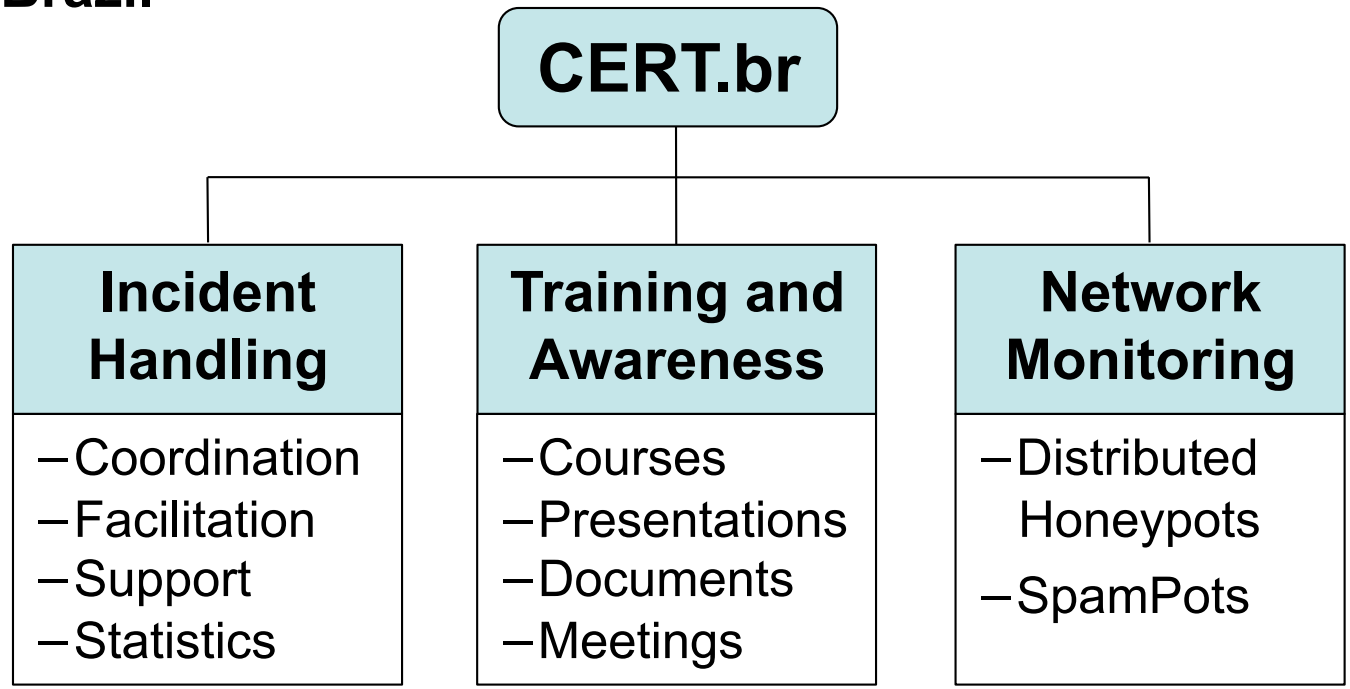
Preventing your Network from Being Abused by Spammers

