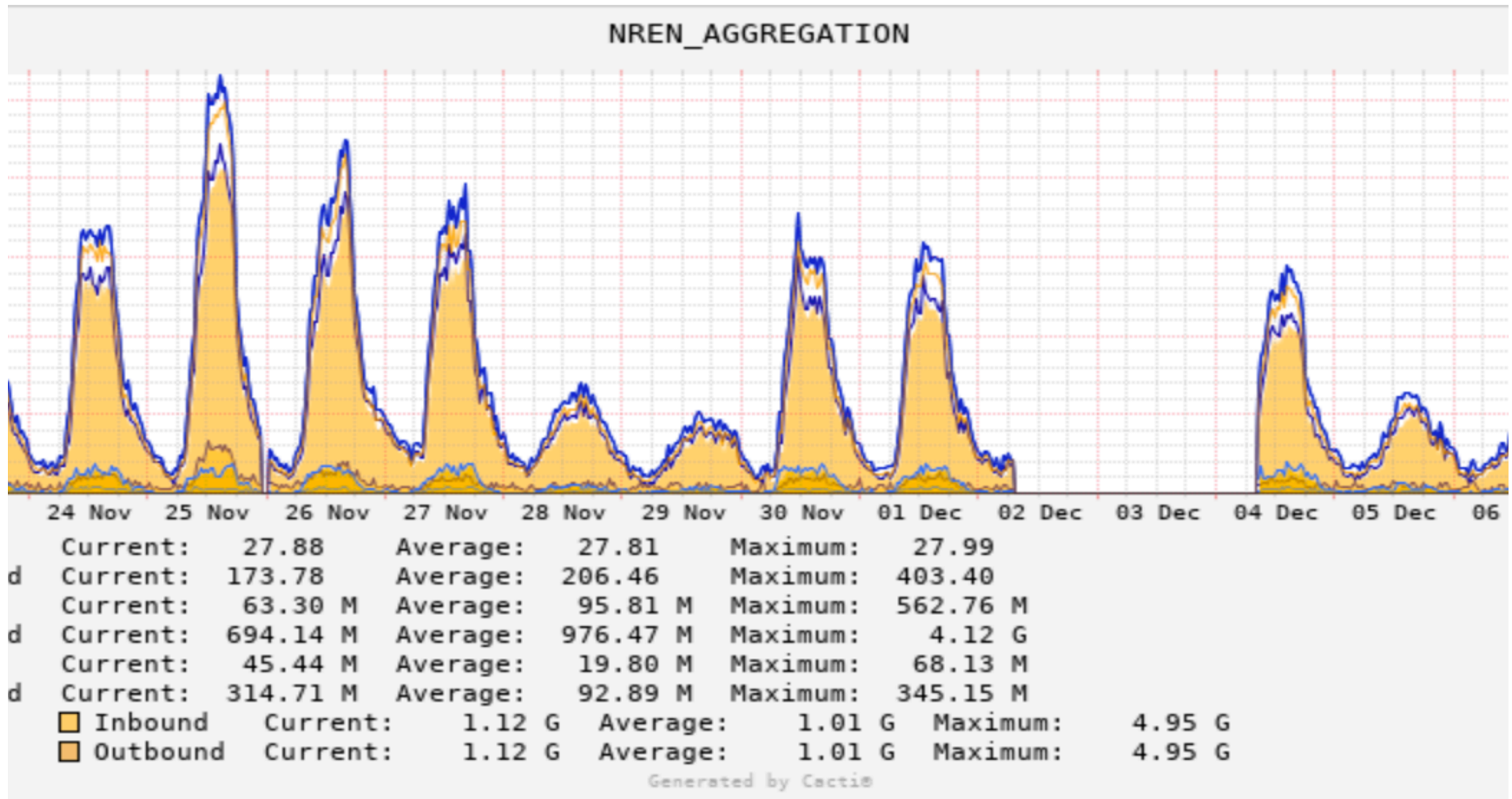- Remote hands
  - Colocation and NRENs

WACREN NOC

Network Operations Center

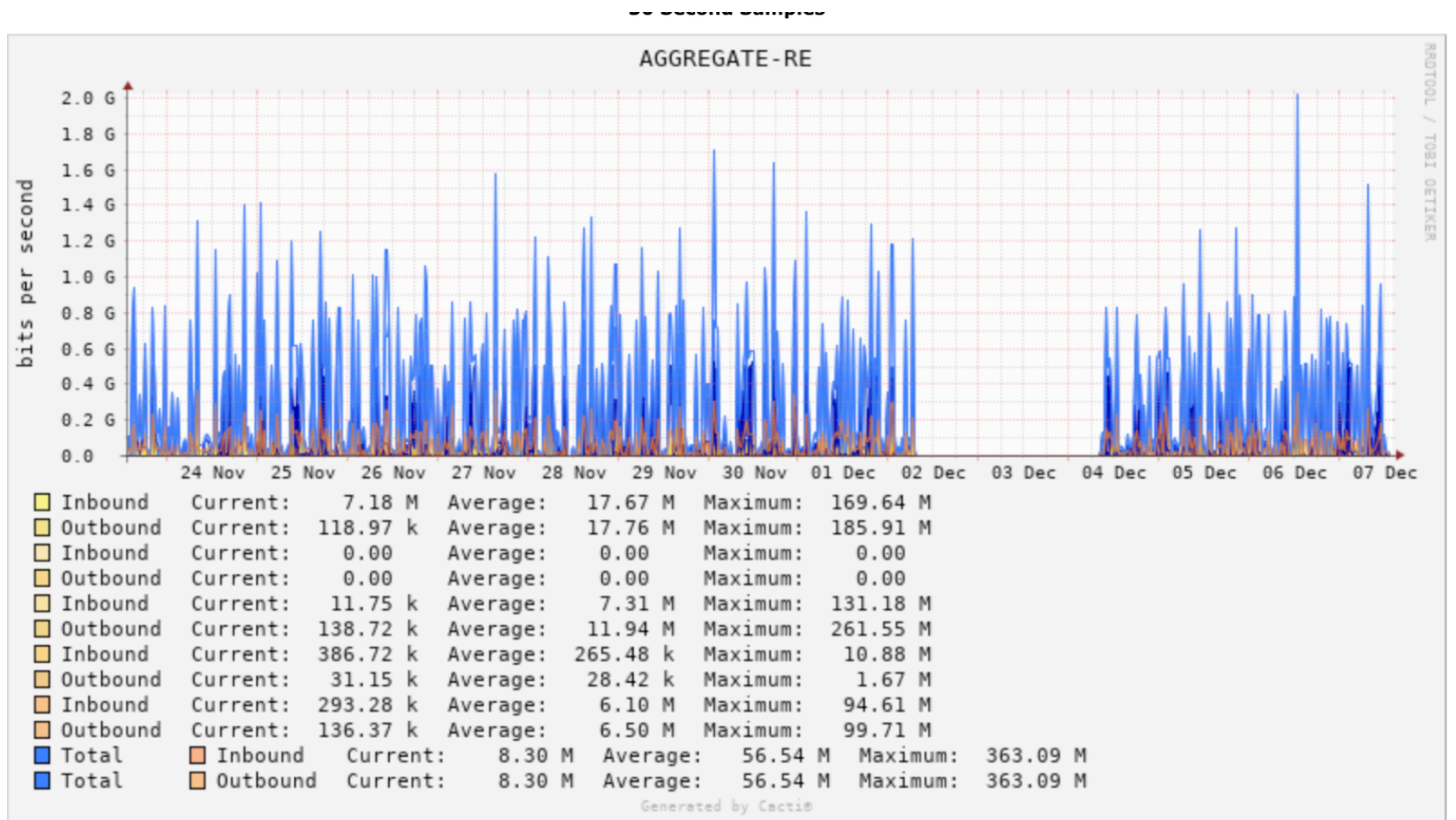|		
CACTI	MRTG	MRTG EV
NAGIOS	SMOKEPING	
NETDOT		
NIMBUS		

Traffic: NREN aggregate

Traffic: Peers REN Aggregate

Documentation

{net.} NETwork DOcumentation Tool

netdot.localdomain

| Management | Contacts | Cable Plant | Advanced | Reports | Export | Help |

| Sites | Closets | Backbone Cables | Horizontal Cables | Circuits |

Sites

Search for returned: 0 matches

Name	Site ID	Street (1)	City
BENIN			Cotonou
DATACENTER KM4	SALLE ZEBRA	Treichville Bd de Marseille KM4	ABIDJAN
EQUINIX	LD8:07:01MC7H:1405	6/7/8/9 Harbour Exchange Square	LONDON
Internet			
MAINONE-ACCRA	CLS-ERP-13	Beech St	ACCRA
MDI-X	LAQ2R16-11	Chief Chuks Ikokwu Street	LAGOS
MEDALLION		No. 26A Hunponu-Wusu Street, Lekki Phase 1	LAGOS
NITA		Abdul Diouf Road, Rodge 3rd Floor	ACCRA
NOC BTI SA	Salle: Colocalisation	Fidjrossè, Rue 12471	Cotonou
ORANGE-CI	Datacenter KM4	Boulevard de Marseille	Abidjan
TOGOCELL	WACREN-TOGOCELL	CACAVELLI	LOME
Telecity			LONDON
Togo			Lomé

PerfSonar

- https://lagos-10g.ps.wacren.net/toolkit/
- http://london-10g.ps.wacren.net/toolkit/

