
caida

.inf
INSTITUTO
DE INFORMÁTICA
UFRGS

disclaimer: half-baked ideas

Biggest DDoS Attack on Record Hits Github

The IT infrastructure that powered Wednesday's attack is ripe for abuse, security firms say.

By Michael Kan March 1, 2018 7:40PM EST

PC REVIEWS BEST PICKS HOW-TO NEWS TIPS BUSINESS EXPLORE SHOP

Biggest Github

The IT infrastructu

By Michael Ka

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTUR

RECORD FLOODS —

US service provider survives the biggest recorded DDoS in history

Nearly 100,000 memcached servers are imperiling the stability of the Internet.

DAN GOODIN - 3/5/2018, 1:24 PM

caida .inf INSTITUTO DE INFORMÁTICA UFRGS

PC REVIEWS BEST PICKS HOW-TO NEWS TIPS BUSINESS EXPLORE SHOP

Biggest Github

The IT int

By M

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTUR

s the biggest

y of the Internet.

ARBOR NETWORKS
The Security Division of NETSCOUT

Attack Map Archives About

BLOG HOME CORPORATE SITE RSS

NETSCOUT Arbor Confirms 1.7 Tbps DDoS Attack; The Terabit Attack Era Is Upon Us

Carlos Morales on March 5, 2018.

caida

.inf INSTITUTO DE INFORMÁTICA UFRGS

PC REVIEWS BEST PICKS HOW-TO NEWS TIPS BUSINESS EXPLORE SHOP

Biggest
Github

The IT int

By

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTUR

The S

ZDNet VIDEOS SMART CITIES WINDOWS 10 CLOUD INNOVATION SECURITY TECH PRO MORE NEWSLETTERS ALL WRIT

JUST IN WHAT IS V2X COMMUNICATION? CREATING CONNECTIVITY FOR THE AUTONOMOUS CAR ERA

Brazil hit by 30 DDoS attacks per hour in 2017

The country is part of a global ranking of the five nations most targeted by cybercriminals, says study.

By Angelica Mari for Brazil Tech | February 21, 2018 -- 14:59 GMT (06:59 PST) | Topic: Security

N
1.

Terabit Attack Era is Upon Us

Carlos Morales on March 5, 2018.

caida

.inf INSTITUTO DE INFORMÁTICA UFRGS

IP spoofing is a
well-known problem

a key component
of such DDoS attacks

addressing spoofing

- attempts to eliminate spoofing, not adopted
- IETF BCPs 38-84, ISOC MANRS
- scrubbing centers (eg Akamai, Cloudflare, Level 3 Anti-DDoS)
- measure use of source address validation (against spoofing)
- the Spoofer project

methodology and corresponding tools
to detect spoofed traffic
in network traces

enable SAV compliance tests
for **IXP** networks

more on expected results

- methodology and the analysis results of the prevalence, causes, and impact of IP source spoofing (observed in IXPs)
- create a tool that enables IXPs to perform compliance tests on SAV, make it available to networking community
- longitudinal measurement about adoption of SAV and filtering after we deployed our tool

what could go wrong?

what could go wrong?

- no collaboration from network operators
- no access to commercial traffic and client information
- coarse-grained data only, eg no flow information
- anonymized data
- overwhelming resource demands to transfer, storage and process data

