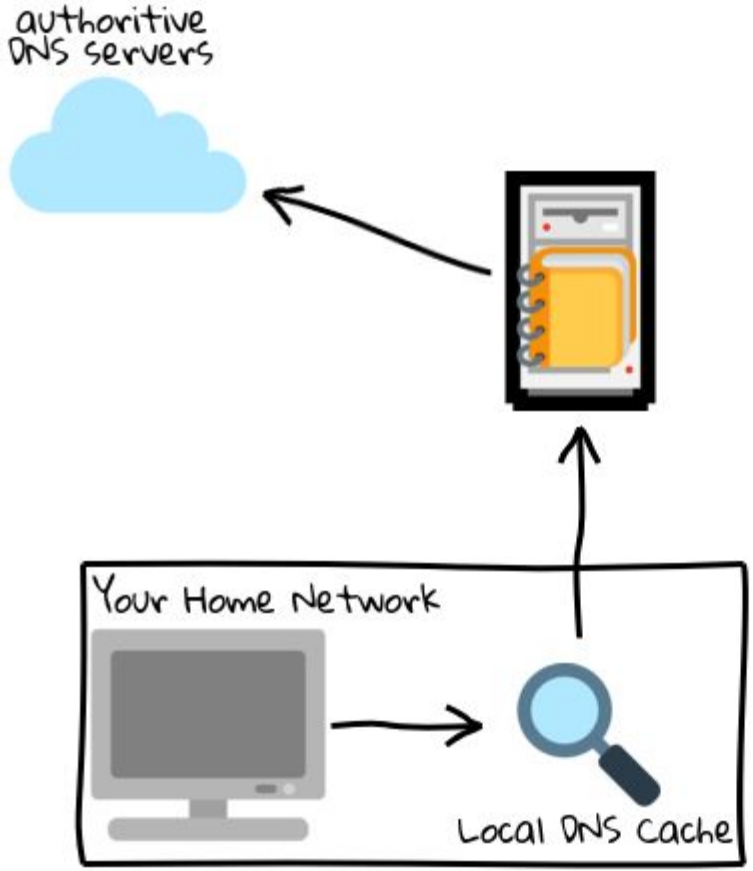
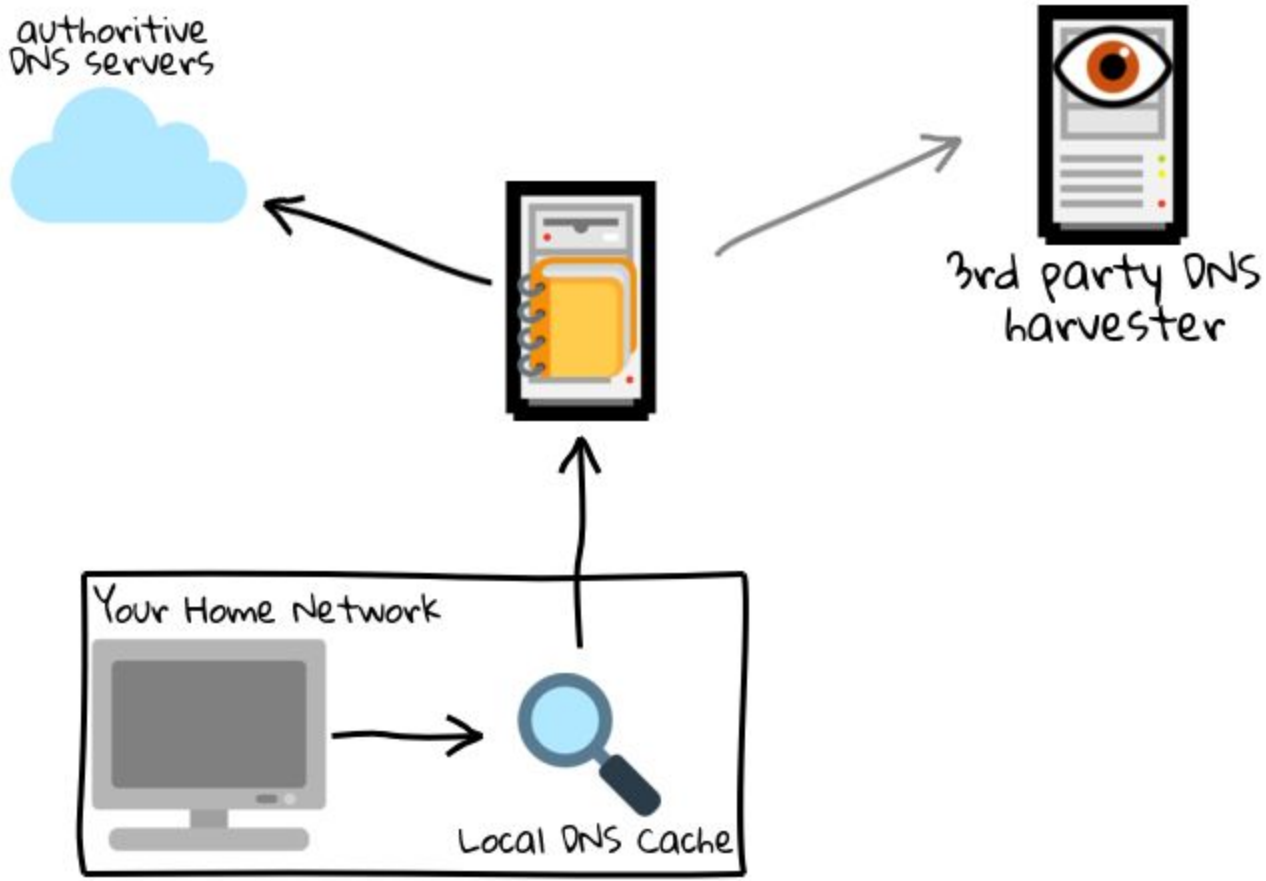
Who is spying on your DNS

