DNS Amplification Attacks as a DDoS Tool and Mitigation Techniques

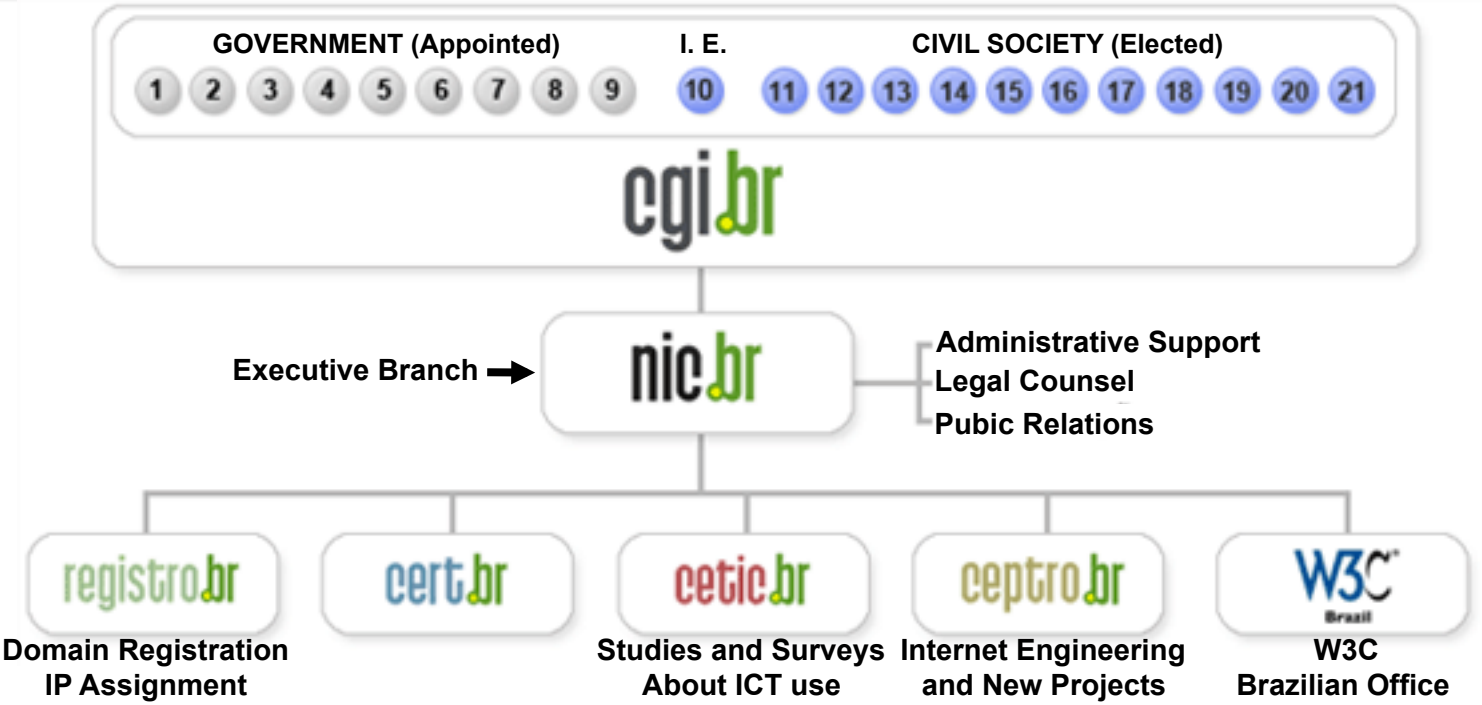
Klaus Steding-Jessen

jessen@cert.br

Computer Emergency Response Team Brazil - **CERT.br**

Network Information Center Brazil - **NIC.br**
Brazilian Internet Steering Committee - **CGI.br**

CGI.br and NIC.br Structure



1 – Ministry of Science and Technology (Coordination)
2 – Ministry of Communications
3 – Presidential Cabinet
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
10 – Internet Expert
11 – Internet Service Providers
12 – Telecommunication Infrastructure Providers
13 – Hardware and Software Industries
14 – General Business Sector Users
15 – Non-governmental Entity
16 – Non-governmental Entity
17 – Non-governmental Entity
18 – Non-governmental Entity
19 – Academia
20 – Academia
21 – Academia

