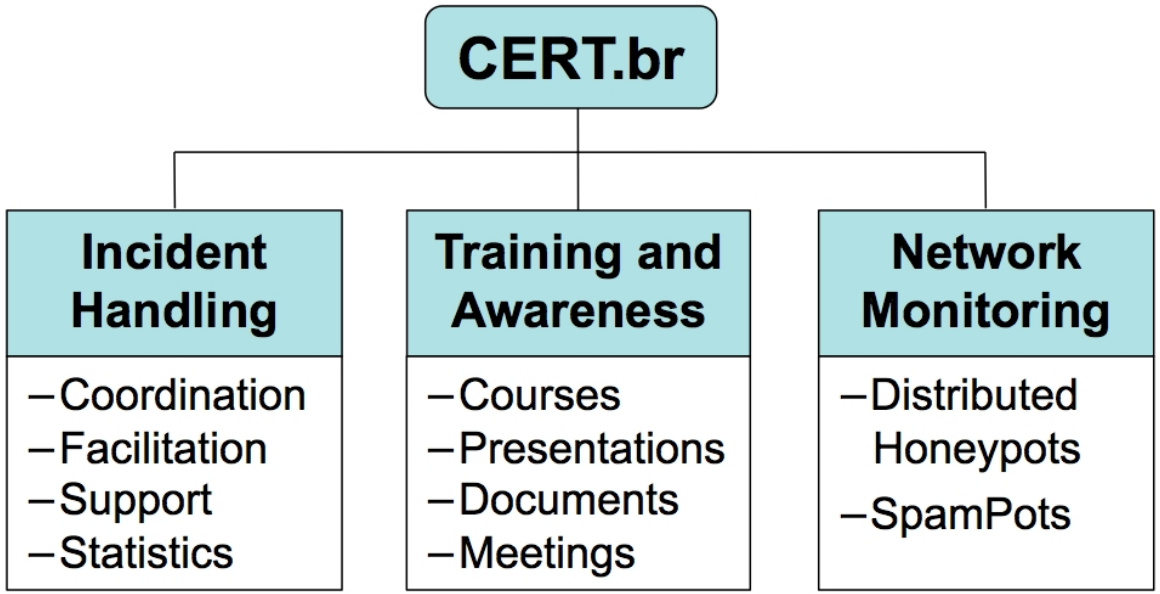
Development of an IPv6 Honeypot

Klaus Steding-Jessen
jessen@cert.br

CERT.br – Computer Emergency Response Team Brazil
NIC.br – Network Information Center Brazil
CGI.br – Brazilian Internet Steering Committee

About CERT.br

Created in 1997 as the national focal point to handle computer security incident reports and activities related to networks connected to the Internet in Brazil.