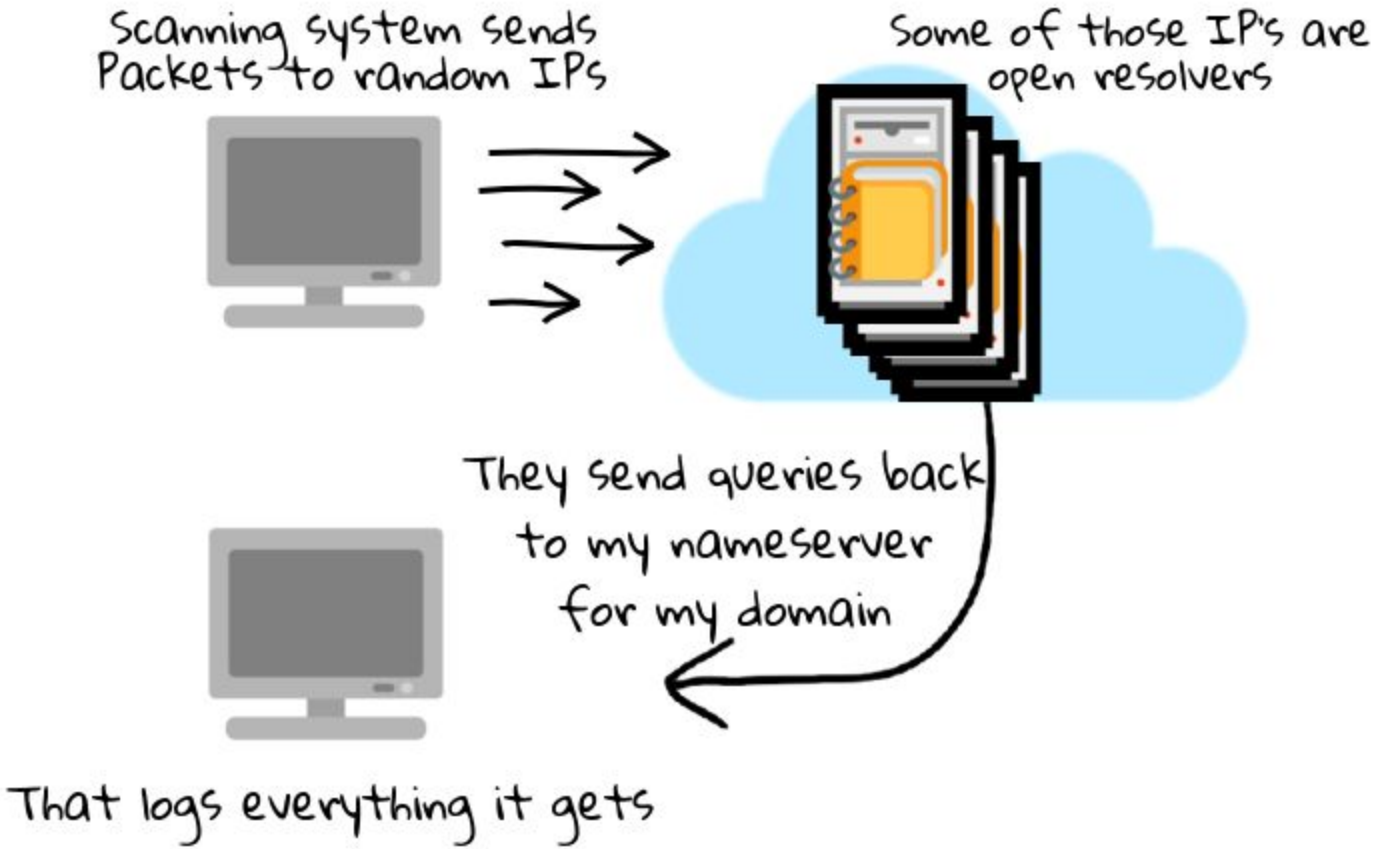
June 20th 2018
