



nic.br

Núcleo de Informação
e Coordenação do
Ponto BR

cgi.br

Comitê Gestor da
Internet no Brasil

registro.br cert.br cetic.br ceptro.br ptt.br

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.

INOC-DBA

ceptro.br nic.br cgi.br



Chair goes round..
Chair goes round.

Unhandled Hosts down

All problem hosts have been acknowledged.

Tactical overview

Type	Totals	Percentage %
Hosts up	4/4	100
Hosts down	0/4	0
Services up	10/26	38.46
Services down	16/26	61.54

Unhandled service problems

Host	Service	Output	Last statechange	Last check
192.168.5.64	NRPE	Connection refused	2011-07-26 16:38:08	2012-01-20 10:42:21
192.168.5.84-linux	/ Disk Usage	CHECK_NRPE: Received 0 bytes from daemon. Check the remote server logs for error messages.	2011-08-1	
192.168.5.84-linux	/tmp Disk Usage	CHECK_NRPE: Received 0 bytes from daemon. Check the remote server logs for error messages.	2011-11-1	
192.168.5.84-linux	CPU Stats	CHECK_NRPE: Received 0 bytes from daemon. Check the remote server logs for error messages.	2011-08-1	
192.168.5.84-linux	Cron Scheduling Daemon	CHECK_NRPE: Received 0 bytes from daemon. Check the remote server logs for error messages.	2011-11-1	
192.168.5.84-linux	Load	CHECK_NRPE: Received 0 bytes from daemon. Check the remote server logs for error messages.	2011-11-1	
192.168.5.84-linux	Memory Usage	CHECK_NRPE: Received 0 bytes from daemon. Check the remote server logs for error messages.	2011-11-1	
192.168.5.84-linux	Open Files	CHECK_NRPE: Received 0 bytes from daemon. Check the remote server logs for error messages.	2011-08-1	
192.168.5.84-linux	Sendmail	CHECK_NRPE: Received 0 bytes from daemon. Check the remote server logs for error messages.	2011-08-1	

Refresh in 4

Unhandled Hosts down

Hostname	Alias
192.168.5.97	192.168.5.97
192.168.5.83-srmp	192.168.5.83-srmp
192.168.5.83	192.168.5.83
192.168.5.71	192.168.5.71
192.168.5.7	192.168.5.7
192.168.5.65	192.168.5.65
192.168.5.52	192.168.5.52
192.168.5.42-mpbs	192.168.5.42-mpbs
192.168.5.42-3dps	192.168.5.42-3dps
192.168.5.42-bps	192.168.5.42-bps
192.168.5.42	192.168.5.42
192.168.5.40	192.168.5.40
192.168.5.102	192.168.5.102
192.168.1.2	192.168.1.2
192.168.1.1	192.168.1.1
192.168.5.199host-b	192.168.5.199 Desc
192.168.5.199host-RENAMED2	192.168.5.199 Desc
192.168.5.198	192.168.5.198

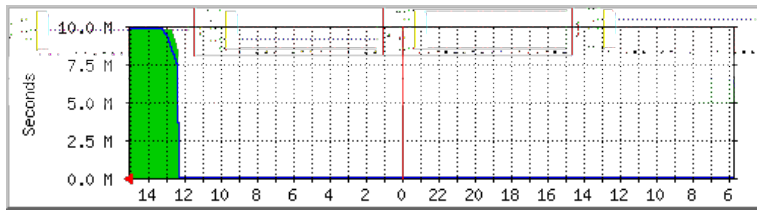
Tactical overview

Type	Totals	Percentage %
Hosts up	107/122	87.7
Hosts down	15/122	12.3
Services up	249/436	57.11
Services down	187/436	42.89