International Partnerships

FIRST Improving Security Together MEMBER

APWG RESEARCH PARTNER www.antiphishing.org

SEIPartner CERT Courses

The Honeynet PROJECT®

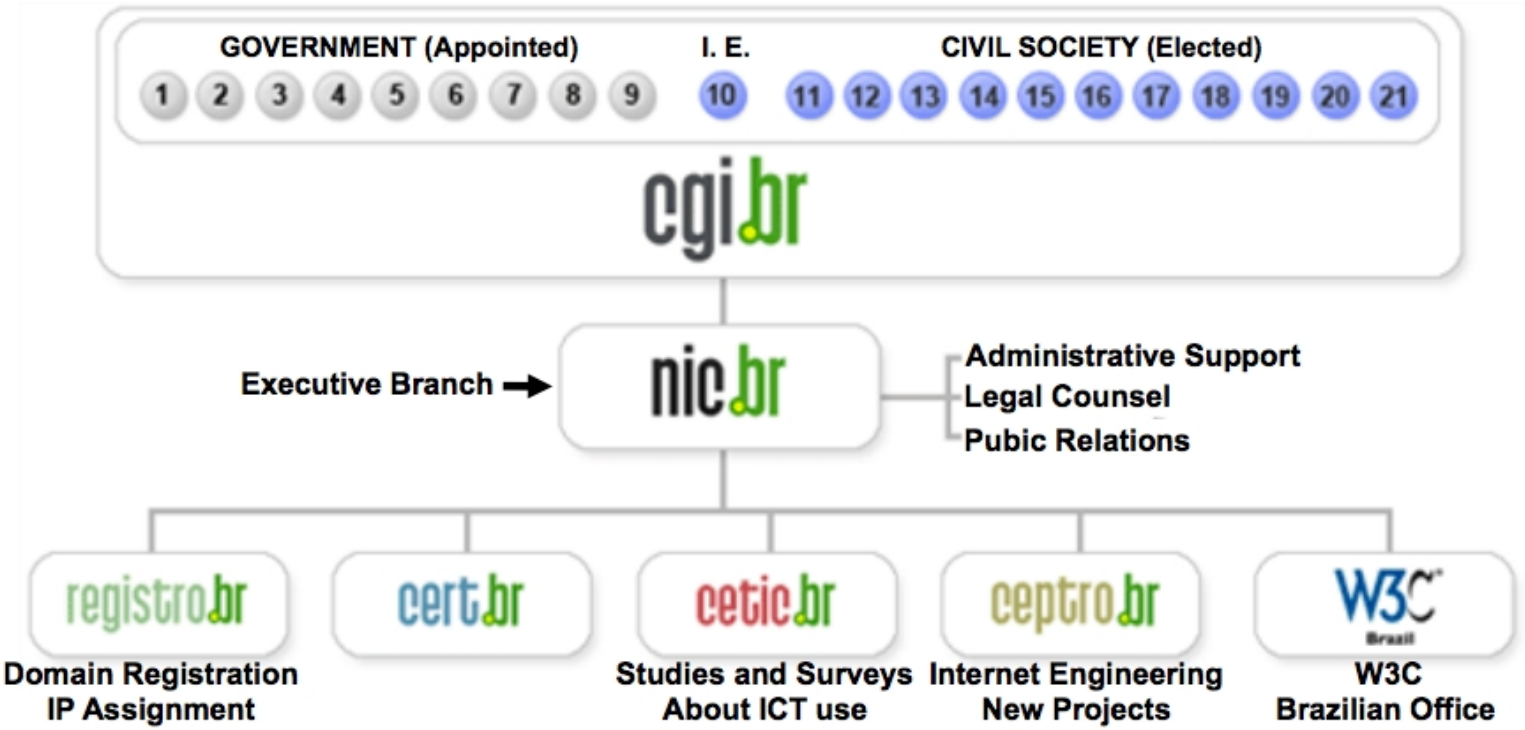
http://www.cert.br/mission.html

Our Parent Organization: CGI.br

Among the diverse responsibilities of The Brazilian Internet Steering Committee – CGI.br, the main attributions are:

- to propose policies and procedures related to the regulation of the Internet activities
- to recommend standards for technical and operational procedures
- to establish strategic directives related to the use and development of Internet in Brazil
- **to promote studies and technical standards for the network and services' security in the country**
- to coordinate the allocation of Internet addresses (IPs) and the registration of domain names using <.br>
- **to collect, organize and disseminate information on Internet services, including indicators and statistics**

CGI.br/NIC.br Structure



01- Ministry of Science and Technology
02- Ministry of Communications
03- Presidential Cabinet
04- Ministry of Defense
05- Ministry of Development, Industry and Foreign Trade
06- Ministry of Planning, Budget and Management
07- National Telecommunications Agency
08- National Council of Scientific and Technological Development
09- National Forum of Estate Science and Technology Secretaries
10- Internet Expert

11- Internet Service Providers
12- Telecom Infrastructure Providers
13- Hardware and Software Industries
14- General Business Sector Users
15- Non-governamental Entity
16- Non-governamental Entity
17- Non-governamental Entity
18- Non-governamental Entity
19- Academia
20- Academia
21- Academia

Agenda

Introduction

Motivation for a Honeypot

The Project

Results

Conclusion

Introduction (1)

IPv6

- standardized in 1998 (RFC 2460)
- not widely adopted yet ($<$ 1% of today's traffic)

Some improvements over IPv4:

- larger address space: 32 to 128 bits
  - no more v4 space by the end of 2010...
- streamlined protocol header
- autoconfiguration
- network layer security (IPSec)
- QoS capabilties
- mobility

Introduction (2)

Some of the attacks against v4 networks are the same:

- attacks against applications
- Denial of Service attacks
- malware

New problems:

- transition methods
- autoconfiguration
- lack of:
  - best practices
  - policies
  - training
  - tools

Motivation for a Honeypot

Force us to study IPv6

Better understand the current level of attacks in IPv6 networks

- scanning, probes, etc
- malware on v4 hosts using tunnels?
- harvesting of email addresses
- spam

The Project (1)

Cooperation beetwen CERT.br and CEPTRO.br

two `/48` IPv6 blocks

- a `/48` block is usually given to enterprises
- a `/48` $= 2^{16}$ `/64` $=$ 65536 `/64` blocks
  or 1208925819614629174706176 IP addresses

one domain

- under `.br`
- hosted at v4/v6 reacheable DNS servers
- just "`AAAA`" records

The Project (2)