Marcelo H. P. C. Chaves
mhp@cert.br

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

CERT.br Activities

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

Anti-Phishing Working Group APWG

SEIPartner CERT Courses

The Honeynet PROJECT®

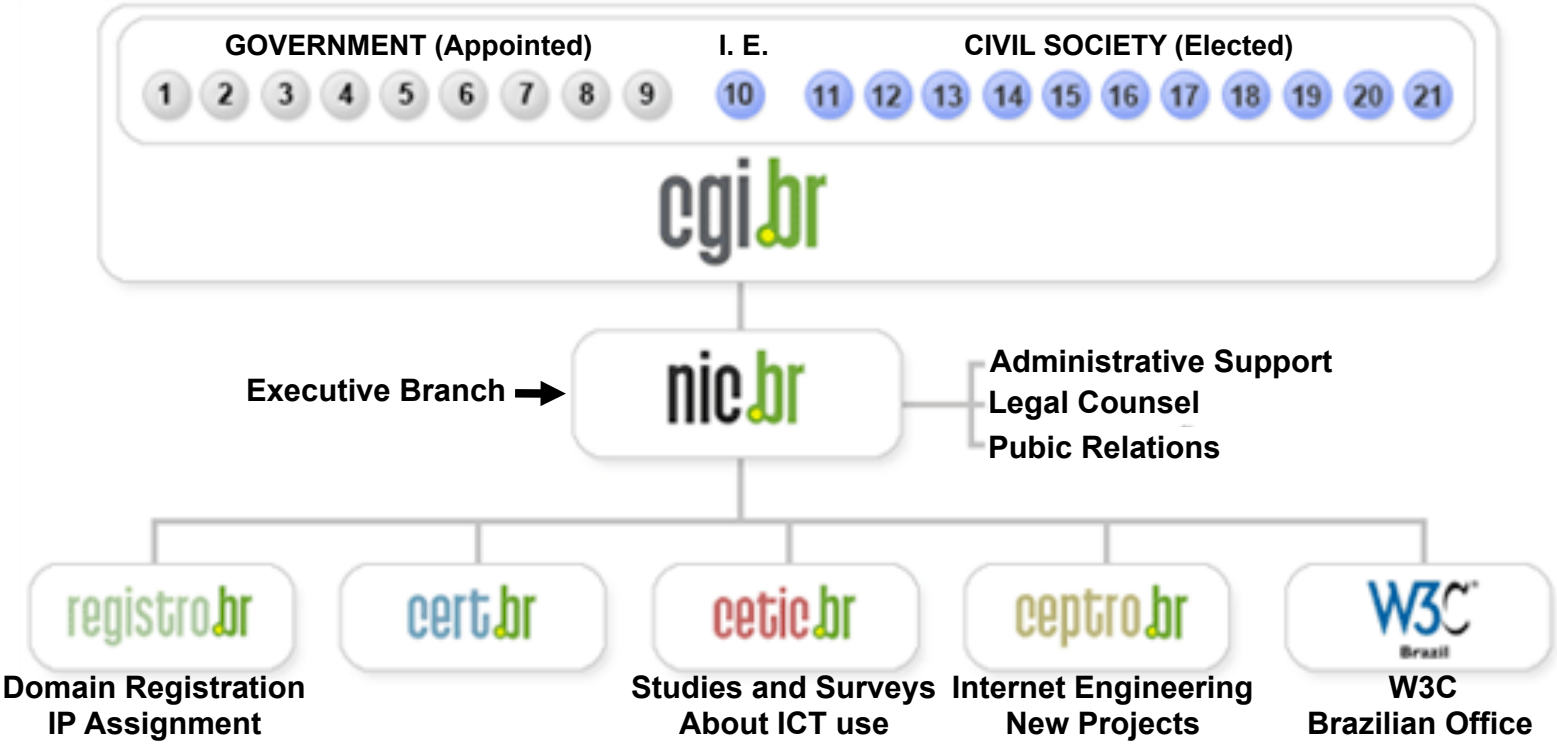
Our Parent Organization:
The Brazilian Internet Steering Committee - CGI.br

CGI.br is a multi-stakeholder organization that, among the diverse responsibilities, has 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 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/internacional/

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

Agenda

- The SpamPots Project
  - 1st Phase Review
  - 2nd Phase
- Port 25 Management
  - Current Scenario
  - Impact
  - Benefits
  - Adoption & Challenges
- User awareness initiatives

cert.br

Understanding and Reducing the Abuse of Brazilian Broadband Networks for sending Spam: SpamPots Project