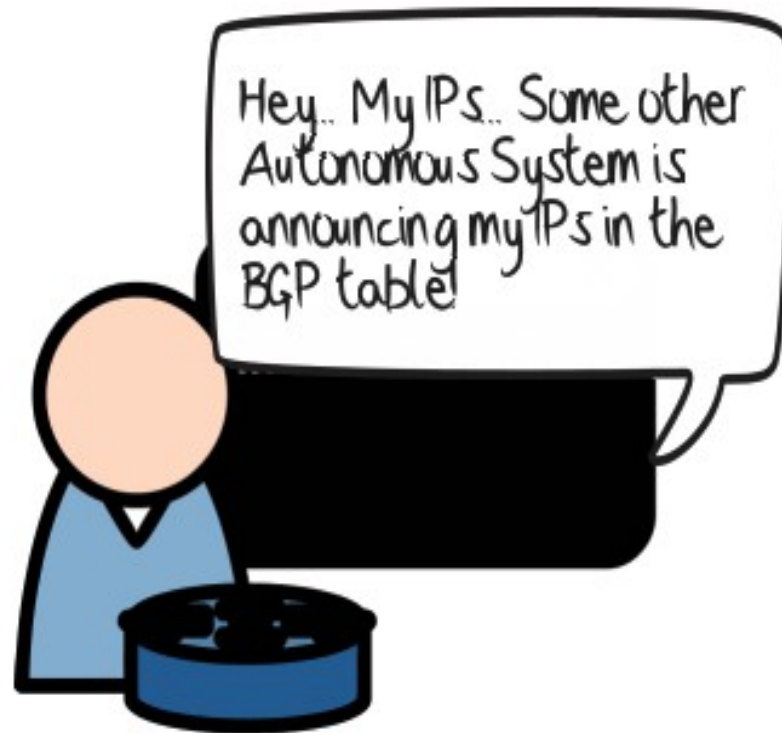
Unhandled service problems

Host	Service	Output	Last statechange	Last check
192.168.5.1	HTTP	CRITICAL - Socket timeout after 10 seconds	2012-01-14 14:14:28	2012-01-20 10:24:28
192.168.5.11	HTTP	CRITICAL - Socket timeout after 10 seconds	2011-07-26 16:22:49	2012-01-20 10:26:31
192.168.5.33	NRPE	Connection refused	2011-07-26 16:37:38	2012-01-20 10:26:22
192.168.5.33	SSH	Connection refused	2011-07-26 16:22:49	2012-01-20 10:27:54
192.168.5.4	CPU Usage	(null)	2011-11-30 16:05:50	2012-01-20 10:24:10
192.168.5.4	Drive C: Disk Usage	(null)	2011-11-30 16:07:11	2012-01-20 10:25:23
192.168.5.4	Drive E: Disk Usage	(Return code of 139 is out of bounds)	2011-07-26 16:20:02	2012-01-20 10:26:40
192.168.5.4	Drive F: Disk Usage	(Return code of 139 is out of bounds)	2011-07-26 16:22:49	2012-01-20 10:27:53

Refresh in 6 seconds 10:29









I will try to talk to
the contact
listed on whois..
They have to stop it now!

Hey.. My IPs.. Some other
Autonomous System is
announcing my IPs in the
BGP table!

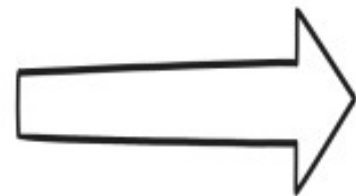
I will try to talk to
the contact
listed on whois..
They have to stop it now!

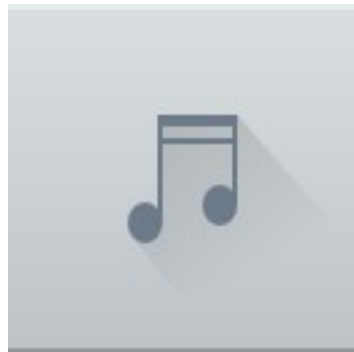
Hey.. My IPs.. Some other
Autonomous System is
announcing my IPs in the
BGP table!



I will try to talk to the contact listed on whois... They have to stop it now!

Hey.. My IPs.. Some other Autonomous System is announcing my IPs in the BGP table!

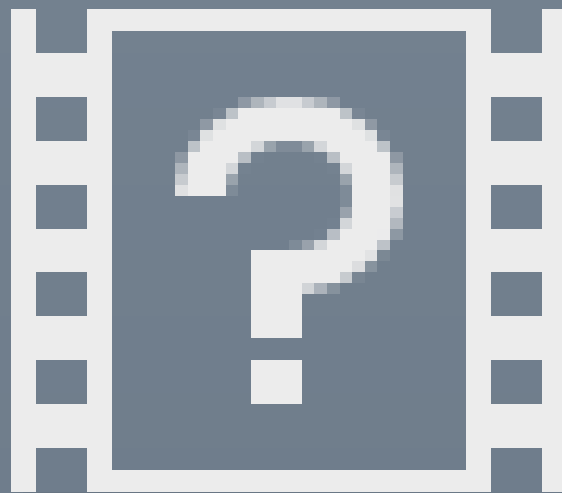




I will try to talk to
the contact
listed on whois..
They have to stop it now!

