Challenges, Pros and Cons of Processing Data Feeds to Notify Constituents on a National Level

Cristine Hoepers
General Manager, CERT.br/NIC.br
cristine@cert.br

Klaus Steding-Jessen
Technical Manager, CERT.br/NIC.br
jessen@cert.br

NatCSIRT 2024
Fukuoka, Japan – June 14-15, 2024

cert.br nic.br cgi.br

cert.br

Computer Emergency Response Team Brazil

National CSIRT of Last Resort

TLP:CLEAR

Services Provided to the Community

Incident Management

- Coordination
- Technical Analysis
- Mitigation and Recovery Support

Situational Awareness

- Data Acquisition
  - Distributed Honeypots
  - SpamPots
  - Threat feeds
- Information Sharing

Knowledge Transfer

- Awareness
  - Development of Best Practices
  - Outreach
- Training
- Technical and Policy Advisory

Affiliations and Partnerships:

FIRST Improving Security Together MEMBER

ACCREDITED BY TI TRUSTED INTRODUCER

APWG RESEARCH PARTNER www.antiphishing.org

CARNEGIE MELLON UNIVERSITY SOFTWARE ENGINEERING INSTITUTE | SEI Partner Network

HN/P

Creation:

August/1996: CGI.br publishes a report with a proposed model for incident management for the country[1]

June/1997: CGI.br creates CERT.br (at that time called NBSO – NIC BR Security Office) based on the report's recommendations[2]

[1] https://cert.br/sobre/estudo-cgibr-1996.html | [2] https://nic.br/pagina/gts/157

Mission

To increase the level of security and incident handling capacity of the networks connected to the Internet in Brazil.

Constituency

Any network that uses Internet Resources allocated by NIC.br

- IP addresses or ASNs allocated to Brazil
- domains under the ccTLD .br

Governance

Maintained by **NIC.br** – The National Internet Registry (NIR)

- all activities are funded by .br domain registration

NIC.br is the **executive branch of CGI.br** – The Brazilian Internet Steering Committee

- a multistakeholder organization
- with the purpose of coordinating and integrating all Internet service initiatives in Brazil

https://cert.br/about/
https://cert.br/sobre/filiacoes/
https://cert.br/about/rfc2350/

TLP:CLEAR

Brazilian Internet in Numbers

Autonomous System Numbers (ASNs)

8949 ASNs

- 2nd in the world (1st is USA)
- Percentage relative to all Latin America and Caribbean
  - 67% of the ASNs
  - 63.2% of IPv4 allocations
  - 68.7% of IPv6 allocations

Source:
https://www.lacnic.net/en/web/lacnic/estadisticas-asignacion
https://pulse.internetsociety.org/blog/where-are-the-internet-networks

Internet Service Providers (ISPs)

11630 ISPs (estimated)

Source:
https://www.cetic.br/pt/pesquisa/provedores/indicadores/
https://www.cetic.br/media/docs/publicacoes/2/20231206151242/executive_summary_ict_providers_2022.pdf

Domains under the ccTLD <.br>

5.338.237 registered domains

- 1.615.343 with DNSSEC

Source:
https://registro.br/dominio/estatisticas/

Internet Exchange

IX.br has 36 PIXes in Brazil

- **34**Tbps peak and **19.8**Tbps average traffic

São Paulo PIX is the biggest in the world

- **2752** participants
- **22.8**Tbps peak and **12.8**Tbps average traffic

Source:
https://ix.br/agregado/
https://ix.br/trafego/agregado/sp

Data updated on May 31st, 2024

Data Sources

Honeypots Deployed by CERT.br

All purpose low-interaction honeypots

– Distributed in networks of 50 partners
  - private companies, ISPs, universities, critical infrastructure and government networks

– Specialized listeners for main network services

– **Full confidence** over
  - context of data collection
  - timestamps

External Threat Feeds

ShadowServer, Shodan.io & TeamCymru

– Mainly data of IPv4 network scans

– Some data from honeypots

– **No full confidence** over
  - context of data collection
  - timestamps
    - no clear timezones
    - may not be NTP synchronized

TLP:CLEAR

Once we have the data que question is: **What and How Often to Notify?**

Challenges to Prioritize

– Diversity of the constituency

– If we send too many notifications constituents
  - get numb
  - don’t know what to resolve first

Our approach

– Try to find the Pareto
  - What are 20% of the problems that if acted upon would make the **biggest change in the overall ecossystem health**

– Current focus
  - CVEs being actively exploited by APTs and ransomware
  - Reduce DDoS potential
    - fix UDP services that allow amplification
    - we re-test the IPs present on the feed
      - we notify only if it really amplifies traffic