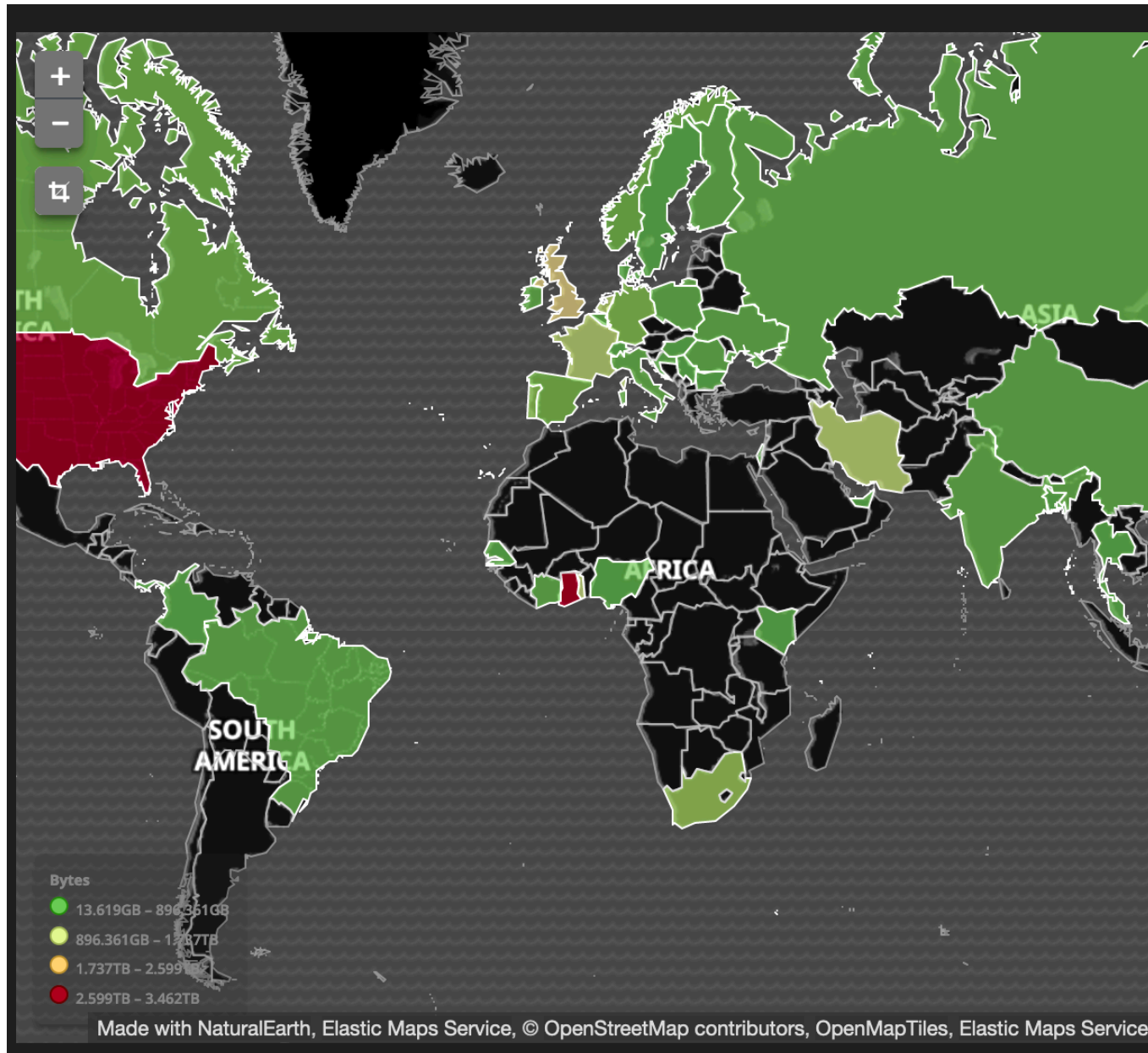| ▲ SOURCE	⬍ DESTINATION	THROUGHPUT	LATENCY (MS)	LOSS
london-10g.ps.wacren.net 196.216.190.2 Graphs | Traceroute ⬈	lagos-10g.ps.wacren.net 196.216.190.18	→ 8.80 Gbps ← 9.13 Gbps	→ 50.8 ← 50.8	→ 0.006% ← 0.006%
london-10g.ps.wacren.net 196.216.190.2 Graphs | Traceroute ⬈	196.32.214.213	→ 505 Mbps ← n/a	→ 80.2 ← n/a	→ 0.014% ← n/a
london-10g.ps.wacren.net 196.216.190.2 Graphs | Traceroute ⬈	196.32.212.82	→ n/a ← n/a	→ 1.45 ← n/a	→ 0.007% ← n/a