1st Phase Review

cgi.br | nic.br

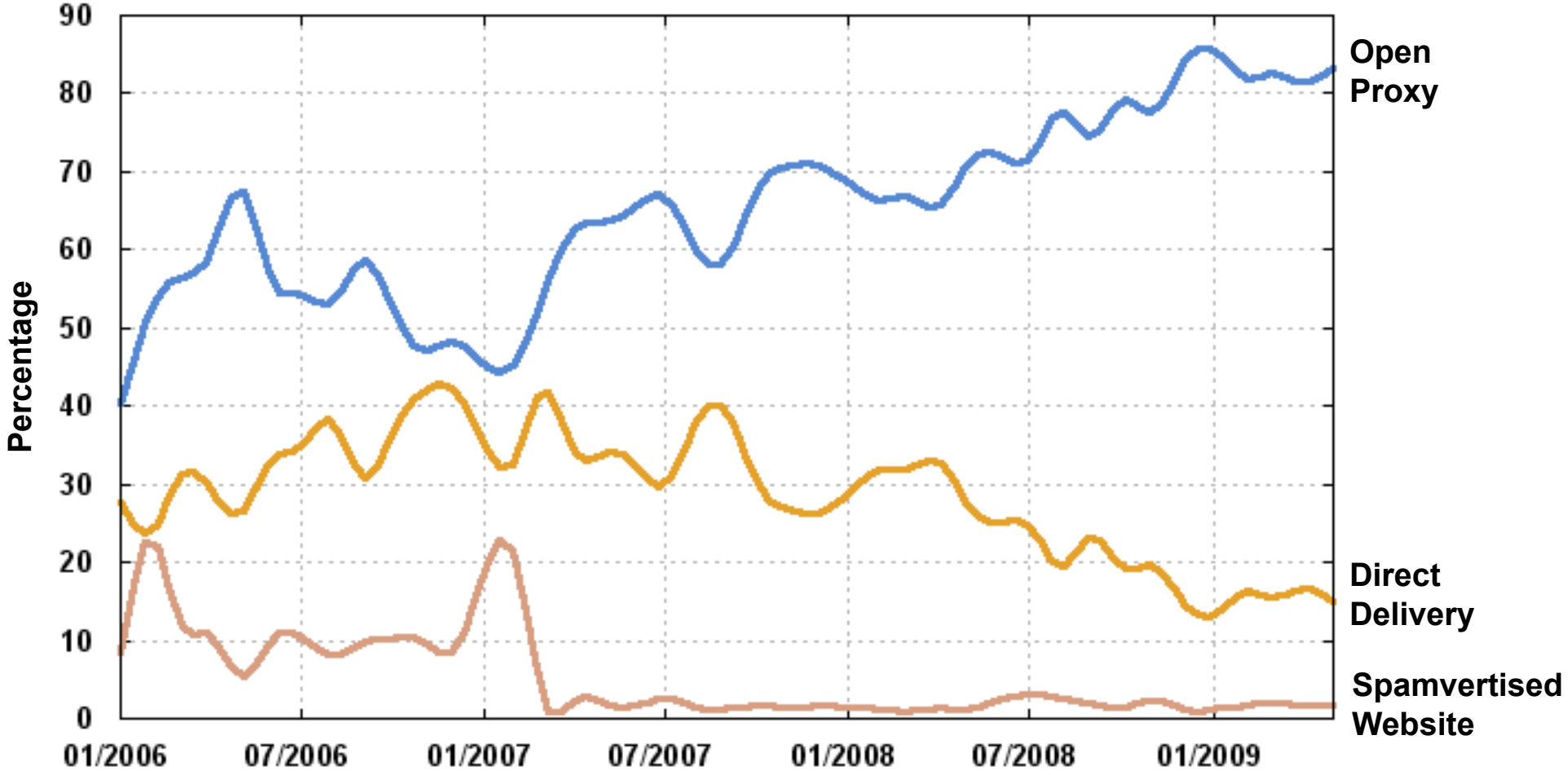
Motivation (1/3)

- Brazil is a big "source" of spam
- Scans for open proxies are always in the top 10 ports in our honeypots' network statistics

  http://www.honeypots-alliance.org.br/stats/
- Spam complaints related to open proxy abuse have increased in the past few years
- Financial fraud is still using spam

Motivation (2/3)

Spams Reported by SpamCop to CERT.br – Most Common Abuse



Months: January 2006 — May 2009

http://www.cert.br/stats/spam/porcentagens/

Motivation (3/3) – Brazil on CBL

"The CBL takes its source data from very large spamtraps/mail infrastructures, and only lists IPs exhibiting characteristics which are specific to open proxies of various sorts (HTTP, socks, AnalogX, wingate etc) and dedicated Spam BOTs which have been abused to send spam, worms/viruses that do their own direct mail transmission (…)"

- Brazil is the leading country on number of IPs listed:
  - complete list has 8,949,708 IPs
  - 1,369,938 (15.31%) from Brazil
  - Other countries with more than 5%: IN (10.35%), RU (8.01%), TR (7.79%) and PL (5.61%)