RC Talks

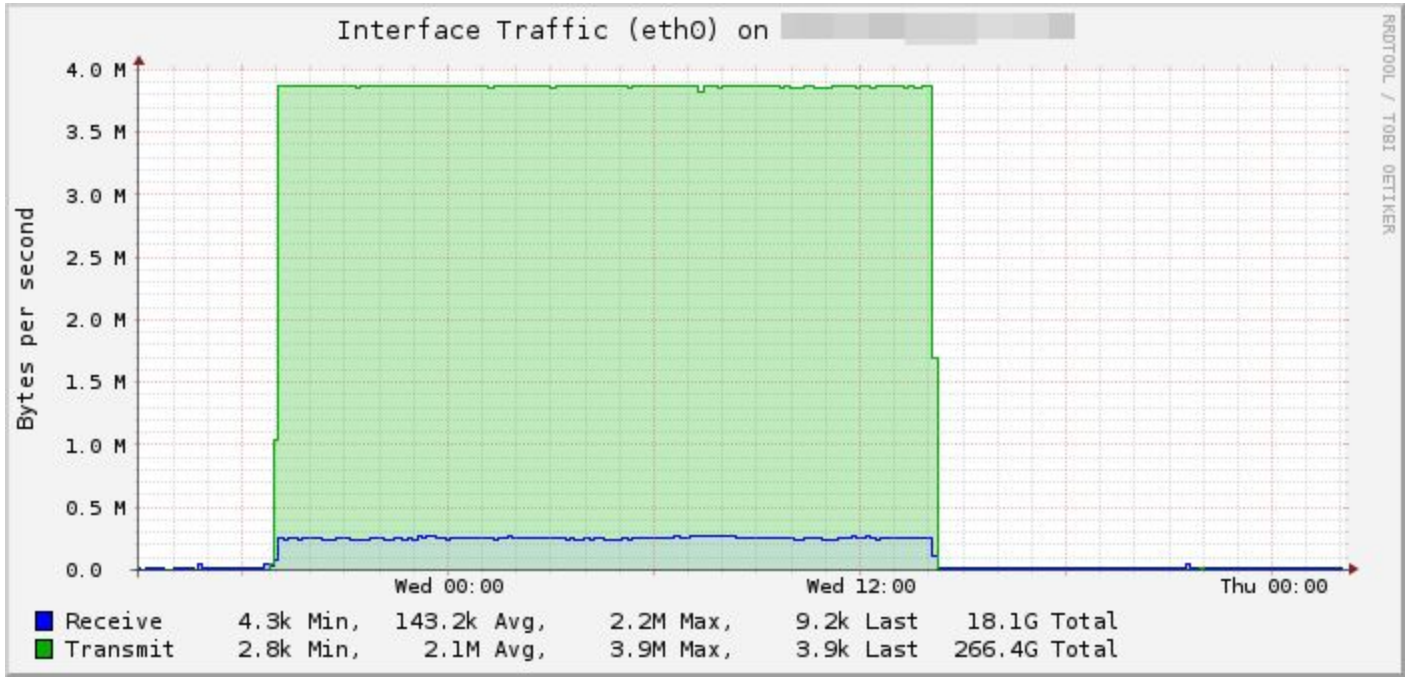
DNS!