london-10g.ps.wacren.net 196.216.190.2 Graphs | Traceroute ⬈	155.0.3.6	→ 297 Mbps ← n/a	→ 80.1 ← n/a	→ 0.712% ← n/a
london-10g.ps.wacren.net 196.216.190.2 Graphs | Traceroute ⬈	p-2p1.test.bldc.net.rt.iu.edu 149.165.227.53	→ 1.42 Gbps ← n/a	→ 44.2 ← n/a	→ 0.003% ← n/a
london-10g.ps.wacren.net 196.216.190.2 Graphs | Traceroute ⬈	perf.newy32aoa.neaar.net 192.203.116.33	→ 9.11 Gbps ← n/a	→ 33.0 ← n/a	→ 0 ← n/a
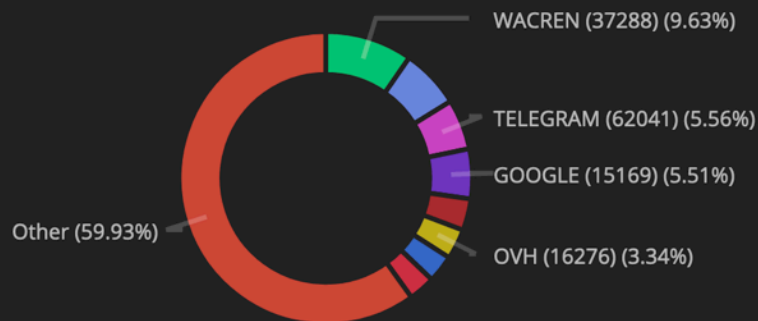
Nimbus: Classification Last 7 days
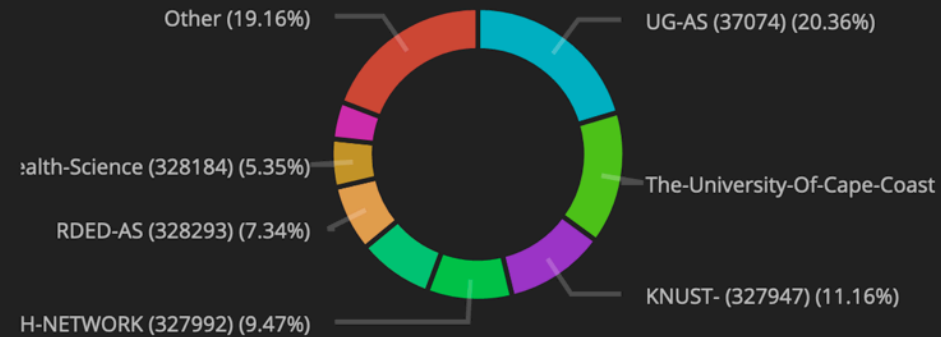
Nimbus: Classification Last 7 days

