nic.br cgi.br | cert.br

Foz do Iguaçu, PR, Brazil
May 22, 2017
LAC-CSIRTs

Notable trends in Brazil: BGP Hijacking for financial fraud and the evolution of Mirai

Cristine Hoepers
General Manager
cristine@cert.br

Klaus Steding-Jessen
Technical Manager
jessen@cert.br

cert.br nic.br cgi.br

BGP Hijacking for Financial Fraud

cert.br nic.br cgi.br

Case 1

Period:

- 2017-03-26 13h
- 2017-03-26 16h

Routers:

- Juniper ACX
- Mikrotik 1009

Prefixes:

- /24 of the Internet Banking
- Two /24 of a public DNS service
- One /24 of a big CDN

GRE tunnels to:

- Hosting provider A (HTTP)
- Hosting provider B (DNS)

Case 2

Period:

- 2017-03-29 22h
- 2017-03-30 09h

Router:

- Mikrotik

Prefix:

- /24 of the Internet Banking

Tunnel:

- unknown

Case 3 – has not replied to notifications

Period:

- 2017-04-11 2h
- 2017-04-11 3h

Router:

- unknown

Prefix:

- /24 of the Internet Banking

Tunnel:

- unknown

Case 4

Period:

- 2017-04-21 11h
- 2017-04-21 13h

Router/server:

- Compromised a Ubuntu server, used to manage the router
- Mikrotik router compromised via Ubuntu

Prefixes:

- Old /24 of the Internet Banking
- New /24 of the Internet Banking

GRE tunnel to:

- Hosting provider C (HTTP)

Recommendations

1. Monitoring:

- BGPmon
  - https://bgpmon.net
- BGPStream
  - https://twitter.com/bgpstream
  - http://bgpstream.caida.org
- Scripts to query looking glass servers
  - Ex: telnet://lg.saopaulo.sp.ix.br

2. Annouce more specific prefix (/24)

- for the networks that host critical services
  - example: internet banking

3. Connect to an Internet eXchange point

- shortest *path* possible to the neighboring networks

Mirai Evolution

cert.br nic.br cgi.br

Source of the Mirai data

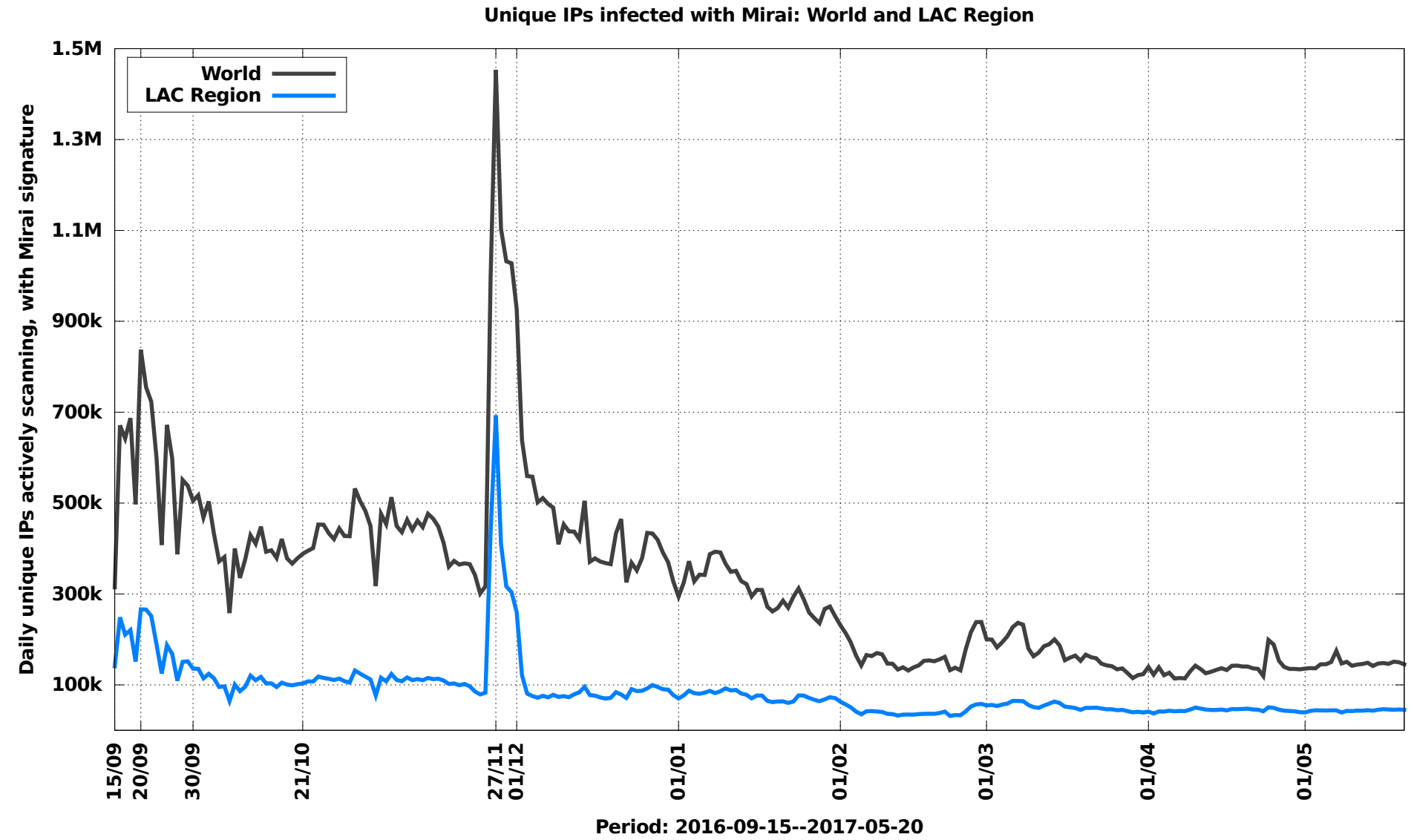
- **Traffic captured in our distributed network of honeypots**