authoritive
DNS servers
Your Home Network
Local DNS Cache

Sometimes....


authoritive
DNS servers
3rd party DNS
harvester
Your Home Network
Local DNS Cache


Scanning system sends
Packets to random IPs
Some of those IP's are
open resolvers
They send queries back
to my nameserver
for my domain
That logs everything it gets


Interface Traffic (eth0) on
RRDTOOL / TOBI OETIKER
Bytes per second
4.0 M
3.5 M
3.0 M
2.5 M
2.0 M
1.5 M
1.0 M
0.5 M
0.0
Wed 00:00
Wed 12:00
Thu 00:00
Receive 4.3k Min, 143.2k Avg, 2.2M Max, 9.2k Last 18.1G Total
Transmit 2.8k Min, 2.1M Avg, 3.9M Max, 3.9k Last 266.4G Total

Hacking Activity from 185.230.223.69

Inbox x geoip/United States x

mtso@matera.com via amazonses.com

to noc

You are receiving this message because you are listed as the contact for the networks/domains below. (see WHOIS query results below).

This message is intended for the person responsible for computer security at your site. If this is not the correct address, please forward this message to the appropriate party.

Our logs show that malicious attempts were made from your network against machines in our domain. This is definitely not an authorized request and we view it as an attempt to probe our network for a vulnerability.

