



nic.br egi.br

cert.br

San Juan, PR

June 16, 2017

National CSIRTs Meeting 2017

The background of the slide is a dark gray circuit board pattern with white lines representing traces and components. The pattern is dense and covers the entire area.

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

**Cristine Hoepers
General Manager
cristine@cert.br**

cert.br nic.br cgi.br

The background of the slide is a dark gray circuit board pattern with white lines representing traces and components. The top and bottom sections of the slide feature this pattern, while the middle section is a solid light gray gradient.

This slide set is TLP: WHITE

cert.br nic.br cgi.br

The background of the slide is a dark gray circuit board pattern with white lines representing traces and components. The top and bottom sections of the slide feature this pattern, while the middle section is a solid light gray gradient.

BGP Hijacking for Financial Fraud

cert.br nic.br cgi.br

Case 1

Period:

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

Prefixes:

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

Routers:

- Juniper ACX
- Mikrotik 1009

GRE tunnels to:

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

Case 2

Period:

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

Prefix:

- /24 of the Internet Banking

Router:

- Mikrotik

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)

Case 5 – denies that it has ever happened

Period:

- 2017-05-24 19h
- 2017-05-24 20h
- 2017-05-29 16h
- 2017-05-29 ??h

Router/server:

- Unknown

Prefixes:

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

GRE tunnel:

- unknown

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. Announce a 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

The background of the slide is a dark gray circuit board pattern with white lines representing traces and components. The pattern is symmetrical and fills the entire frame.

