

The logo for NIC.br features the text "nic.br" in a bold, sans-serif font. The ".br" is a vibrant green color, while "nic" is black. Below the text, the full name "Brazilian Network Information Center" is written in a smaller, black, sans-serif font.

nic.br
Brazilian Network
Information Center

The logo for EGI.br features the text "egi.br" in a bold, sans-serif font. The ".br" is a vibrant green color, while "egi" is black. Below the text, the full name "Brazilian Internet Steering Committee" is written in a smaller, black, sans-serif font.

egi.br
Brazilian Internet
Steering Committee

A horizontal row of six domain logos: "registro.br", "cert.br", "cetic.br", "ceptro.br", "ceweb.br", and "ix.br". Each logo has its ".br" in green and the rest in white. They are set against a dark grey background with a circuit-like pattern.

registro.br cert.br cetic.br ceptro.br ceweb.br ix.br



1 2 3 4 5 6 7 8 9

GOVERNMENT (Appointed)

10 11 12 13 14 15 16 17 18 19 20 21

CIVIL SOCIETY (Elected)

e

Government Representatives:

- 1 Ministry of Science and Technology (Coordination)
- 2 Presidential Cabinet
- 3 Ministry of Communications
- 4 Ministry of Defense
- 5 Ministry of Development, Industry and Foreign Trade
- 6 Ministry of Planning, Budget and Management
- 7 National Telecommunications Agency
- 8 National Council of Scientific and Technological Development
- 9 National Forum of Estate Science and Technology Secretaries

Civil Society Representatives:

- 10 Internet Expert
- 11 a 14 General Business Sector Users
Internet Service Providers
Telecommunication Infrastructure Providers
Hardware and Software Industries
- 15 a 18 Non-governmental Entity
- 19 a 21 Academia

CGI.br members and former members
(only the current members have right to vote)

GENERAL ASSEMBLY

7 members elected by the General Assembly

ADMINISTRATIVE
COUNCIL

AUDIT
COMMITTEE

ADMINISTRATION
.....
LEGAL
.....
COMUNICATION
.....
ADVISORIES:
CGI.br and PRESIDENT

EXECUTIVE
BOARD

1 2 3 4 5

registro.br

Domain Registration
IP Assignment

cert.br

Security and
Incident Response

cetic.br

Studies and Surveys
About ICT use

ceptro.br

Internet Engineering
and New Projects

ceweb.br

Web Technologies

ix.br

Traffic Exchange

W3C
Brasil

Web Standards

- 1 Chief Executive Officer
- 2 Administrative and Financial Director
- 3 IT and Services Director
- 4 Director of Special Projects and Development
- 5 Consulting Director for CGI.br activities

INTERNET SECURITY IN BRAZIL - MANRS

PROGRAM FOR A SAFER INTERNET

Gilberto Zorello <gzorello@nic.br>

Future Internet Technology Workshop – São Paulo - 3/20/2019

registro.br nic.br cgi.br

Internet Security and Stability

Current Internet Structure

The Internet works on the basis of cooperation between Autonomous Systems:

- It is a “**network of networks**”
- There are over **60,000** different core networks (Autonomous Systems) across the Internet under independent technical management
- **The BGP routing structure works on the basis of cooperation and trust**
- BGP has no data validation.
- **Result: there is no day that Internet Security incidents do not occur**



BGP has no validation for the data Which Leads To ...