Please see that your customer/user ceases this activity. Quite

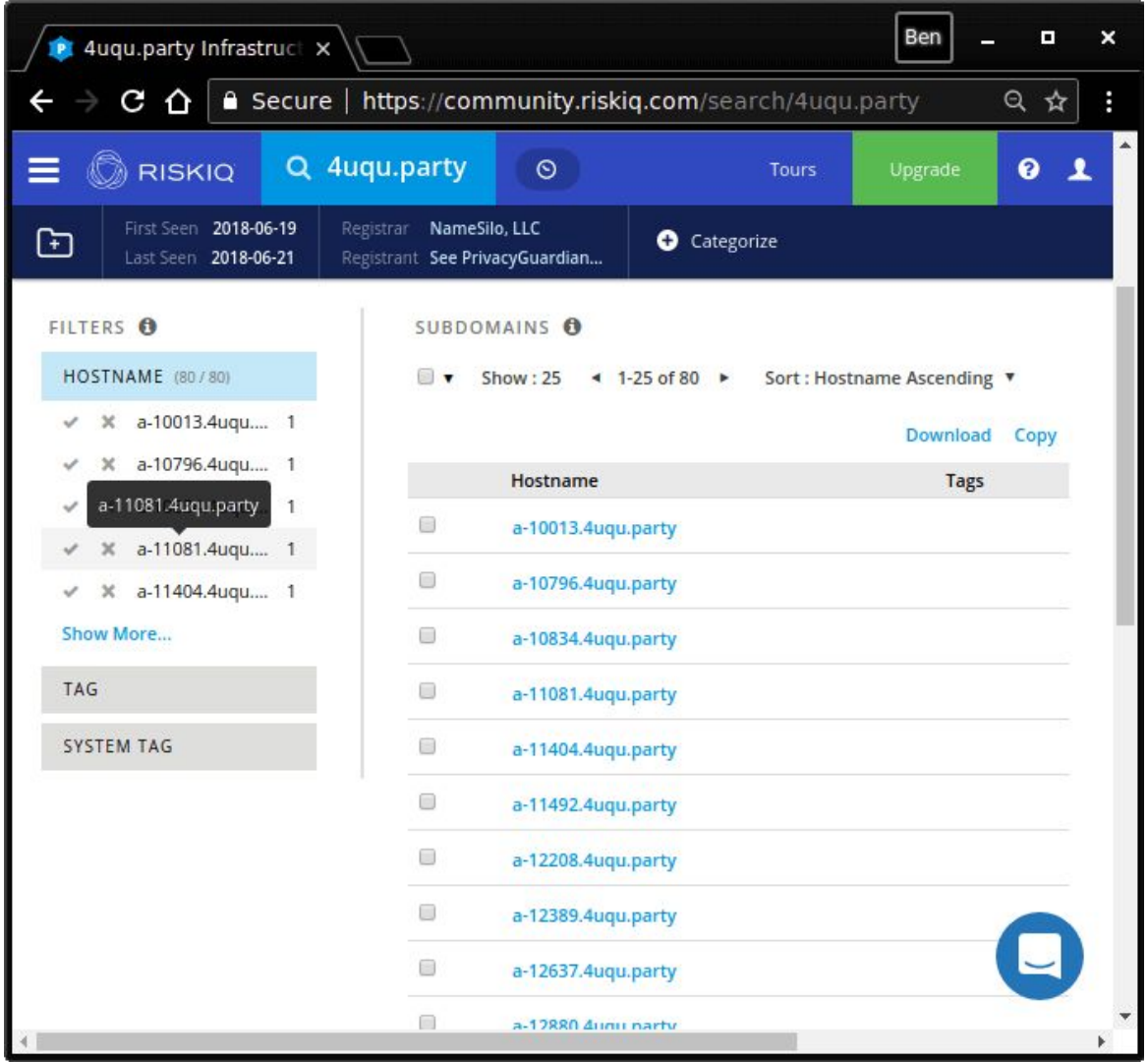
Dear Administrator(s),

Our security system detected an IP address of your responsibility (185.230.223.69) tried to abuse one or more machines in our network. We hope this is the correct emailaddress for abuse reports; if not, please make sure the correct emailaddress is registerd in the registry's WHOIS.

Additionally you may found a X-ARF report attached to this document, with all relevant details for automated complaint parsing. Learn more about X-ARF: http://www.x-arf.org/specification.html

Here's a summary of the abuse:

2018-06-20 01:21:05 CEST Trying to use our servers as DNS resolver


4uqu.party Infrastruct
Ben
Secure | https://community.riskiq.com/search/4uqu.party
RISKIQ
4uqu.party
Tours
Upgrade
First Seen 2018-06-19
Last Seen 2018-06-21
Registrar NameSilo, LLC
Registrant See PrivacyGuardian...
Categorize
FILTERS
HOSTNAME (80 / 80)
a-10013.4uqu.... 1
a-10796.4uqu.... 1
a-11081.4uqu.party 1
a-11081.4uqu.... 1
a-11404.4uqu.... 1
Show More...
TAG
SYSTEM TAG
SUBDOMAINS
Show : 25
1-25 of 80
Sort : Hostname Ascending
Download
Copy
Hostname
Tags
a-10013.4uqu.party
a-10796.4uqu.party
a-10834.4uqu.party
a-11081.4uqu.party
a-11404.4uqu.party
a-11492.4uqu.party
a-12208.4uqu.party
a-12389.4uqu.party
a-12637.4uqu.party

Now the strange stuff

Enter a AS number in the format of "ASXXX" or just freetype a name

Search: Stealth Co

ISP Name = Stealth Communications

Resolvers:

AS	%	Raw Number
Stealth Communications	25 %	1
Google LLC	75 %	3

Search: China TeleCom w

ISP Name = China Telecom Next Generation Carrier Network

Resolvers:

AS	%	Raw Number
Packet Clearing House	0 %	3
Data Communication Business Group	0 %	3
IS	0 %	1
No.31Jin-rong Street	59 %	425
TDS TELECOM	0 %	1
Korea Telecom	0 %	1
China Telecom Next Generation Carrier Network	6 %	47
China Telecom (Group)	0 %	1
China Telecom(Group)	9 %	67
China Telecom (Group)	0 %	2
CHINA UNICOM China169 Backbone	1 %	14
HongKong Commercial Internet Exchange	0 %	1
Hong Kong Broadband Network Ltd.	0 %	1
HGC Global Communications Limited	0 %	1
Guangdong Mobile Communication Co.Ltd.	0 %	2
Google LLC	14 %	101
Emirates Integrated Telecommunications Company PJSC (EITC-DU)	0 %	1
ASN for Shandong Provincial Net of CT	0 %	2
asn for Liaoning Provincial Net of CT	0 %	1
China Unicom IP network China169 Guangdong province	0 %	1
IDC China Telecommunications Corporation	0 %	1
Liquid Telecommunications Ltd	0 %	4


NETFLIX
VINCHA
STRANGER
PINGS
Vincha recordS

DNS 

2018-06-20 05:27:15 IP 197.96.129.180.51587 > 45.76.133.249.53: 32906 [1au] A? a-6848.4uqu.party. (46)
2018-06-20 05:28:51 IP 197.96.129.180.39401 > 45.76.133.249.53: 20872 [1au] ANY? a-6848.4uqu.party. (46)
2018-06-20 05:28:51 IP 197.96.129.180.35844 > 45.76.133.249.53: 2062 [1au] ANY? a-6848.4uqu.party. (46)
2018-06-20 05:28:52 IP 197.96.129.180.60279 > 45.76.133.249.53: 14686 [1au] ANY? a-6848.4uqu.party. (46)

AS6848 Telenet BVBA

ks
- Home
- eport
- port
- port
- s
- outes
- ort
- stics
- s
- s App
- nnel
- tion
- s

AS Info | Graph v4 | Graph v6 | Prefixes v4 | Prefixes v6 | Peers v4 | Peers v6 | Whois | IRR | IX

Company Website: http://www.telenet.be

Country of Origin: Belgium

Internet Exchanges: 1

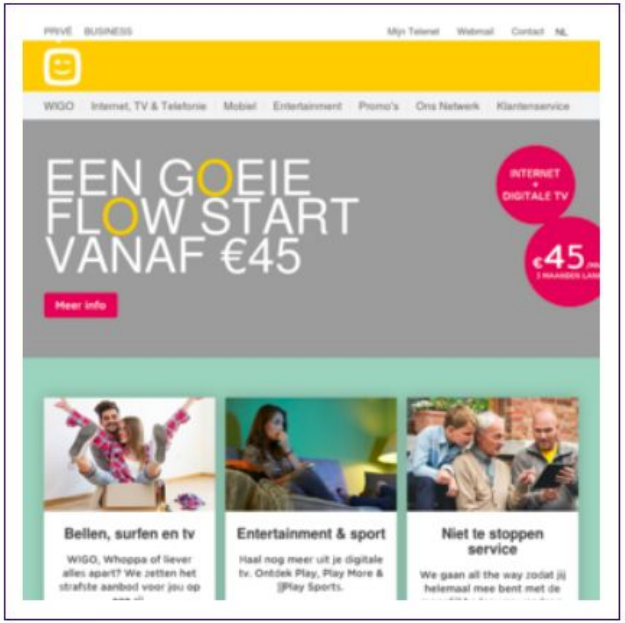
Prefixes Originated (all): 104
Prefixes Originated (v4): 99
Prefixes Originated (v6): 5

Prefixes Announced (all): 266
Prefixes Announced (v4): 242
Prefixes Announced (v6): 24

BGP Peers Observed (all): 46
BGP Peers Observed (v4): 46
BGP Peers Observed (v6): 15

IPs Originated (v4): 2,049,024
AS Paths Observed (v4): 778
AS Paths Observed (v6): 467

Average AS Path Length (all): 3.884
Average AS Path Length (v4): 3.896
Average AS Path Length (v6): 3.863



2018-06-20 05:27:15 IP 197.96.129.180.51587 > 45.76.133.249.53: 32906 [1au] A? a-6848.4uqu.party. (46)
2018-06-20 05:28:51 IP 197.96.129.180.39401 > 45.76.133.249.53: 20872 [1au] ANY? a-6848.4uqu.party. (46)
2018-06-20 05:28:51 IP 197.96.129.180.35844 > 45.76.133.249.53: 2062 [1au] ANY? a-6848.4uqu.party. (46)
2018-06-20 05:28:52 IP 197.96.129.180.60279 > 45.76.133.249.53: 14686 [1au] ANY? a-6848.4uqu.party. (46)