The Brazilian Internet Steering Committee - CGI.br

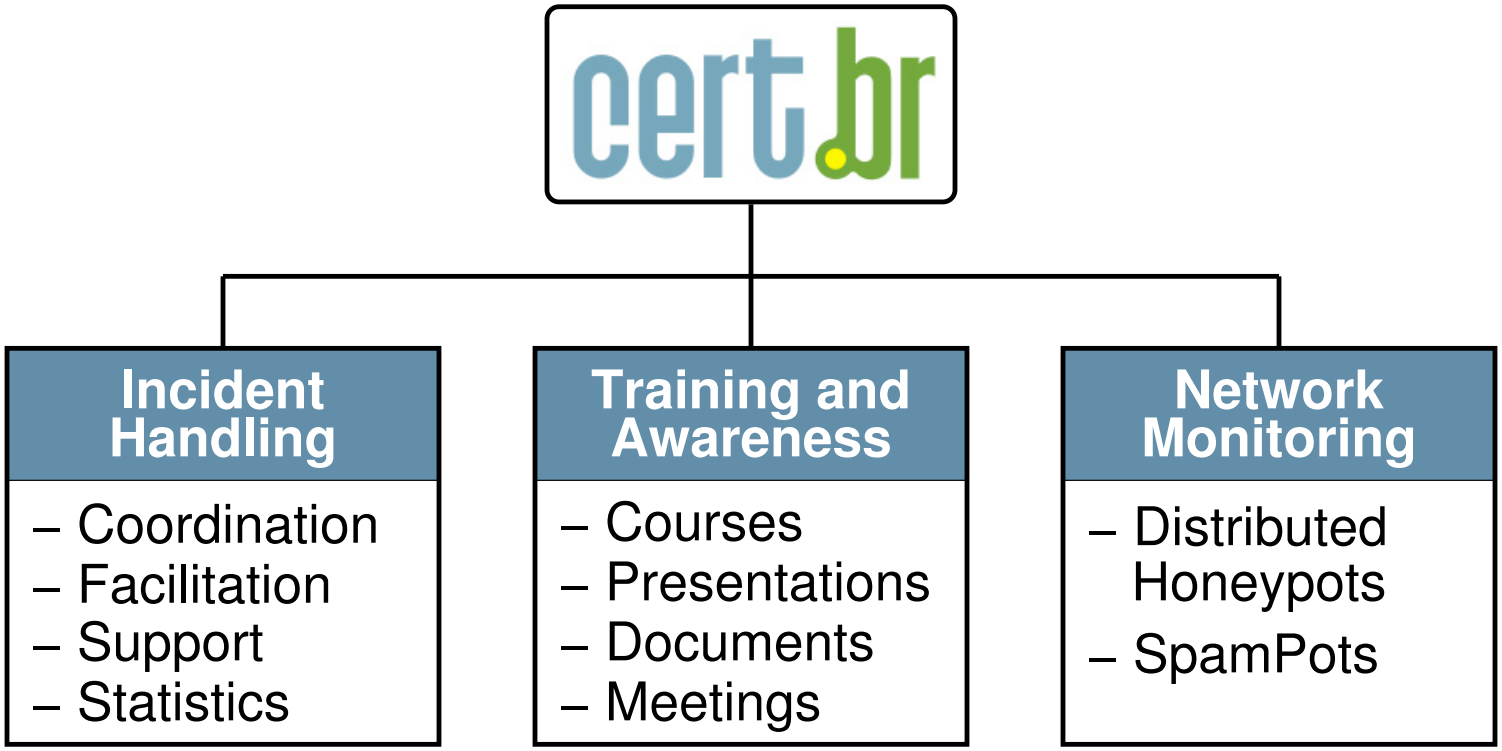
CGI.br is a multi-stakeholder organization created in 1995 by the Ministries of Communications and Science and Technology to coordinate all Internet related activities in Brazil.

Among the diverse responsibilities reinforced by the Presidential Decree 4.829, has as the main attributions:

- **to propose policies and procedures related to the regulation of 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 recommend technical standards for the network and services' security in the country**
- **to coordinate the allocation of Internet addresses (IP) and the registration of domain names using <.br>**
- **to collect, organize and disseminate information on Internet services, including indicators and statistics**