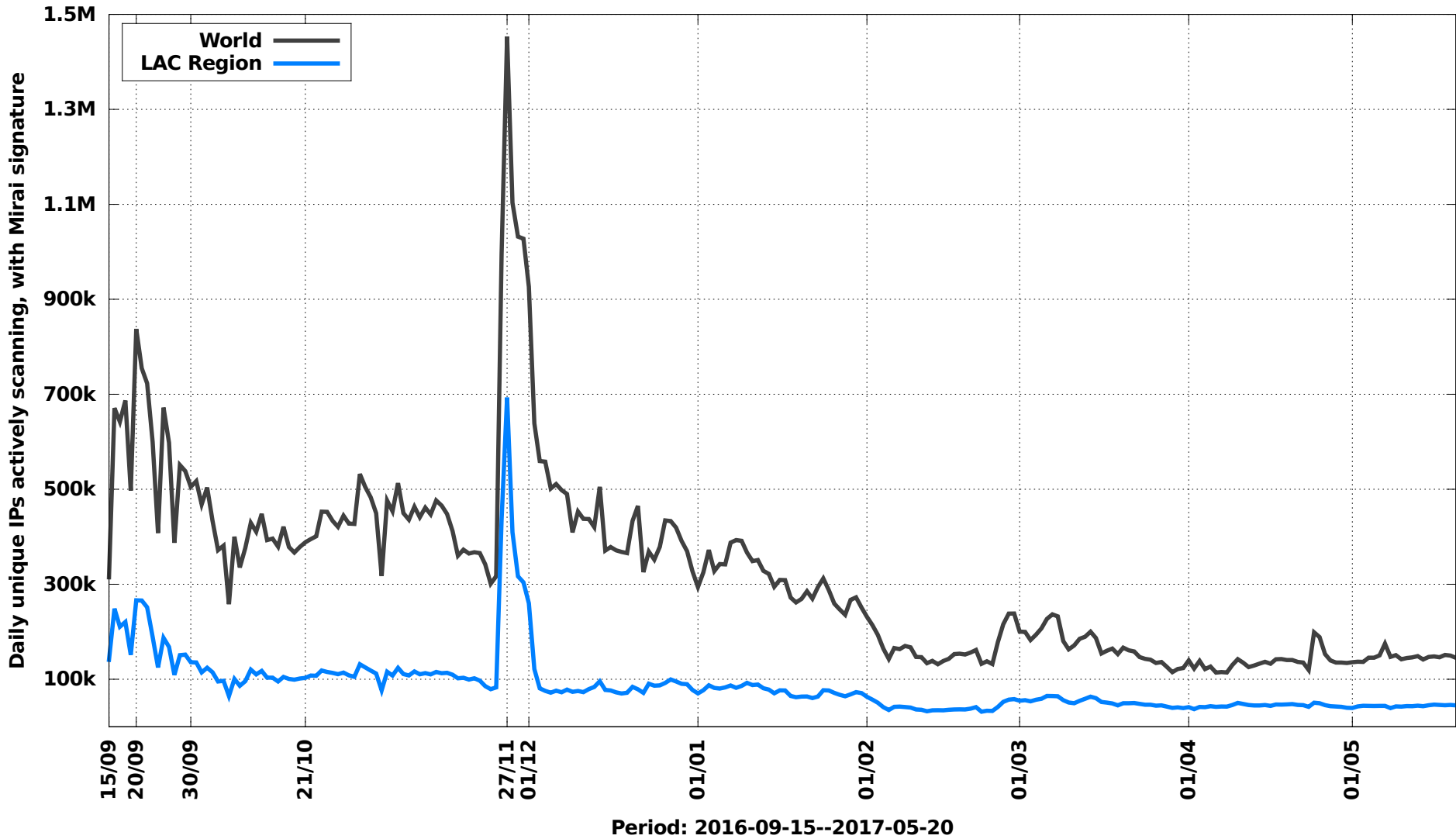
Mirai Evolution

cert.br nic.br cgi.br

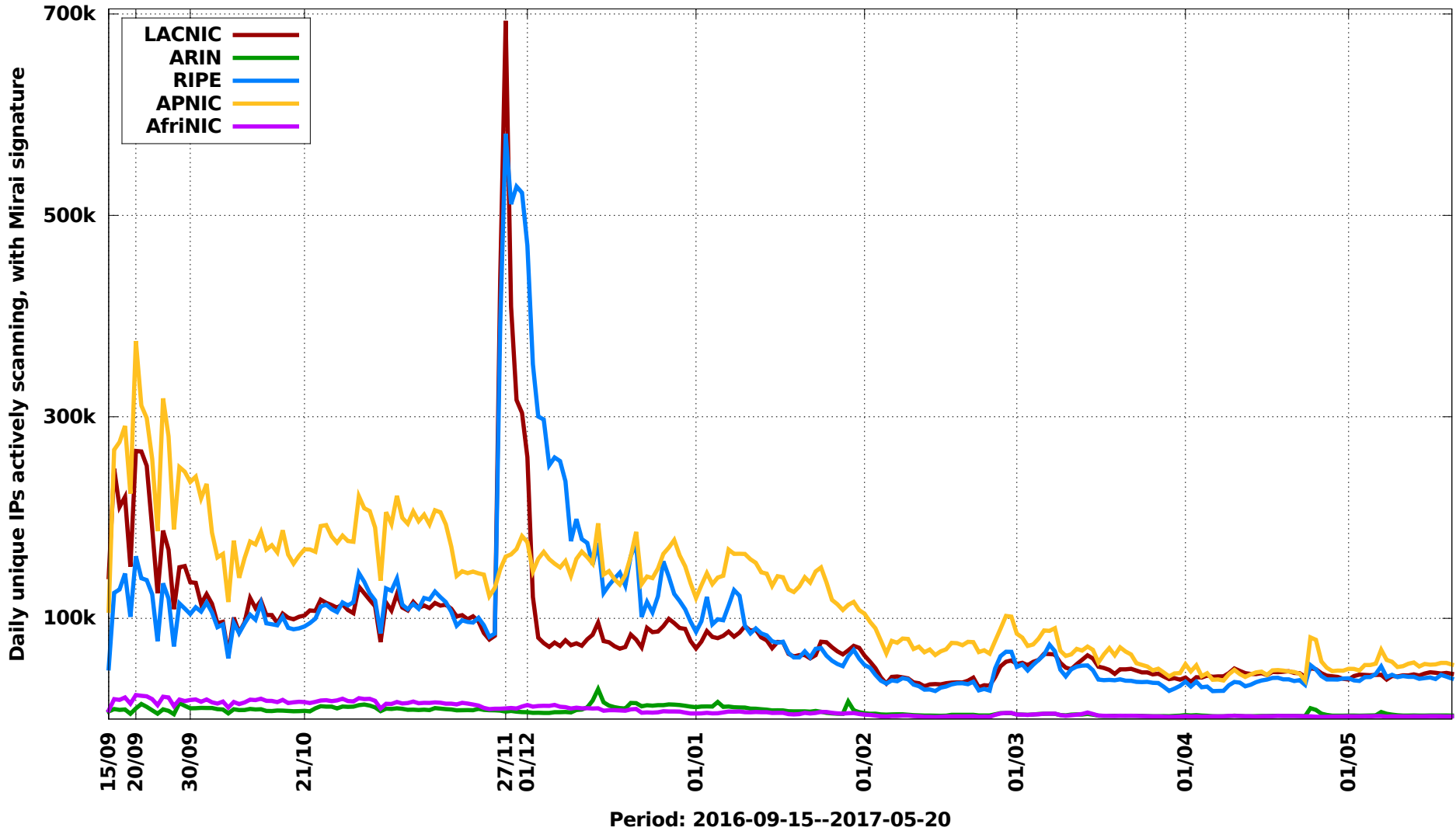
Source of the Mirai data

- **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/>

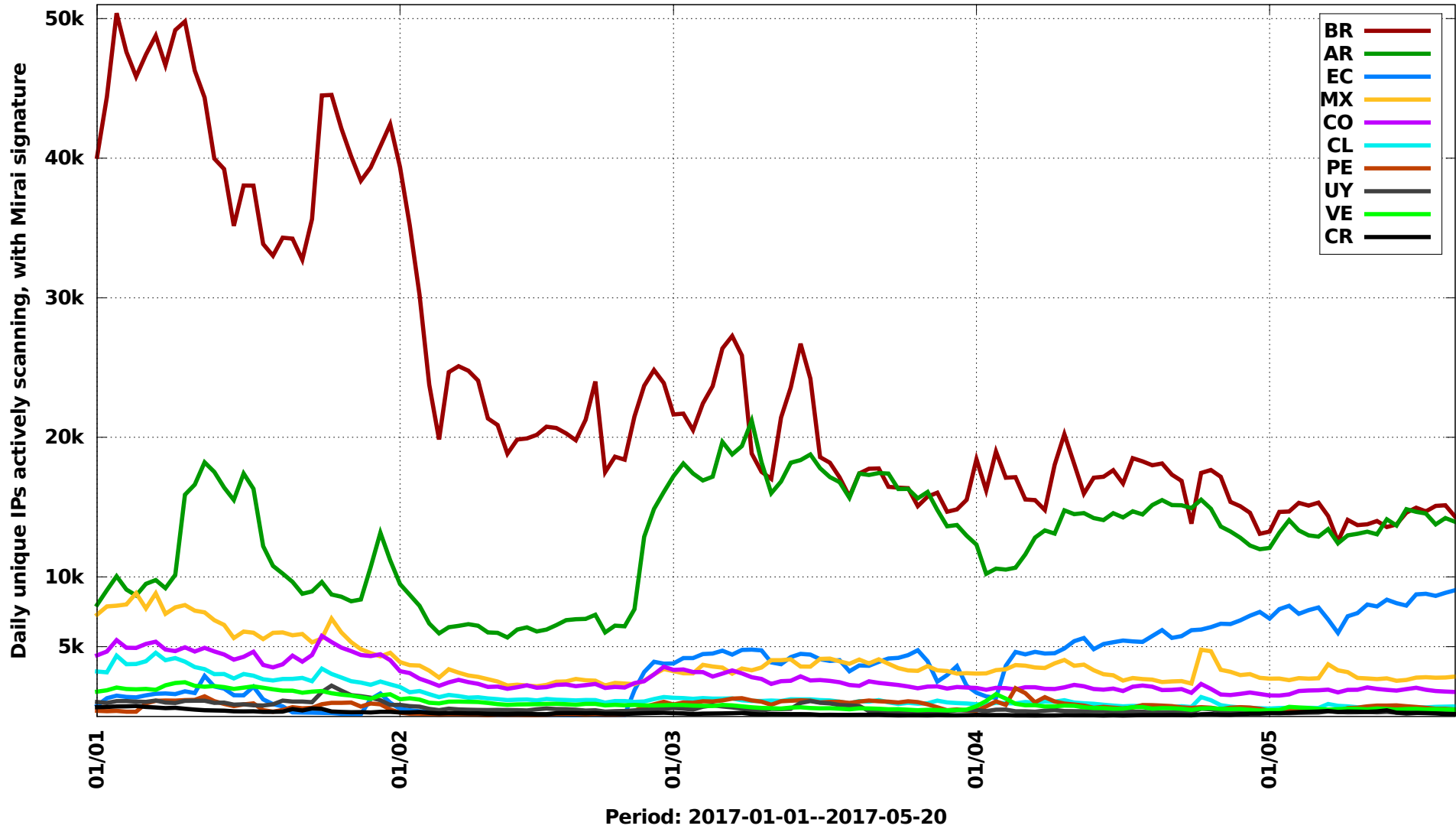
Unique IPs infected with Mirai: World and LAC Region



Unique IPs infected with Mirai: 5 RIRs



Unique IPs infected with Mirai: Top 10 CCs, LAC Region



Thank You

www.cert.br

 cristine@cert.br

 [@certbr](https://twitter.com/certbr)

June 16, 2017

nic.br **cgi.br**

www.nic.br | www.cgi.br