TLP:CLEAR

Data Workflow

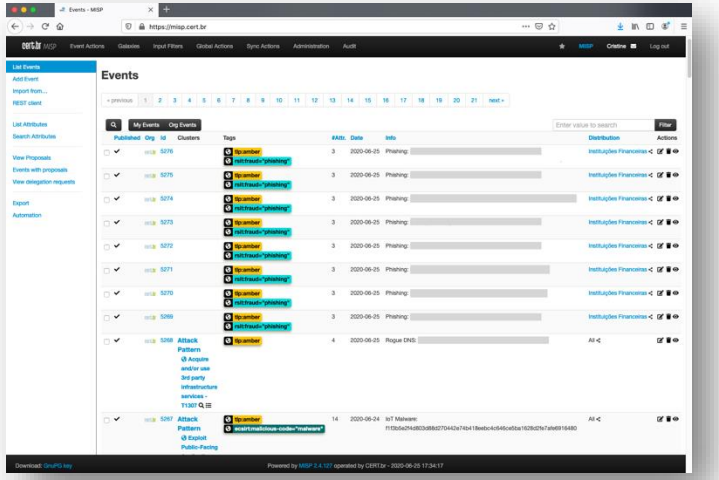
CERT.br Honeypots

External Threat Feeds

Email Notifications to Autonomous Systems, including

- How to fix the problem
- How to test/verify the problem/solution

Public Statistics
https://stats.cert.br/



Sharing of Indicators through MISP
https://cert.br/misp/

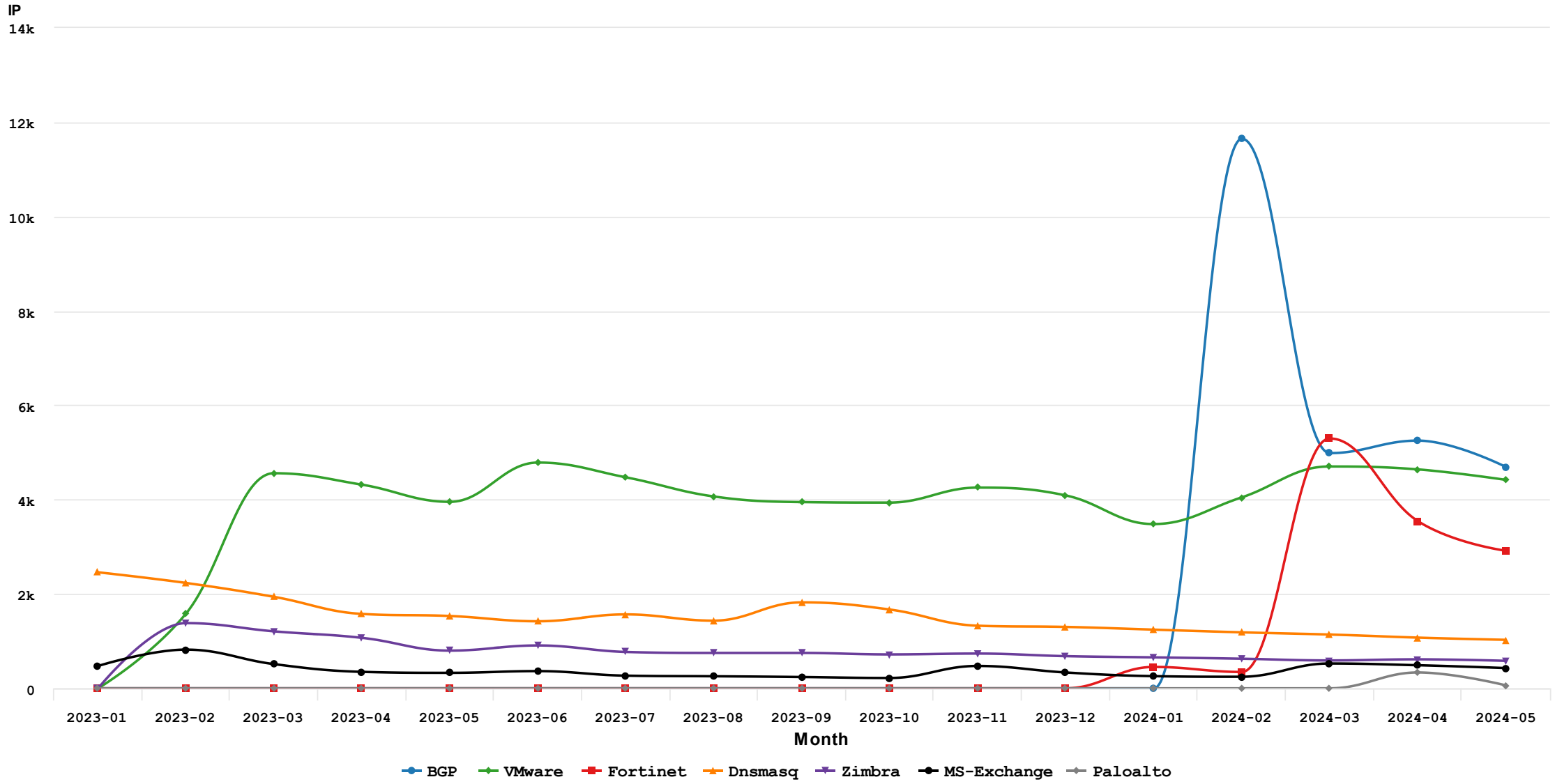
Are things improving?