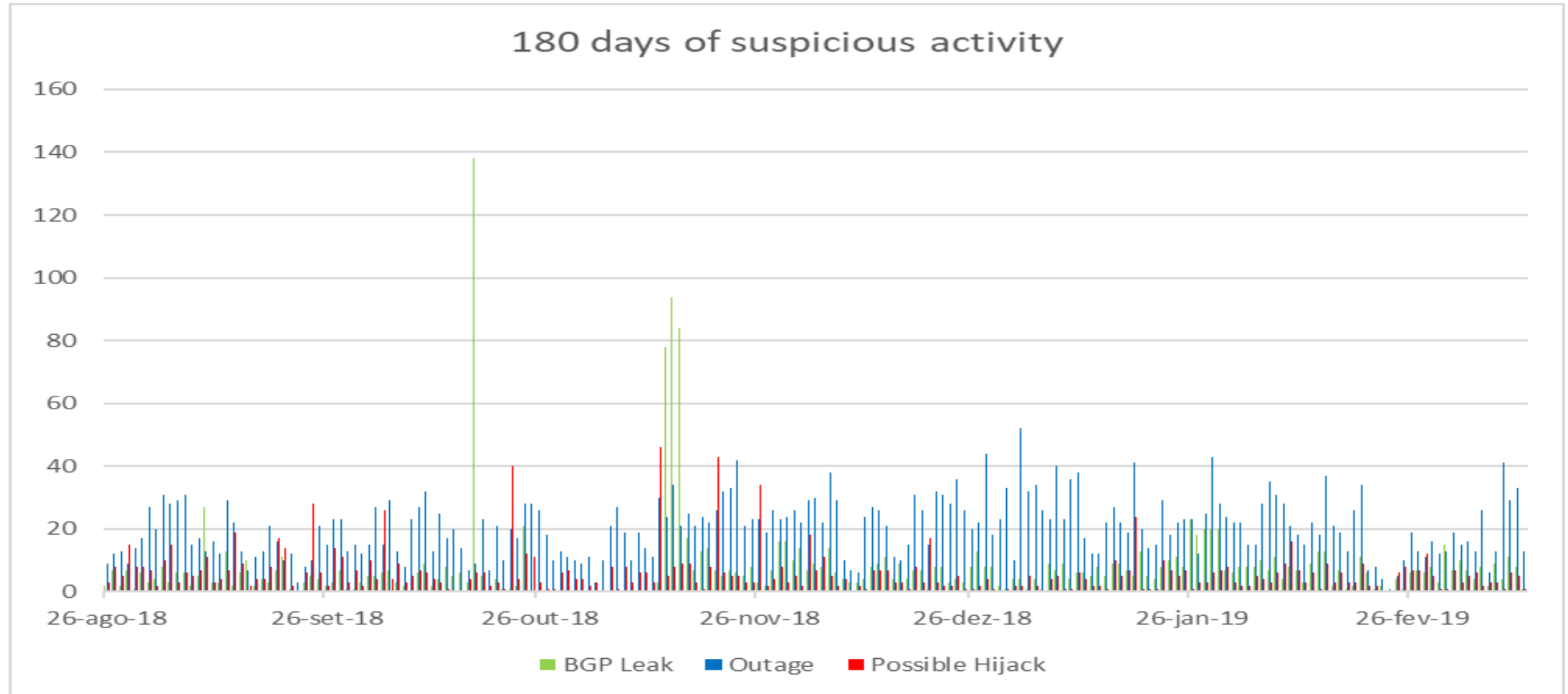
The collage features several news snippets from CNET and CSO:

- CNET Article:** "How Pakistan knocked YouTube offline (and how to make sure it never happens again)". Subtitle: "Large scale BGP hijack out of India". Posted by Andree Toonk - November 6, 2015 - Hijack - 1 Comment.
- CNET Article:** "Routing Leak briefly takes down Google". Posted by Doug Madory - March 12, 2015 - COMMENTS (35) - VIEWS: 37374 - ENGINEERING, INTERNET, LATENCY, PERFORMANCE, SECURITY.
- CNET Article:** "Massive route leak causes internet slowdown". Posted by Andree Toonk - June 12, 2015 - BGP Instability - No Comments.
- CNET Article:** "Global Collateral Damage of TMnet leak". Posted by Doug Madory - June 12, 2015 - COMMENTS (1) - VIEWS: 41213 - SECURITY, UNCATEGORIZED.
- CNET Article:** "DDoS Attacks Storm Linode Servers Worldwide". BY DOUGLAS BONDERUD • JANUARY 5, 2016.
- CNET Article:** "On-going BGP Hijack Targets Palestinian ISP". Posted by Doug Madory - January 12, 2016 - UNCATEGORIZED.
- CNET Article:** "UK traffic diverted through Ukraine". Posted by Doug Madory - March 13, 2015 - COMMENTS (34) - VIEWS: 47297 - SECURITY.
- CNET Article:** "Global Impacts of Recent BGP Hijacking". Posted by Doug Madory - October 14, 2015 - COMMENTS (2) - VIEWS: 9681 - PERFORMANCE, SECURITY.
- Table:** A table titled "Global Impacts of Recent BGP Hijacking" with columns: Event type, Country, ASN, and Start time.
- CNET Article:** "BGP hijack incident by Syrian Telecommunication". Posted by Andree Toonk - December 9, 2014 - Hijack - 2 Comments.
- CNET Article:** "The Vast World of Fraudulent Routing". Posted by Doug Madory - January 29, 2015 - COMMENTS (17) - VIEWS: 36909 - SECURITY.
- CSO Article:** "DDoS attack on BBC may have been biggest in history". Home > Data Protection > Cyber Attacks/Espionage.

Event type	Country	ASN	Start time
BGP Leak		Origin AS: PO box T511 Phonexay road - Xaysettha district (AS 131267) Leaker AS: Viettel Corporation (AS 7552)	2016-01-13 12:25:47
BGP Leak		Origin AS: Lirex net EOOD (AS 8262) Leaker AS: Traffic Broadband Communications Ltd. (AS 48452)	2016-01-13 12:11:26