Hey.. My IPs.. Some other
Autonomous System is
announcing my IPs in the
BGP table!



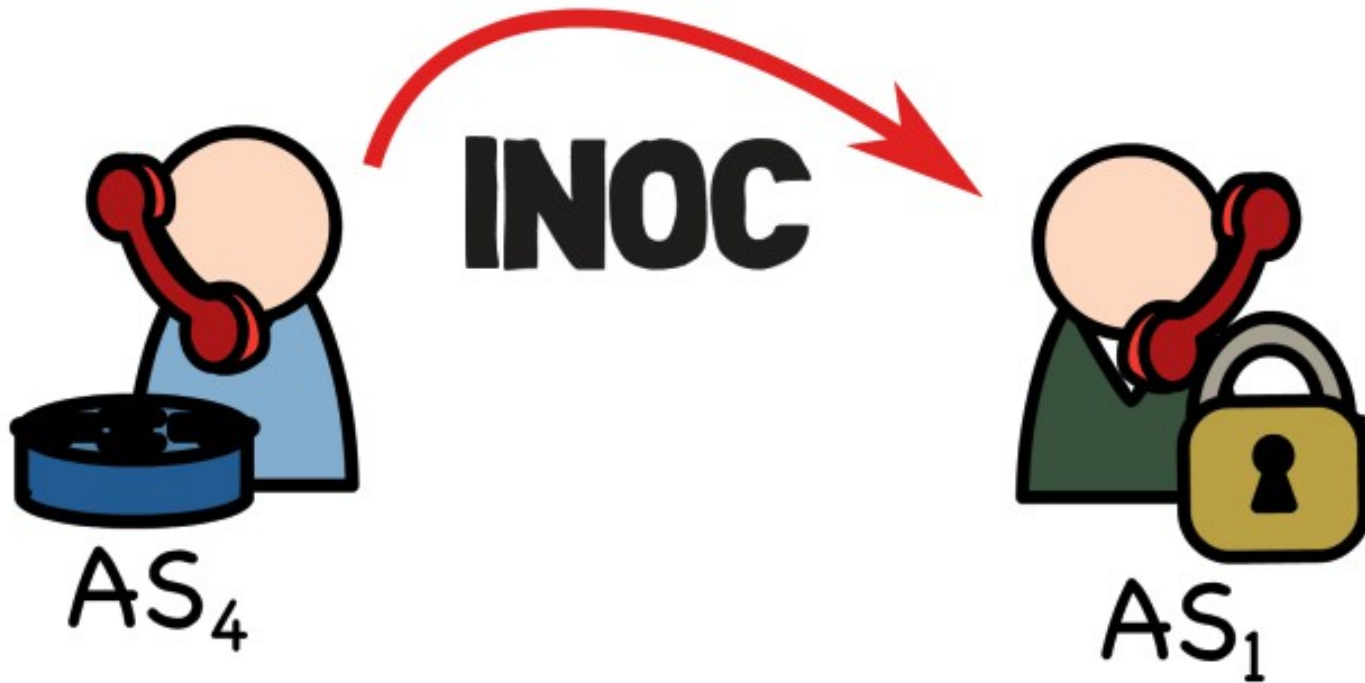


NA NA NA

Sim, comissário...

Batman!!