cert.br nic.br cgi.br

TLP:CLEAR

CERT.br notifications: number of IP addresses of servers with vulnerabilities

2023-01 -- 2024-05

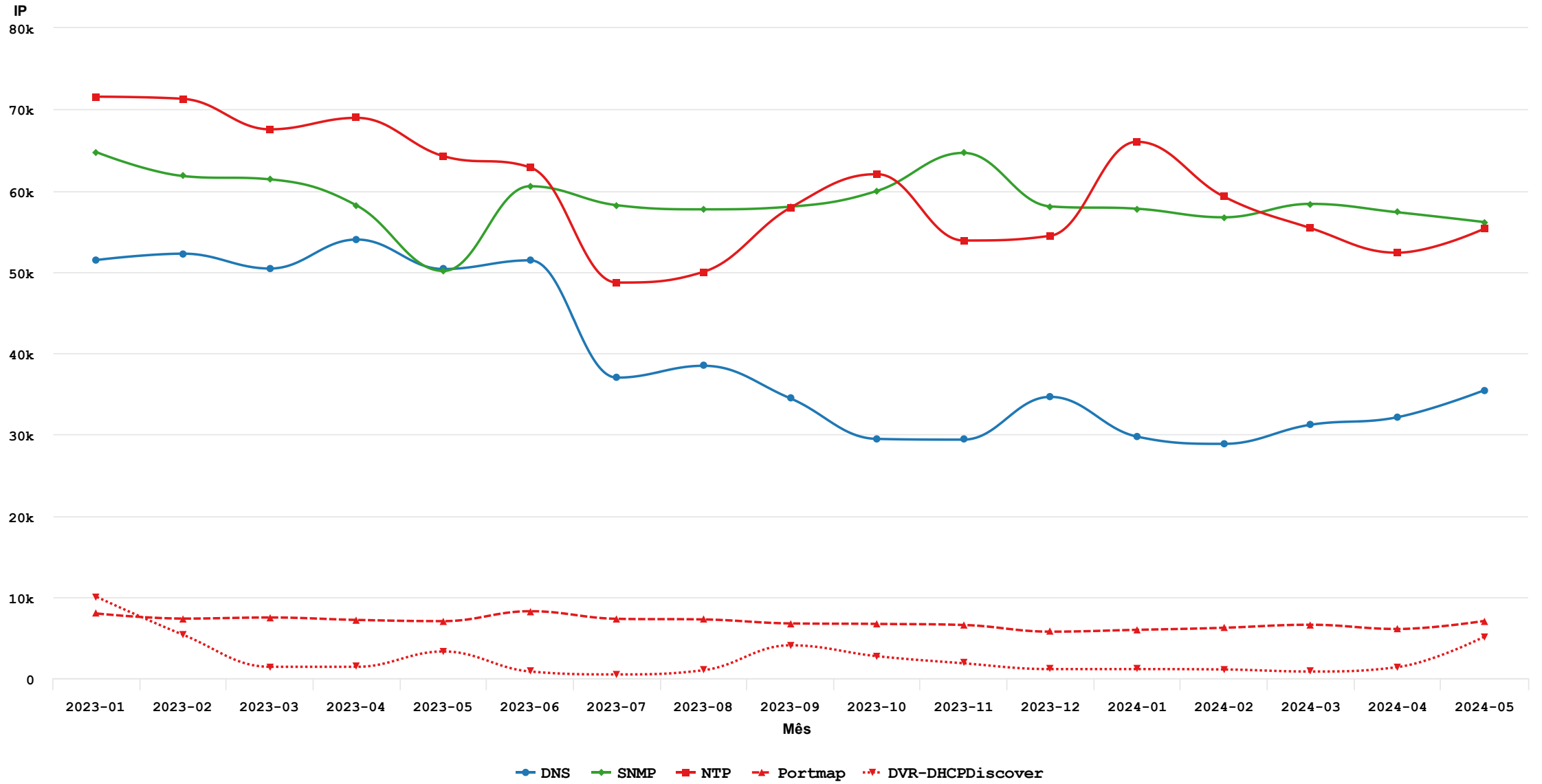


Source: CERT.br — https://stats.cert.br/ — by Highcharts.com

TLP:CLEAR

CERT.br notifications: number of IP addresses with services that allow amplification

2023-01 -- 2024-05



Source: CERT.br — https://stats.cert.br/ — by Highcharts.com

Shouldn’t numbers show more improvement?
Notifiying is just the beginning…

TLP:CLEAR

Usual motives for not patching/improving configurations:

– Lack of staff/experience

– “*What if it stops working?*” mentality

– Products that have different patching processes if you pay for support

- e.g. “update button” vs. a series of complex (“*scary*”) commands

TLP:CLEAR

When data is not “actionable”
Global Cloud Services: the additional challenge

– Increasingly we are receiving feeds and reports including:
  - IPs in use in Brazil but **NOT** allocated to a Brazilian ASN

– The Cloud providers, in general
  - do not have appropriate report channels
  - do not notify their clients

– We just can’t act on the data most of the times
  - we have no context to determine the cloud’s client organization affected

Arigatō Gozaimasu!

Thank You!

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

@ Incident reports to: cert@cert.br 𝕏 @certbr

https://cert.br/

nic.br cgi.br

www.nic.br | www.cgi.br