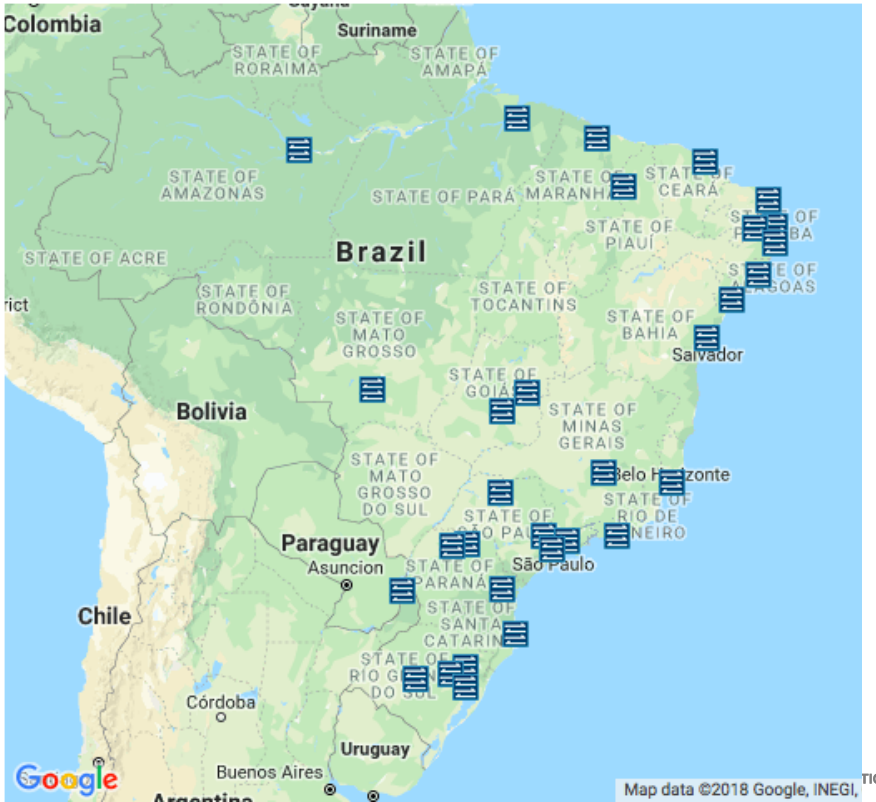
current status

- access to detailed data from a large IXP
- expanding access to other vantage points
- developing a processing pipeline: transformation and processing (filtering and classification) of (i) bogon, (ii) unrouted, and (iii) AS-specific traffic

where could we apply this?

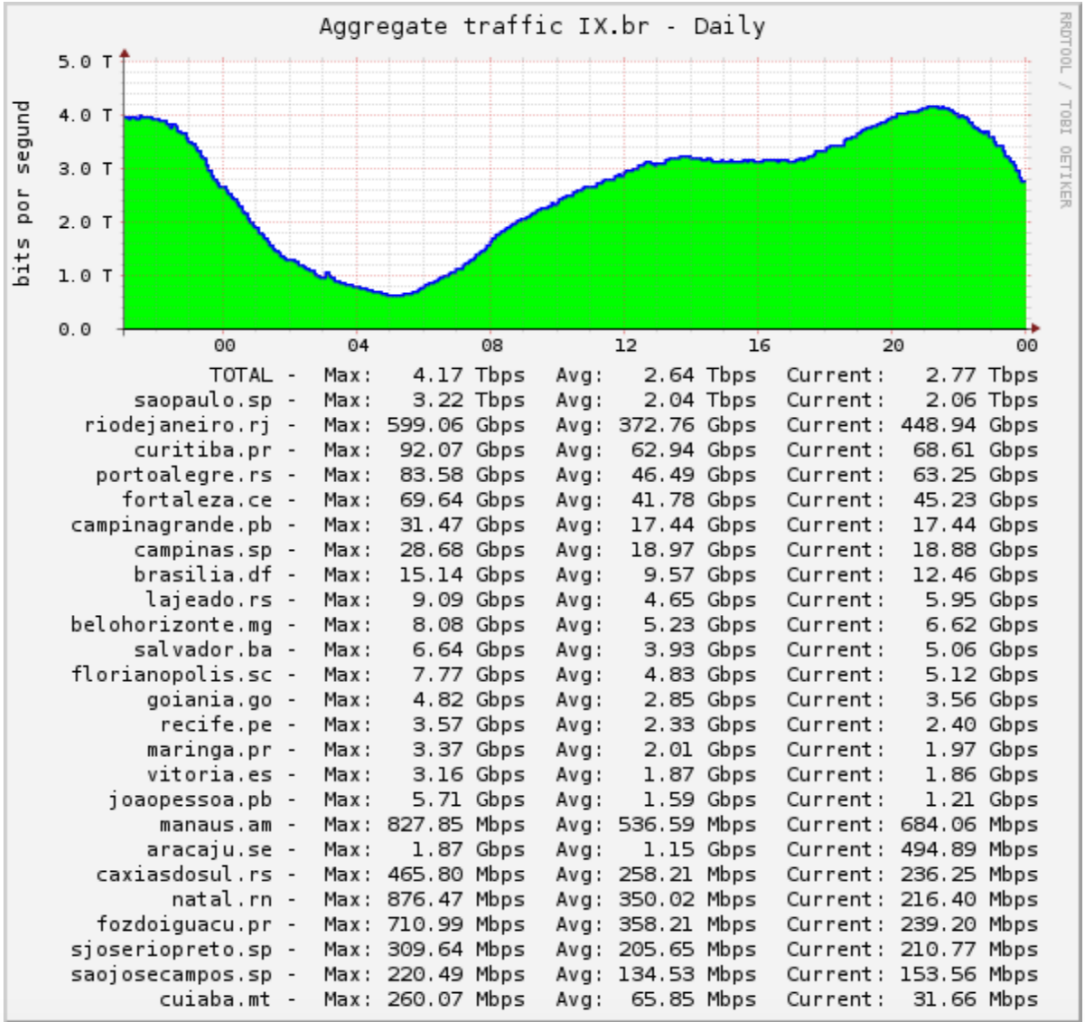
Brazilian IX.br ecosystem

- over **5.3k ASes**
- **30 IXPs** unevenly distributed in 27 states
- total of **~2,300** member ASes, **~1,650** distinct ones
- **~102** colocation facilities (directly connected to the IX.br)
- **~4.4 Tb/s** average traffic peak over the last 30 days for all IX.br ecosystem