http://www.cgi.br/english/

CERT.br Activities



FIRST Improving Security Together MEMBER

APWG RESEARCH PARTNER www.antiphishing.org

SEI Partner Carnegie Mellon

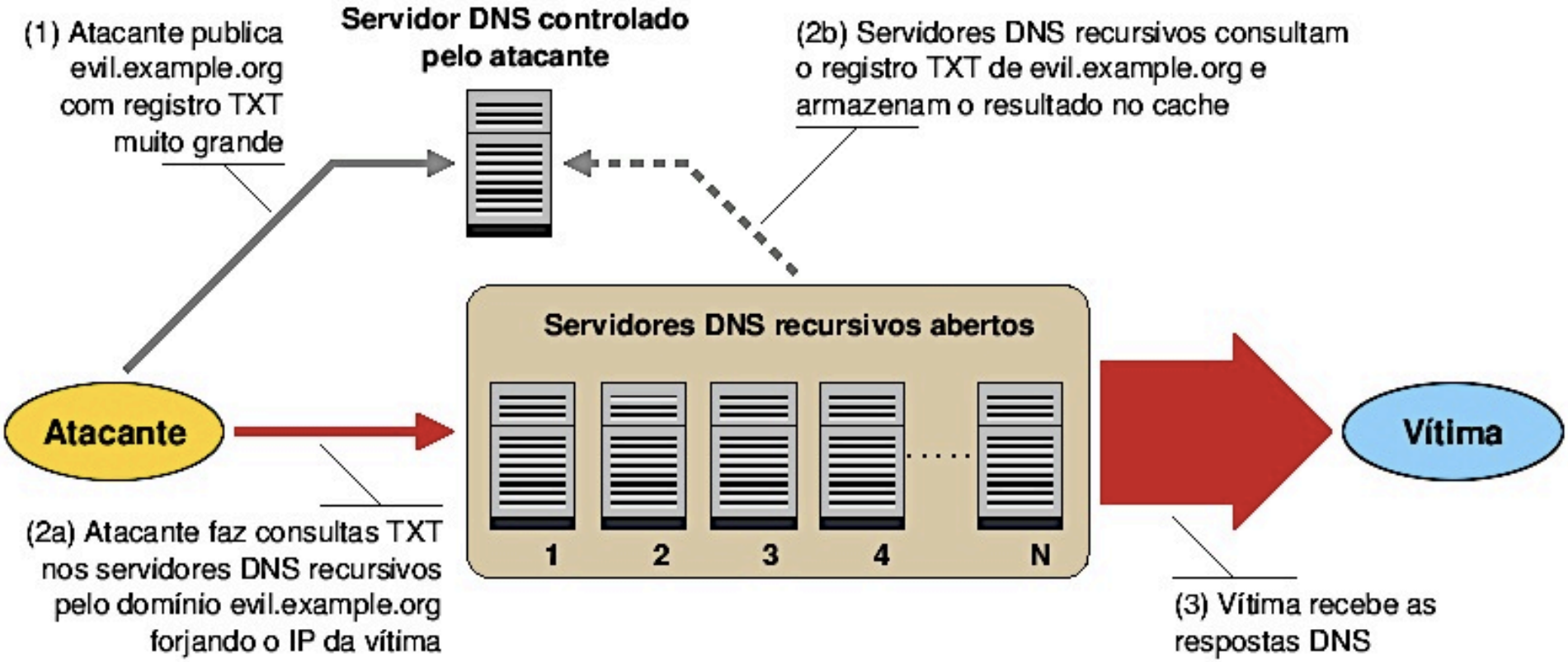
The Honeynet PROJECT

http://www.cert.br/about/

Agenda

- DRDoS attacks using big DNS records for amplification
- Solution
- Mitigation
  - close open resolvers
  - rate limiting in authoritative DNS servers

Anatomy of a DRDoS Attack using Open Resolvers



Recomendações para Evitar o Abuso de Servidores DNS Recursivos Abertos

http://www.cert.br/docs/whitepapers/dns-recursivo-aberto/

Big DNS Record Example (70x amplification)

```
; <<>> DiG 9.7.6-P1 <<>> directedat.asia ANY
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13971
;; flags: qr rd ra; QUERY: 1, ANSWER: 259, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
;directedat.asia.               IN      ANY

;; ANSWER SECTION:
directedat.asia.        14226   IN      A       204.11.52.123
directedat.asia.        14226   IN      A       204.11.52.124
directedat.asia.        14226   IN      A       204.11.52.125

[...]

;; Query time: 49 msec
;; SERVER: 190.90.225.253#53(190.90.225.253)
;; WHEN: Mon May  6 14:27:09 2013
;; MSG SIZE  rcvd: 4252
```

Solution and Possible Mitigations

Solution for attacks using IP spoofing is the wide adoption of Ingres/Egress filtering

- BCP 38: Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing
  http://tools.ietf.org/html/bcp38

Mitigations

- Fix Open Recursive DNS Servers
  - should answer only to client networks
- Implement rate limiting in authoritative DNS Servers

CERT.br Effort to Close Open Resolvers in Brazil

- **Partnership with the Open DNS Resolver Project**
  - **Received the list of all Brazilian open resolver**

- **Send notification to all ASNs**
  - **More than 70 thousand open resolvers**
  - **Notification sent to network owner with details about how to test and solve the problem**
  - **Online document in Portuguese with more detailed information and configuration examples**
    - **http://www.cert.br/docs/whitepapers/dns-recursivo-aberto/**

Questions?

Klaus Steding-Jessen
jessen@cert.br

- **CGI.br - Brazilian Internet Steering Committee**
  http://www.cgi.br/
- **NIC.br**
  http://www.nic.br/
- **CERT.br**
  http://www.cert.br/