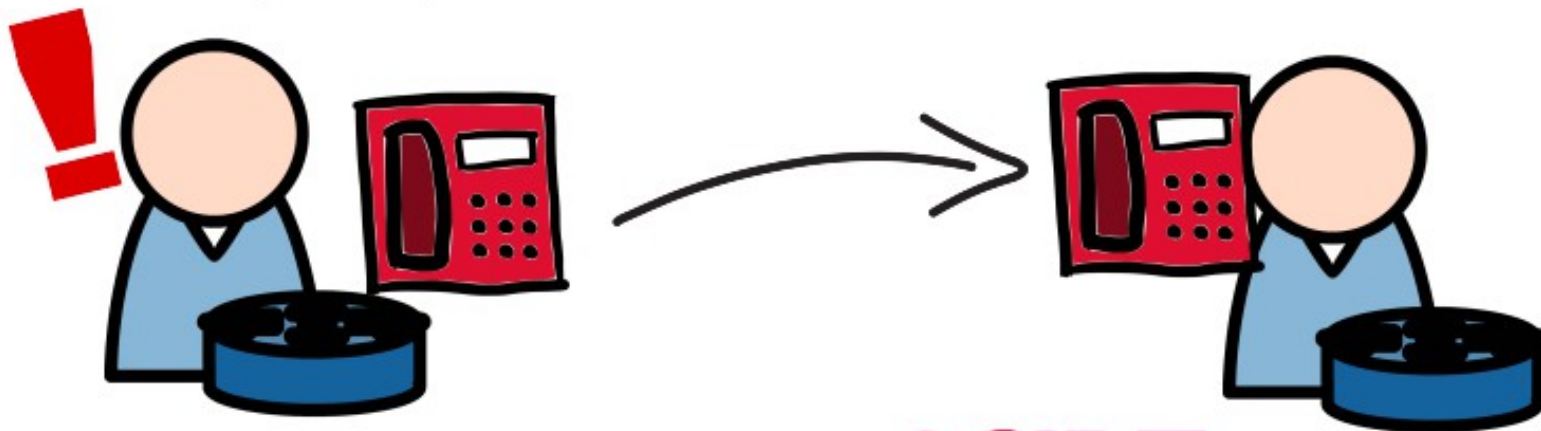
INOC-DBA

INTER-NETWORK OPERATION CENTER

DIAL BY AUTONOMOUS SYSTEM NUMBER
HOTLINE PHONE SYSTEM

Autonomous System
number (ASN)