Internet Security and Stability

No day without an incident



Internet Security and Stability

Current Situation

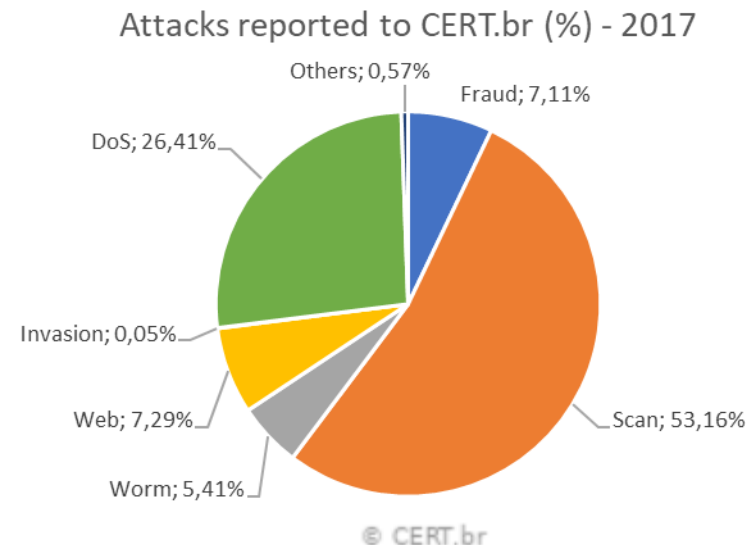
Attacks on the infrastructure and services available on the Internet are increasingly common

NIC.br examines the tendency of the attacks with data obtained by:

- Handling of security incidents
- Measurements on honeypots distributed over the Internet
- Measurements on IX.

There is an increasing rate of notifications of scans, frauds and DDoS

Network security is critical to securing the future of the Internet so that it can remain open and diverse and grow with today's business models and new models that will reliably utilize new technologies.



Program for Safer Internet Initiative



Launched by CGI.br e NIC.br

IX Forum 11 in Dec / 17



Support: Internet Society and Brazilian Associations of Internet Service Providers

Objective: to act in support of the Internet technical community to:

- Reduce Denial of Service attacks originating in Brazilian networks
- Reduce the Prefix Hijacking, Route Leak, and Source IP Spoofing
- Reduce the vulnerabilities and configuration failures in network elements
- Approach the different teams responsible for network security and stability
- **Create a culture of security**

Program for Safer Internet Action Plan

To solve the security problems, the actions must be carried out by the operators of the AS, with the support of NIC.br

Coordinated actions to be performed by NIC.br:

- Raising awareness through lectures, courses and trainings
- **Creating educational materials and best practices**
- Interaction with Provider Associations and their affiliates for dissemination of the Safety Culture, adoption of Best Practices, as **MANRS**, and mitigation of existing problems
- **Implementation of route filters at IX.br, which contributes to the improvement of the general scenario**
- Establishment of metrics and monitoring the effectiveness of actions



Program for Safer Internet

Necessary actions of the technical community

- **Close the vulnerable open service ports that allow amplification attacks**
 - Configure properly services opened that can be abused in amplification attacks, as specified at CERT.br notifications
- **Implement the actions recommended by MANRS**
 - Filtering of routes and false origin addresses (antispoofing), and information for collaborative actions among network operators
- **Perform hardening of equipment and networks**
 - Map threats, mitigate risks, and take corrective actions in seven dimensions: authentication, authorization, access, audit, system, records and settings





MANRS

Mutually Agreed Norms for
Routing Security

<http://manrs.org>

MANRS - Mutually Agreed Norms for Routing Security

The MANRS Program, supported by the Internet Society, defends the Internet Security and Stability

- **Main concept: We're all in this together!!**
- Network operators have the responsibility to ensure a robust and reliable routing infrastructure!
- **The security of your network depends on the other networks!**
- The security of other networks depends on your network!
- **Implement the actions of MANRS and join the initiative**
- As more network operators work together, then fewer problems everyone will have!



MANRS – Four Actions

Everyone should implement these recommendations:

1. Filtering: prevent propagation of incorrect routing information

- Help to protect against threats such as Prefix Hijacking and Route Leak

2. Anti-spoofing: prevent traffic with spoofed source IP addresses

- Prevents infected computers initiating amplification attacks

3. Coordination: facilitate global communication between network operators

- Allows security teams to easily warn other networks about issues they are experiencing caused by this network

4. Global Validation: facilitate validation of routing information on a global scale

- Communicate the correct announcements with adjacent networks, publicly documented, to facilitate global validation



MANRS

MANRS - Benefits

Benefits for Service Providers that implement MANRS:

- Adds competitive value in a market where everyone offers similar, price-driven services
- **Shows to its clients competence and commitment in the security area**
- Helps to resolve network issues
- **Companies indicate that they would pay more for effectively safe services (451 Research)**
- Eleven Brazilian companies already participate in the MANRS initiative



MANRS



Program for Safer Internet

Development of the Program

- Best Current Operational Practices Course for Autonomous Systems
- Tutorials on Best Routing and Hardening Practices
- Lectures on the Program for Safer Internet and the MANRS in the events of NIC.br and Partner Associations
- Actions with large operators - reduction of vulnerable IP addresses:
 - **Mar/18:** 581k for large ISPs and 144k ISPs and corporate AS
 - **Today:** 198k for large ISPs and 162k ISPs and corporate AS
- Actions with the largest Associations of Internet Service Providers
- Actions with industry to deliver CPEs with security specifications

Thank you

Gilberto Zorello <gzorello@nic.br>

nic.br **cgi.br**

www.nic.br | www.cgi.br