Peering Opportunities by Destination ASN

Destination ASN ⇕	Total Flows ⇕	Total Bytes ⇕	Total Packets ⇕
UG-AS (37074)	1.499 b	47.836TB	52.891 b
Univ-Health-Science (328184)	386.208 m	12.611TB	13.164 b
The-University-Of-Cape-Coast-AS (328212)	339.77 m	34.545TB	33.315 b
KNUST- (327947)			
GHANAIAN-ACADEMIC-RESEARCH-NETWORK (			

Peering Opportunities by Source ASN

Source ASN ⇕	Total flows ⇕	Total Bytes ⇕	Total Packets ⇕
WACREN (37288)	14.995 m	22.372TB	18.864 b
FACEBOOK (32934)	78.782 m	15.198TB	14.403 b
TELEGRAM (62041)	7.748 m	12.883TB	11.319 b
GOOGLE (15169)	183.552 m	12.75TB	13.319 b
LEVEL3 (3356)	7.558 m	8.14TB	6.241 b
OVH (16276)	45.457 m	7.799TB	6.267 b

Nimbus: Classification

Last 7 days

Bytes
● 13.619GB – 896.361GB
● 896.361GB – 1.737TB
● 1.737TB – 2.599TB
● 2.599TB – 3.462TB

Made with NaturalEarth, Elastic Maps Service, © OpenStreetMap contributors, OpenMapTiles, Elastic Maps Service

Nimbus: Alert

Last 7 days

TC - Alert Top 10 ASNs

alert_asn: Descending	Count
WLINK-NEPAL-AS-AP (17501)	198,729
CHINA169-BACKBONE (4837)	181,307
GOOGLE (15169)	167,218
HINET (3462)	155,943
SEMRUSH-AS (209366)	143,147
rain (37105)	128,363
OVH (16276)	117,130
CNNIC-TENCENT-NET-AP (45090)	95,249
AMAZON-AES (14618)	93,633
KIXS-AS-KR (4766)	82,332

TC - Alert Top 10 Source Ports
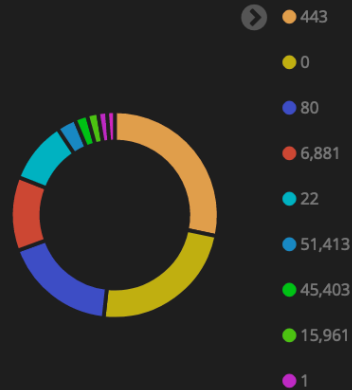
- 443
- 0
- 80
- 6,881
- 22
- 51,413
- 45,403
- 15,961
- 1

TC - Alert Top 10 Destination Ports

- 23
- 443
- 80
- 22
- 37,215
- 5,555
- 3
- 445
- 6,881

TC - Alert Top 10 Source IP

- 155.12.255.215
- 102.176.253.133
- 169.239.248.150
- 169.239.248.114
- 129.122.16.11
- 169.239.248.94
- 102.223.92.109

TC - Alert Top 10 Destination IP

- 155.12.255.215
- 197.255.68.205
- 102.176.253.133
- 169.239.248.150
- 169.239.248.114
- 156.38.96.11
- 156.38.97.11
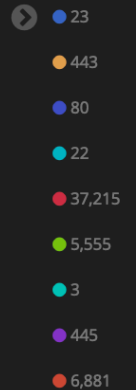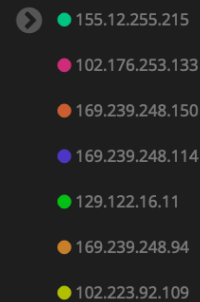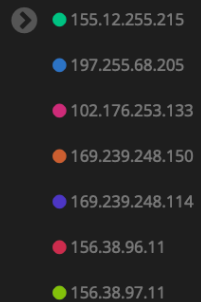
Nimbus: Alert

Last 7 days

TC - Alert Bottom 10 Signatures

alert_signature: Descending	Count
bot-mirai	1,213,697
bot	932,772
bot-smokeloader	620,877
bot-ponyloader	430,471
bruteforce	392,502
controller-httpcnc	345,410
bot-proxyback	298,964
bot-andromeda	221,741
proxy	57,300
spam	12,408

Questions ?