identification of the network
in the global BGP routing

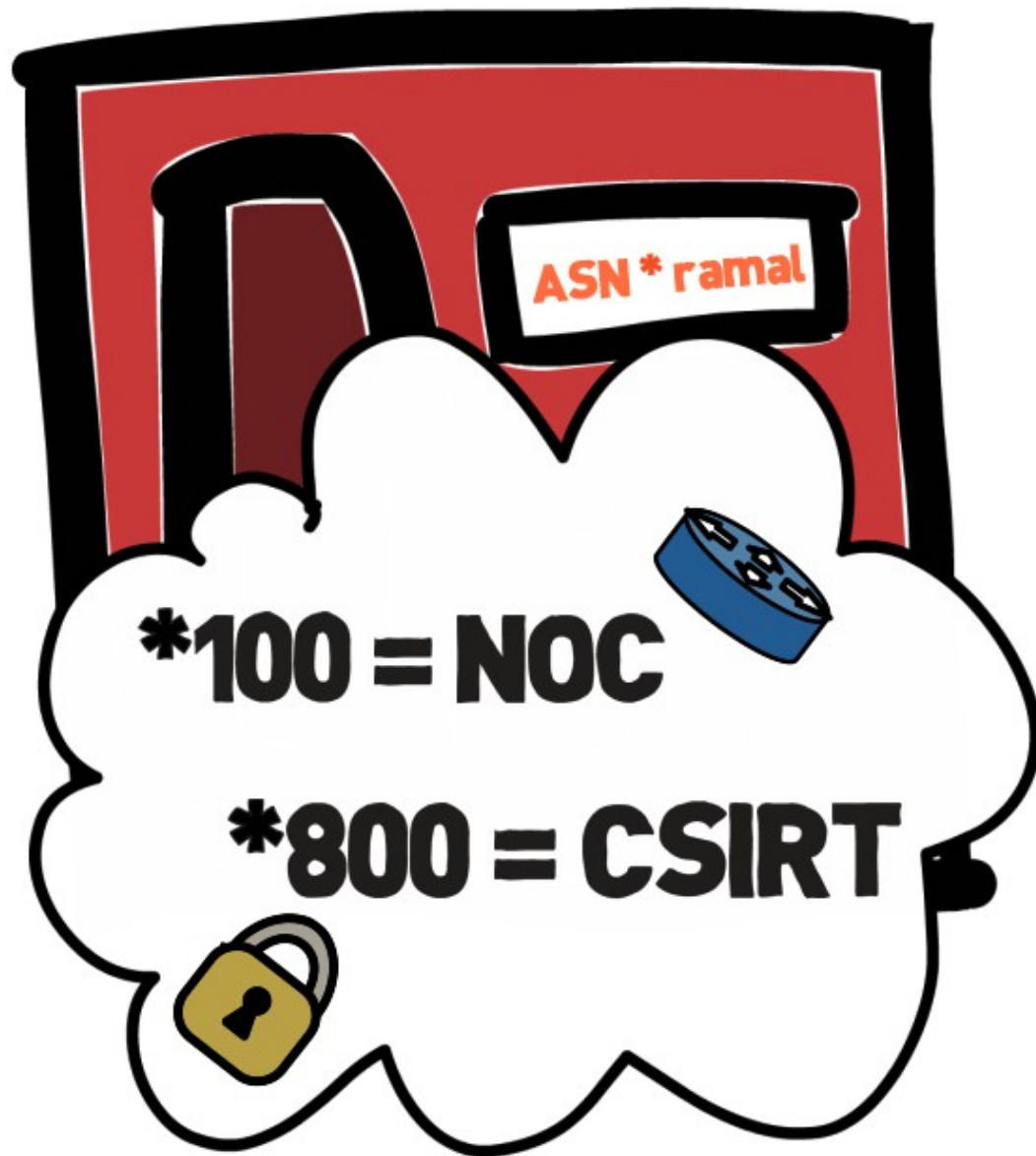


- routing problems
- security incidents
- peering agreements

...

CSIRTs

NOCs



Inter NOC – Dial by ASN **INOC-DBA**



INOC-DBA (Inter-**N**etwork **O**perations **C**enter **D**ial **B**y **A**SN) is a hotline phone system created and operated by Packet Clearing House in 2002.

Inter NOC – Dial by ASN **INOC-DBA**



The INOC-DBA provides a direct and private way of communication between the **Network Operations Centers** and **Security Incident Response Teams** of the Autonomous Systems.

In other words... Is a communication shortcut to the people who can solve your problem.

Inter NOC – Dial by ASN **INOC-DBA**



- The heart of the INOC-DBA is the IETF-standard **SIP protocol** (RFC 3261), an open VoIP standard that has broad support.

Inter NOC – Dial by ASN **INOC-DBA**



SIP Protocol

- Act over TCP and UDP 5060 ports to negotiate sessions.
- Media exchanged via RTP protocol (RFC 1889) in a pair of UDP ports. In our case, between UDP 10000 and UDP 20000.
- **Some problems with NAT.**

Inter NOC – Dial by ASN **INOC-DBA**



HOW IT WORKS

Every INOC phone number is a composition of the AS Number with some chosen extension of three number, linked by the asterisk digit.

ASN*Extension

Inter NOC – Dial by ASN **INOC-DBA**



HOW IT WORKS

In order to simplify even more the communication, some standard extensions were established:

- **ASN*100 - NOC**
- **ASN*800 - CSIRT**

Inter NOC – Dial by ASN **INOC-DBA-BR**



Supported by CGI.br and NIC.br, since 2005:

- independent server in Brazil
- Integrated (*) with PCH's INOC-DBA system
- NIC.br lended VoIP phones for ASs when it was necessary.

Inter NOC – Dial by ASN **INOC-DBA-BR**



Asterisk

(open source software PABX)

- Multi codec and multi VoIP protocol support.
- Voicemail and conference room.
- URA and queues support.