AS3741 Internet Solutions

Quick Links

- BGP Toolkit Home
- BGP Prefix Report
- BGP Peer Report
- Exchange Report
- Bogon Routes
- World Report
- Multi Origin Routes
- DNS Report
- Top Host Report
- Internet Statistics
- Looking Glass
- Network Tools App
- Free IPv6 Tunnel
- IPv6 Certification
- IPv6 Progress
- Going Native
- Contact Us

AS Info | Graph v4 | Graph v6 | Prefixes v4 | Prefixes v6 | Peers v4 | Peers v6 | Whois | IRR | IX

Company Website: http://www.is.co.za
Company Looking Glass: http://local-route-server.is.co.za
Company Route Server: http://local-route-server.is.co.za

Country of Origin: South Africa

Internet Exchanges: 10

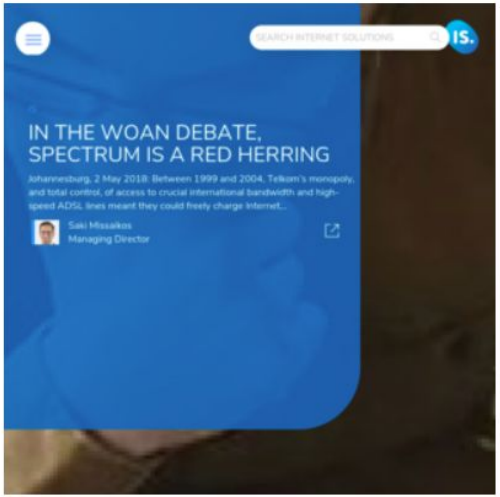
Prefixes Originated (all): 248
Prefixes Originated (v4): 245
Prefixes Originated (v6): 3

Prefixes Announced (all): 704
Prefixes Announced (v4): 687
Prefixes Announced (v6): 17

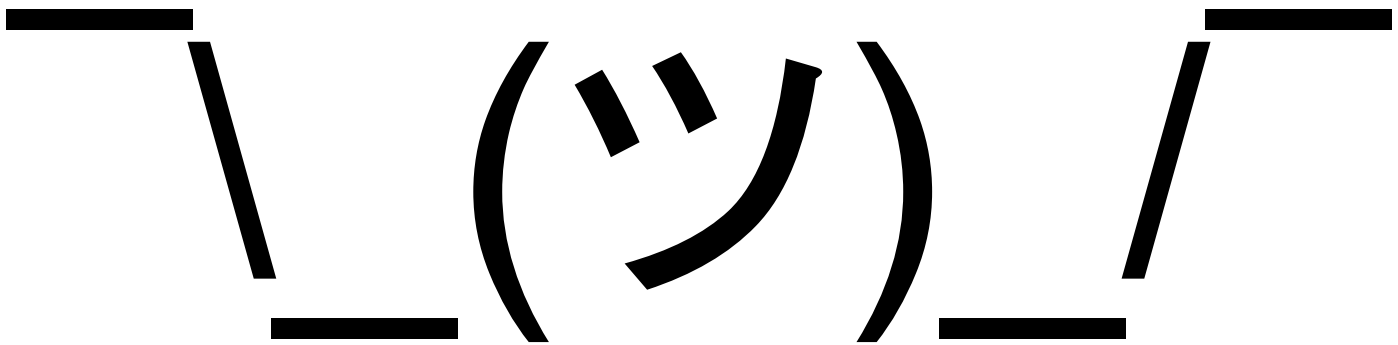
BGP Peers Observed (all): 683
BGP Peers Observed (v4): 674
BGP Peers Observed (v6): 375

IPs Originated (v4): 3,013,376
AS Paths Observed (v4): 94,069
AS Paths Observed (v6): 19,460

Average AS Path Length (all): 4.141
Average AS Path Length (v4): 4.165
Average AS Path Length (v6): 4.029



¯_(ツ)_/¯



The internet is motivated by politics and money

Not by logic