one IPv6 server

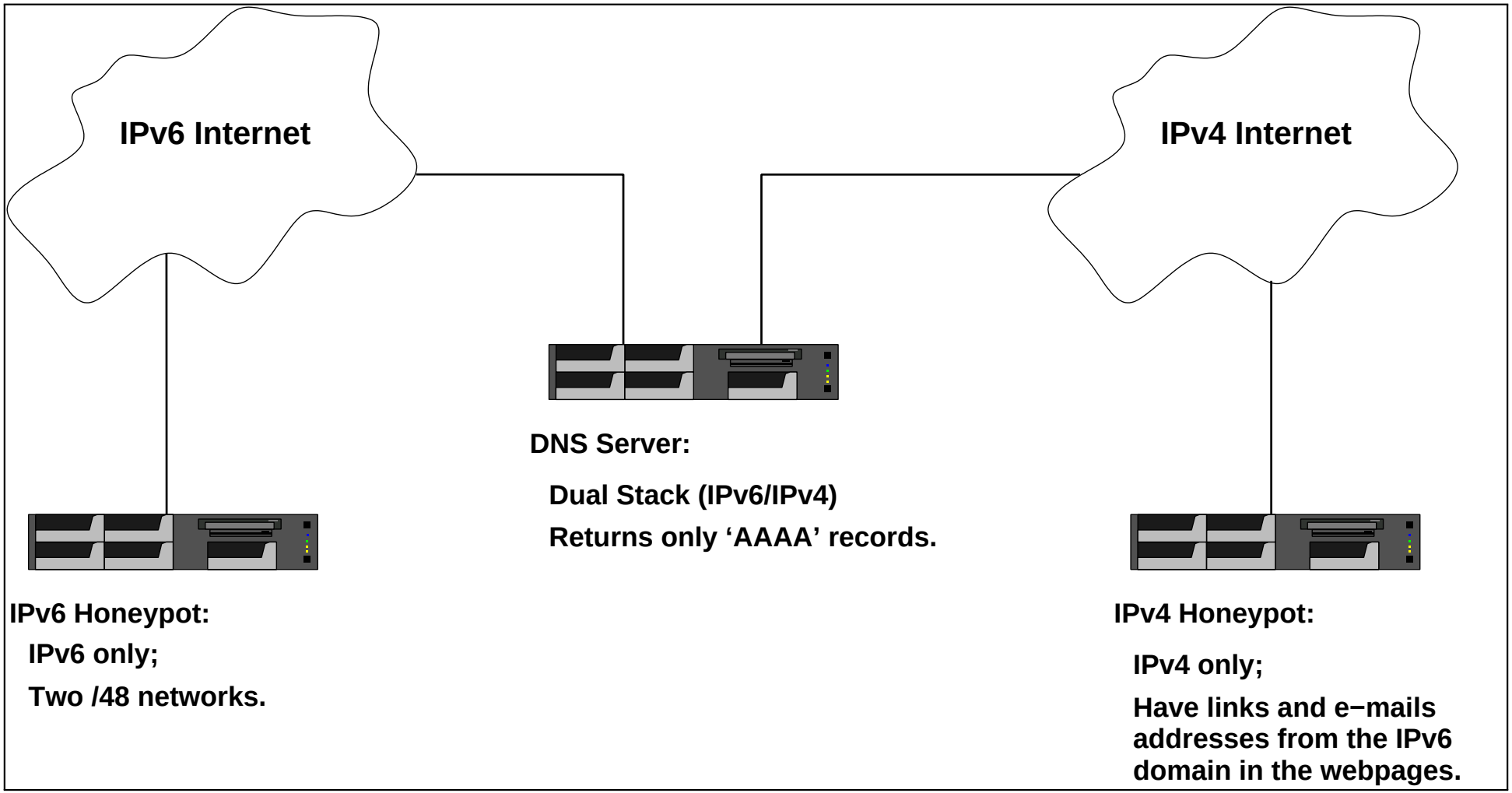
- reachable via IPv6 only
- receiving traffic from those two `/48` IPv6 blocks
  - logging all traffic and generating alerts
- hosting an web server
  - fake content
  - dinamically generated email addresses on each page and inside files
- hosting an mailserver server
  - `MX` for this domain
  - configured to receive email to every address on our domain

The Project (3)

one IPv4 server

- reachable via IPv4 only
- hosting an web server
  - on a different domain
  - activelly being harvested by spammers
  - receiveing spam on a daily basis
- with references to the IPv6 server
  - emails
  - links

The Project (4)



Results (1)

Since deployment (end of march, 2009) we have observed very little activity:

- 1 IP using a native IPv6 address
  - DNS query from a `.edu` server
  - no DNS service running at our end
  - misconfiguation? probe?
- 3 IPs using 6to4
  - `2002::/16` space, reserved for 6to4 deployments (RFC3056)
  - HTTP activity, following a link
  - Windows machines from `.no`, `.pt`, `.ir`

Results (2)

- 1 IP using a IPv4 to IPv6 gateway
  - HTTP activity
  - Linux machine using the SixXS-IPv6Gate
    http://ipv4gate.sixxs.net/
- 1 IP using Teredo
  - 2001:0000::/32) space, reserved for Teredo
  - HTTP activity, following a link from wikipedia

Conclusions

- overall IPv6 acitivity is still very low
  - malicious or not
- transition methods like 6to4 and Teredo being used
- popular search engines do not work with IPv6-only sites

References

- CERT.br
  http://www.cert.br/
- CEPTRO.br
  http://www.ceptro.br/
- IPv6.br
  http://www.ipv6.br/

- This presentation will be available (soon) at:
  http://www.cert.br/docs/presentations/