Inter NOC – Dial by ASN INOC-DBA-BR



Mordor's NOC
6666*100



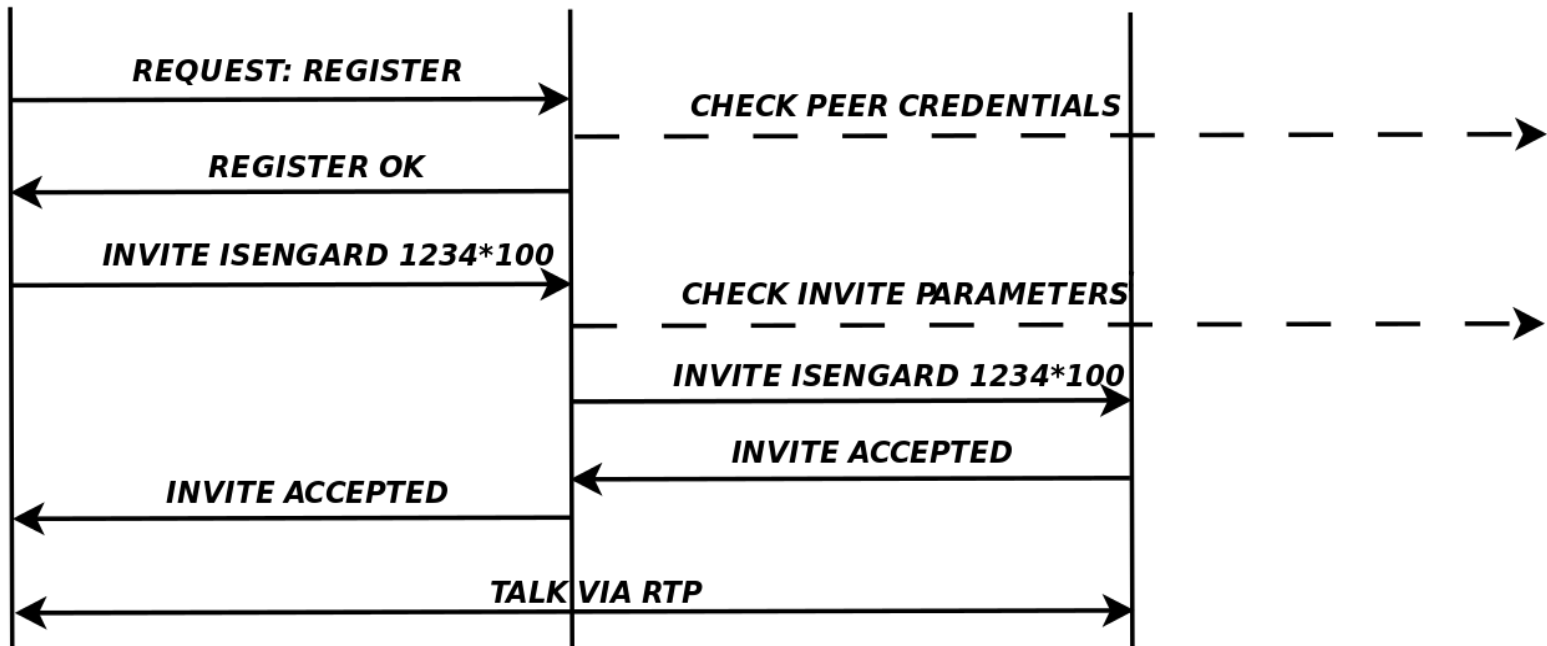
INOC-DBA BR ASTERISK SERVER



Isengard's NOC
1234*100



INOC-DBA BR DATABASE



Inter NOC – Dial by ASN INOC-DBA-BR



Linphone para PCs

O Linphone é um software livre e de código aberto disponível para plataformas Linux, Windows e Mac OS. É uma excelente escolha.



Zoiper para PCs

O Zoiper desktop é um softphone desenvolvido pela empresa brasileira, com opções de conferência de voz e videoconferência e está disponível para Linux, Windows e Mac OS. É amigável e sua versão gratuita foi homologada para uso comercial.



Linphone para telefones móveis

O Linphone Mobile é um aplicativo livre e de código aberto (assim como o desktop), disponível para iOS (6.0 ou superior), Windows Phone 8 e Blackberry.



Zoiper para telefones móveis

O Zoiper Mobile é um softphone desenvolvido pela empresa brasileira, disponível para iOS (6.0 ou superior) e Windows Phone 8. Ele é funcional e simples de utilizar.

back in time...



- stable
- can be online 24/7



- NIC.br lending phones
- high costs to NIC.br
- logistics
- slow growing of the network



Telefones VoIP



today...



Softphones SIP

Inter NOC – Dial by ASN **INOC-DBA-BR**

1 – Create account in PAS
(Autonomous System Portal)

2 – Associate your AS

3 – Create INOC-DBA extension

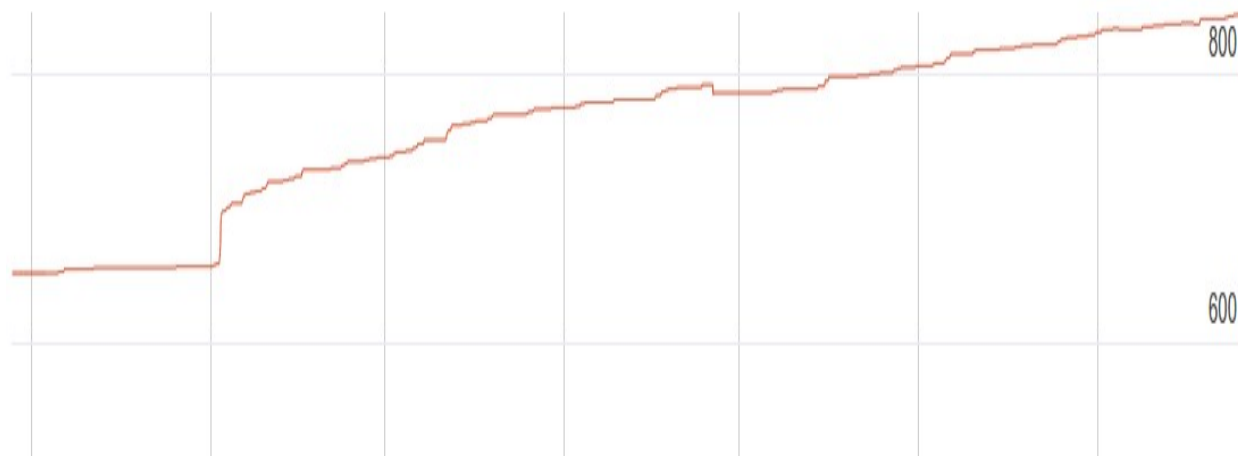
- Steps 2 and 3 require approval from whois contacts (e-mail)