Brazilian IX.br ecosystem

- over **5.3k ASes**
- **30 IXPs** unevenly distributed in 27 states
- total of **~2,300** member ASes, **~1,650** distinct ones
- **~102** colocation facilities (directly connected to the IX.br)
- **~4.4 Tb/s** average traffic peak over the last 30 days for all IX.br ecosystem



TOTAL	-	Max:	4.17 Tbps	Avg:	2.64 Tbps	Current:	2.77 Tbps
saopaulo.sp	-	Max:	3.22 Tbps	Avg:	2.04 Tbps	Current:	2.06 Tbps
riodejaneiro.rj	-	Max:	599.06 Gbps	Avg:	372.76 Gbps	Current:	448.94 Gbps
curitiba.pr	-	Max:	92.07 Gbps	Avg:	62.94 Gbps	Current:	68.61 Gbps
portoalegre.rs	-	Max:	83.58 Gbps	Avg:	46.49 Gbps	Current:	63.25 Gbps
fortaleza.ce	-	Max:	69.64 Gbps	Avg:	41.78 Gbps	Current:	45.23 Gbps
campinagrande.pb	-	Max:	31.47 Gbps	Avg:	17.44 Gbps	Current:	17.44 Gbps
campinas.sp	-	Max:	28.68 Gbps	Avg:	18.97 Gbps	Current:	18.88 Gbps
brasilia.df	-	Max:	15.14 Gbps	Avg:	9.57 Gbps	Current:	12.46 Gbps
lajeado.rs	-	Max:	9.09 Gbps	Avg:	4.65 Gbps	Current:	5.95 Gbps
belohorizonte.mg	-	Max:	8.08 Gbps	Avg:	5.23 Gbps	Current:	6.62 Gbps
salvador.ba	-	Max:	6.64 Gbps	Avg:	3.93 Gbps	Current:	5.06 Gbps
florianopolis.sc	-	Max:	7.77 Gbps	Avg:	4.83 Gbps	Current:	5.12 Gbps
goiania.go	-	Max:	4.82 Gbps	Avg:	2.85 Gbps	Current:	3.56 Gbps
recife.pe	-	Max:	3.57 Gbps	Avg:	2.33 Gbps	Current:	2.40 Gbps
maringa.pr	-	Max:	3.37 Gbps	Avg:	2.01 Gbps	Current:	1.97 Gbps
vitoria.es	-	Max:	3.16 Gbps	Avg:	1.87 Gbps	Current:	1.86 Gbps
joaopessoa.pb	-	Max:	5.71 Gbps	Avg:	1.59 Gbps	Current:	1.21 Gbps
manaus.am	-	Max:	827.85 Mbps	Avg:	536.59 Mbps	Current:	684.06 Mbps
aracaju.se	-	Max:	1.87 Gbps	Avg:	1.15 Gbps	Current:	494.89 Mbps
caxiasdosul.rs	-	Max:	465.80 Mbps	Avg:	258.21 Mbps	Current:	236.25 Mbps
natal.rn	-	Max:	876.47 Mbps	Avg:	350.02 Mbps	Current:	216.40 Mbps
fozdoiguacu.pr	-	Max:	710.99 Mbps	Avg:	358.21 Mbps	Current:	239.20 Mbps
sjoseriopreto.sp	-	Max:	309.64 Mbps	Avg:	205.65 Mbps	Current:	210.77 Mbps
saojosecampos.sp	-	Max:	220.49 Mbps	Avg:	134.53 Mbps	Current:	153.56 Mbps
cuiaba.mt	-	Max:	260.07 Mbps	Avg:	65.85 Mbps	Current:	31.66 Mbps

ix.br daily traffic breakdown

caida

.inf INSTITUTO DE INFORMÁTICA UFRGS

we need *validation*

- scientific contribution?
- confirm/challenge previous work?
- perform IPv6 analysis?
- correlate with IPv4 space grey-market address transfers?
- locate and investigate malicious ASes in BGP AS-Path?
- security hygiene best practices?
- …

Using IXPs to Measure Improvements in Source Address Validation Filtering of Inter-Domain Traffic

Lucas Muller, **Marinho Barcellos**,
Bradley Huffaker, Matthew Luckie, kc claffy

AIMS 2018

.inf
INSTITUTO
DE INFORMÁTICA
UFRGS