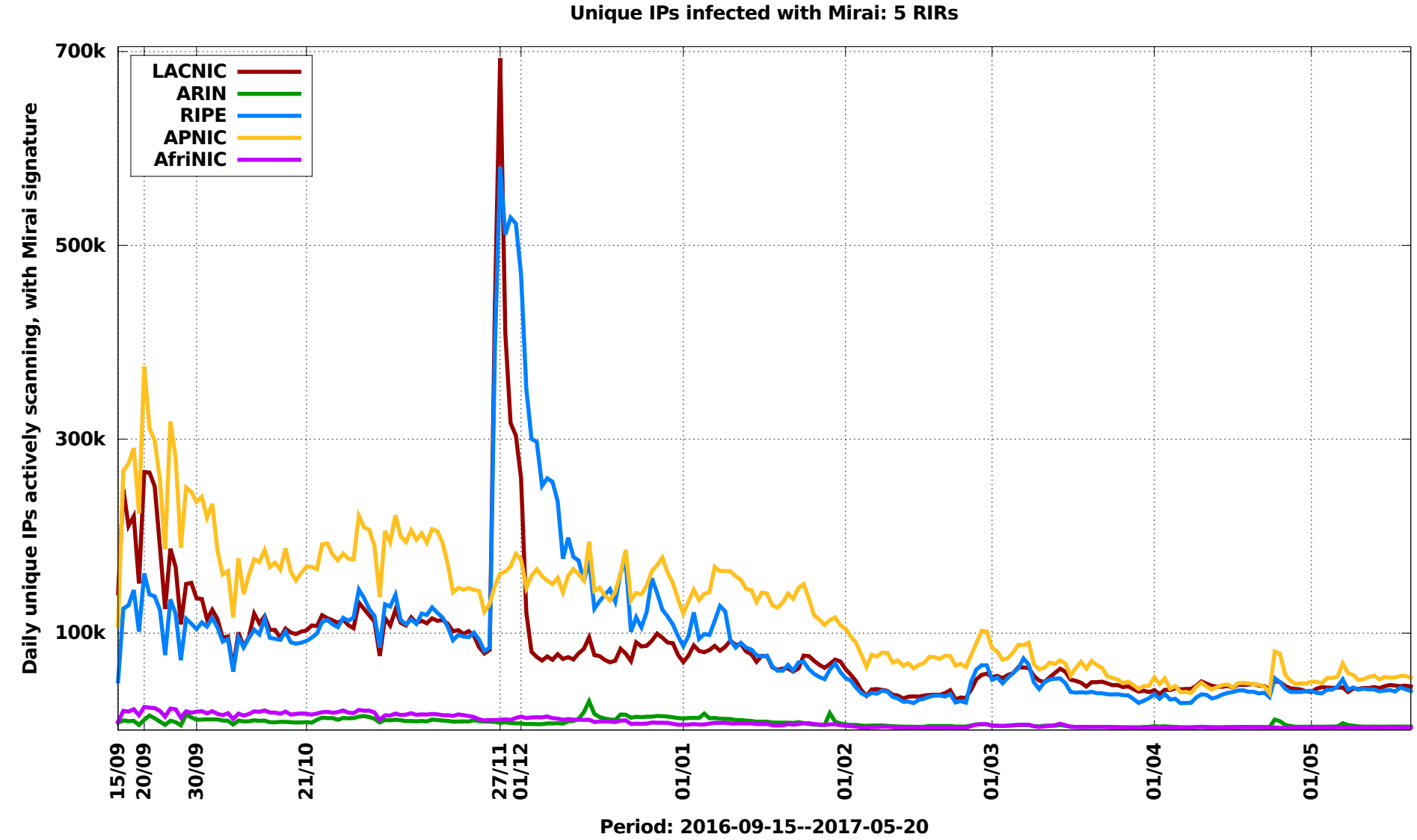
  https://honeytarg.cert.br/honeypots/

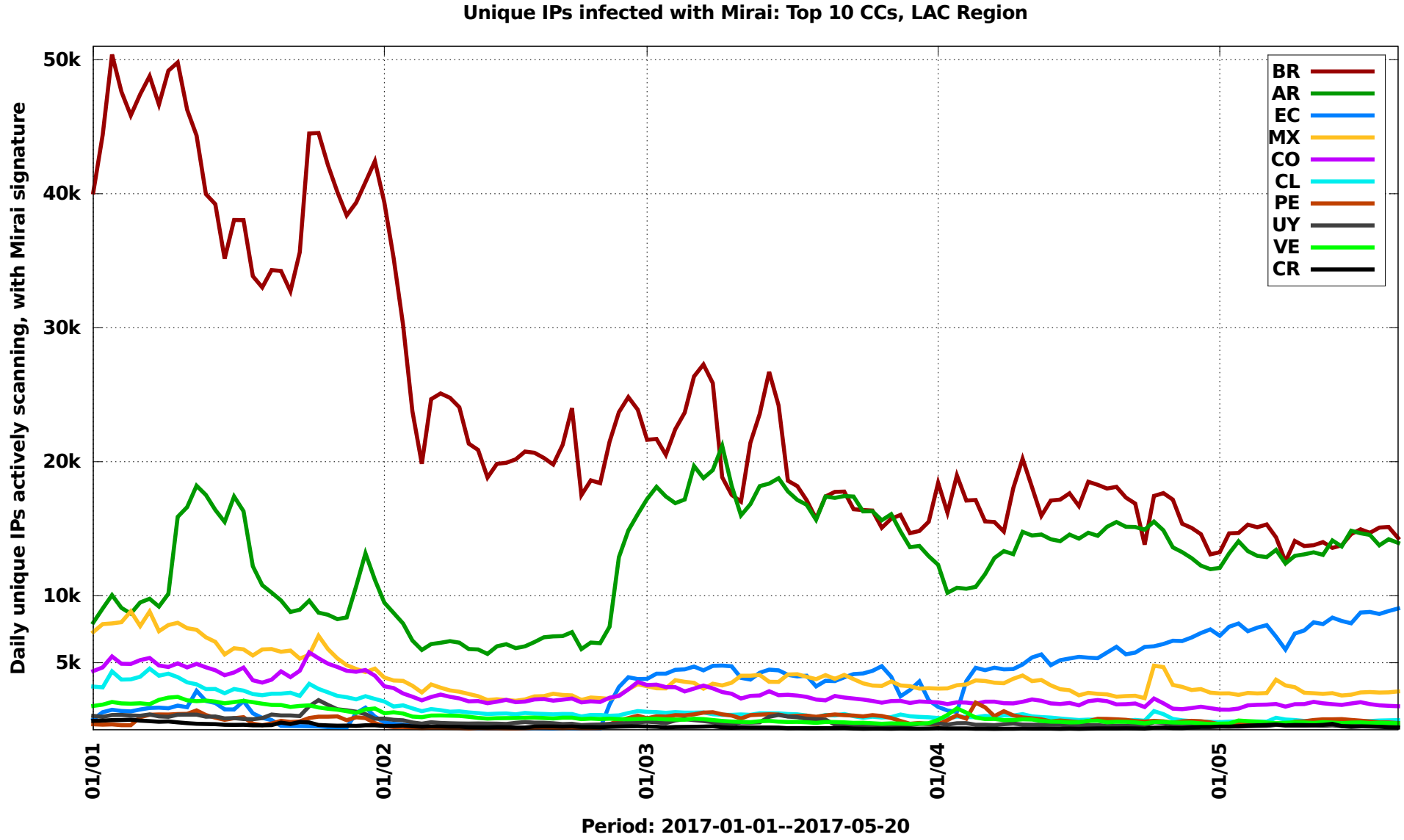
- **Identifies a very specific Mirai scanning signature**
  - **scanning for ports 23, 2323, 7547, 5555, 23231, 37777, 6789, 22, 2222 and 81**

- **It is the metric being used for Mirai by CyberGreen**

  https://stats.cybergreen.net/


Unique IPs infected with Mirai: World and LAC Region
World
LAC Region
Daily unique IPs actively scanning, with Mirai signature
1.5M
1.3M
1.1M
900k
700k
500k
300k
100k
15/09
20/09
30/09
21/10
27/11
01/12
01/01
01/02
01/03
01/04
01/05
Period: 2016-09-15--2017-05-20


Unique IPs infected with Mirai: 5 RIRs
Daily unique IPs actively scanning, with Mirai signature
700k
500k
300k
100k
LACNIC
ARIN
RIPE
APNIC
AfriNIC
15/09
20/09
30/09
21/10
27/11
01/12
01/01
01/02
01/03
01/04
01/05
Period: 2016-09-15--2017-05-20


Unique IPs infected with Mirai: Top 10 CCs, LAC Region
Daily unique IPs actively scanning, with Mirai signature
50k
40k
30k
20k
10k
5k
BR
AR
EC
MX
CO
CL
PE
UY
VE
CR
01/01
01/02
01/03
01/04
01/05
Period: 2017-01-01--2017-05-20

Obrigado
Gracias
Thank You

www.cert.br

cristine@cert.br jessen@cert.br @certbr

May 22, 2017

nic.br cgi.br

www.nic.br | www.cgi.br