Inter NOC – Dial by ASN

INOC-DBA-BR

845 users



607 - distinct Autonomous Systems

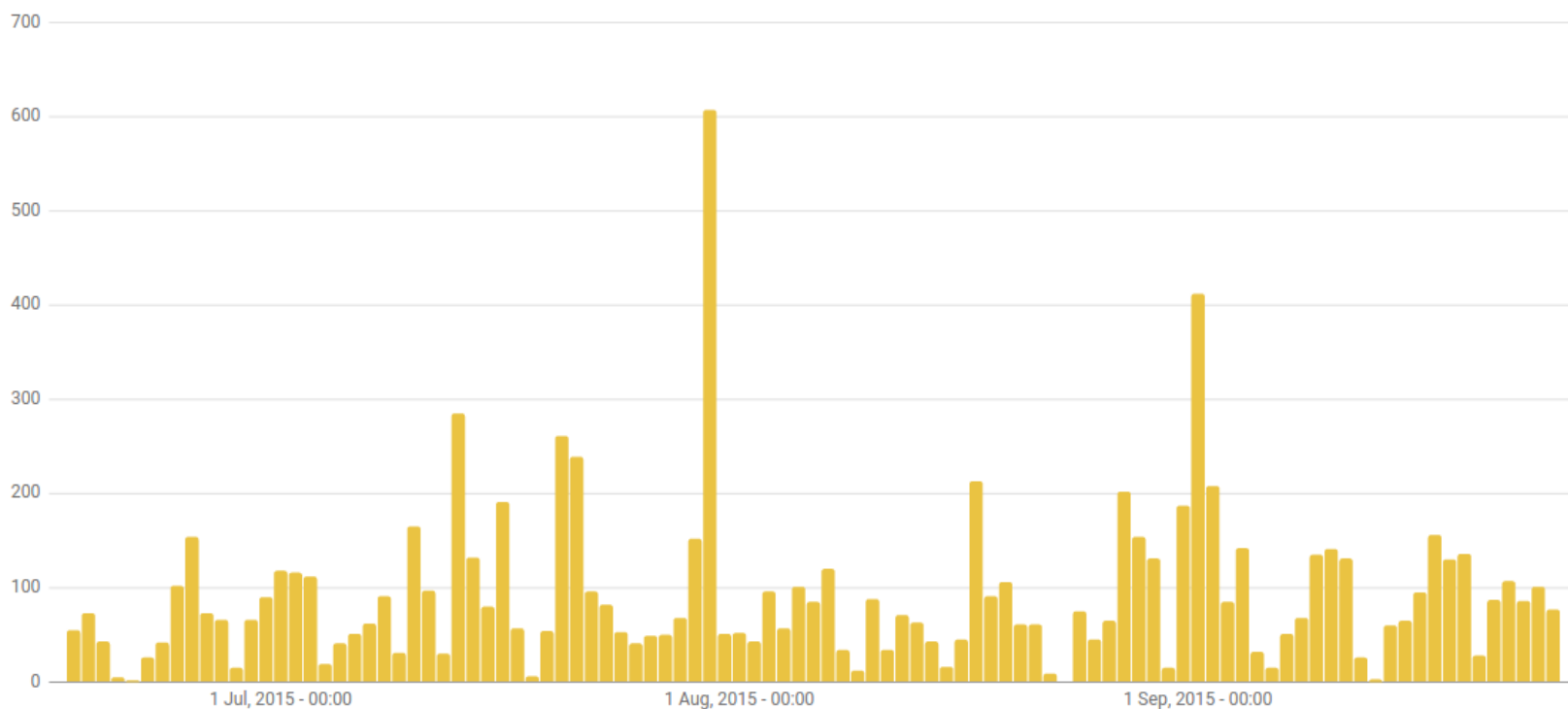
578 - *100 extensions

80 - *800 extensions

Inter NOC – Dial by ASN

INOC-DBA-BR

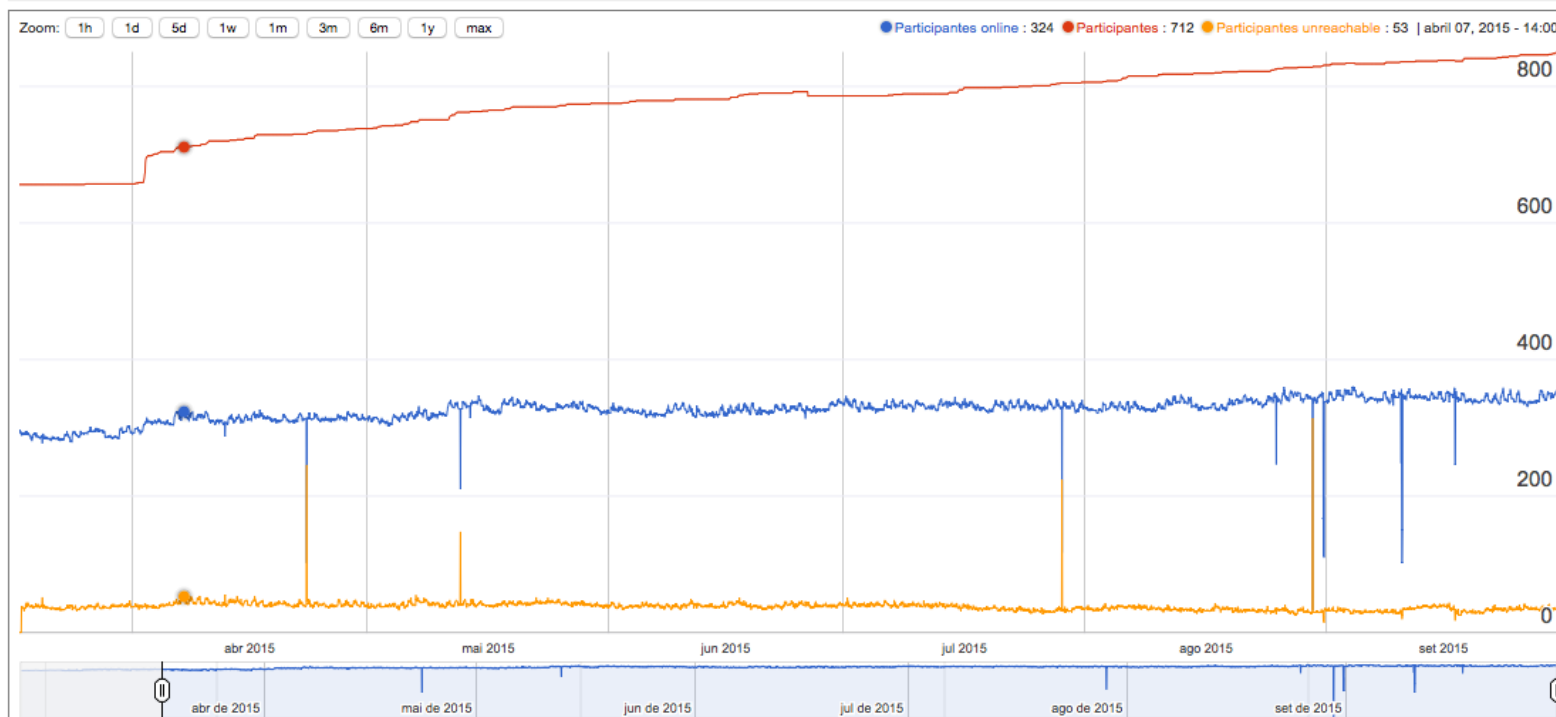
- 69 calls/day



Inter NOC – Dial by ASN INOC-DBA-BR

- Problems...

Quantidade de participantes online



Inter NOC – Dial by ASN

INOC-DBA-BR

Questions...

- What do you think? Should we try it in the LAC region?
- How we solve the problem with whois contacts?
- Should we do something else to improve communication between our NOCs and CSIRTs? Maybe an AS-Whats-App? AS-Telegram?

<https://inoc-dba-web.pch.net/inoc-dba/>

<http://inoc.nic.br>

Obrigado

www.ceptro.br

© moreiras@nic.br

© @moreiras

01 de novembro de 2015

nic.br **cgi.br**

www.nic.br | www.cgi.br