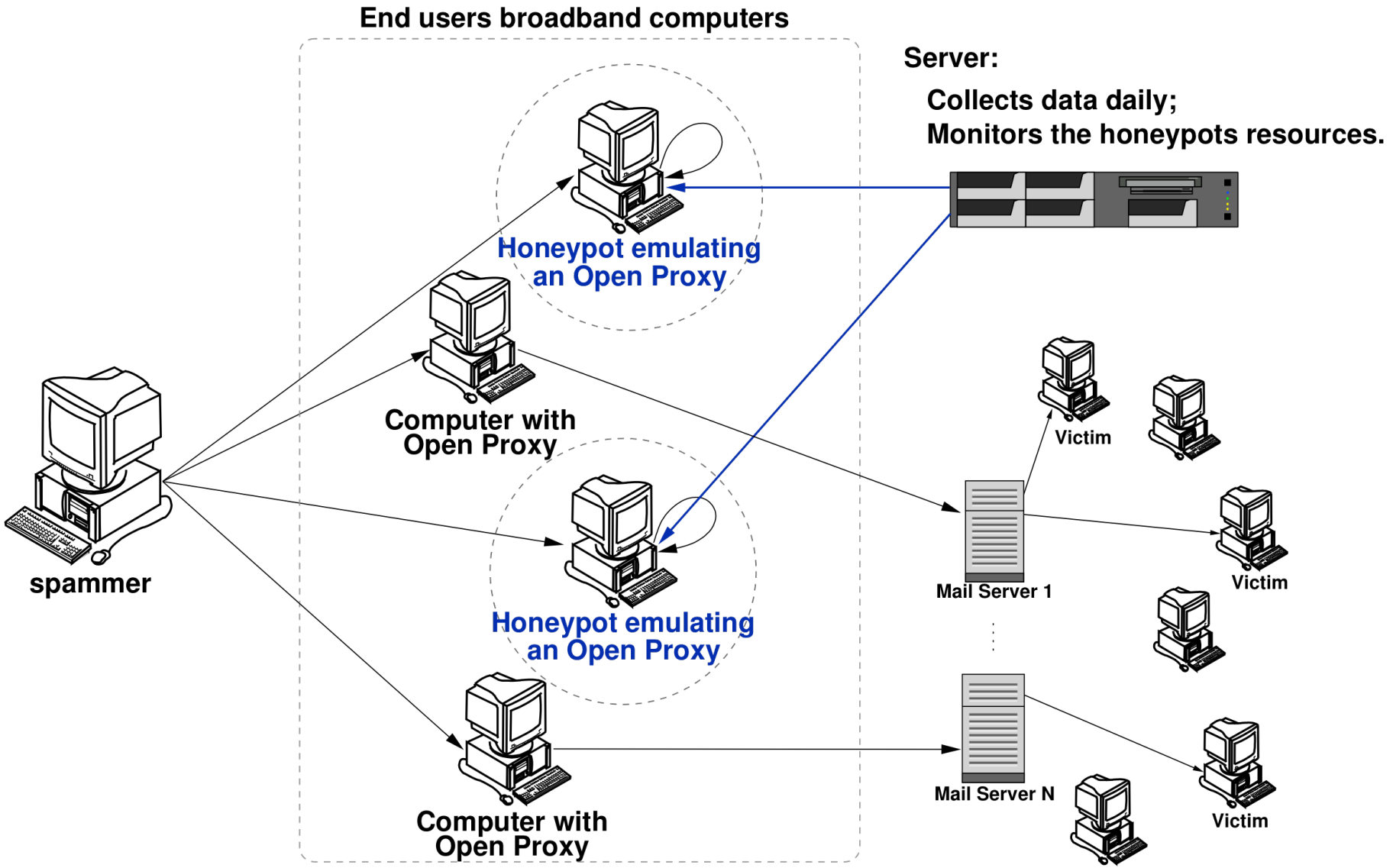
Domain	count	% tot
telebahia.net.br	431122	4.82
telesp.com.br	278250	3.11
brasiltelecom.net.br	260306	2.91
telet.com.br	79963	0.89
netservicos.com.br	74254	0.83
gvt.net.br	53777	0.60
ig.com.br	47858	0.53
timbrasil.com.br	36499	0.41
ctbctelecom.net.br	26684	0.30
embratel.net.br	19150	0.21
canbrasnet.com.br	18683	0.21
ig.com	9442	0.11

Data extracted on 2009/06/19 -- http://cbl.abuseat.org/

The SpamPots Project

- Main Goals
  - Have metrics about the abuse of our networks
    - Basically measure the problem from a different point of view: **abuse of infrastructure** X spams received at the destination
  - Help develop the spam characterization research
  - Measure the abuse of end-user machines to send spam
- Structure of the 1st phase
  - Deployment of 10 low-interaction honeypots, **emulating open proxy/relay services** and capturing spam
    - 5 broadband providers
    - 1 home and 1 business connection each

Location of the Sensors in the 1st Phase



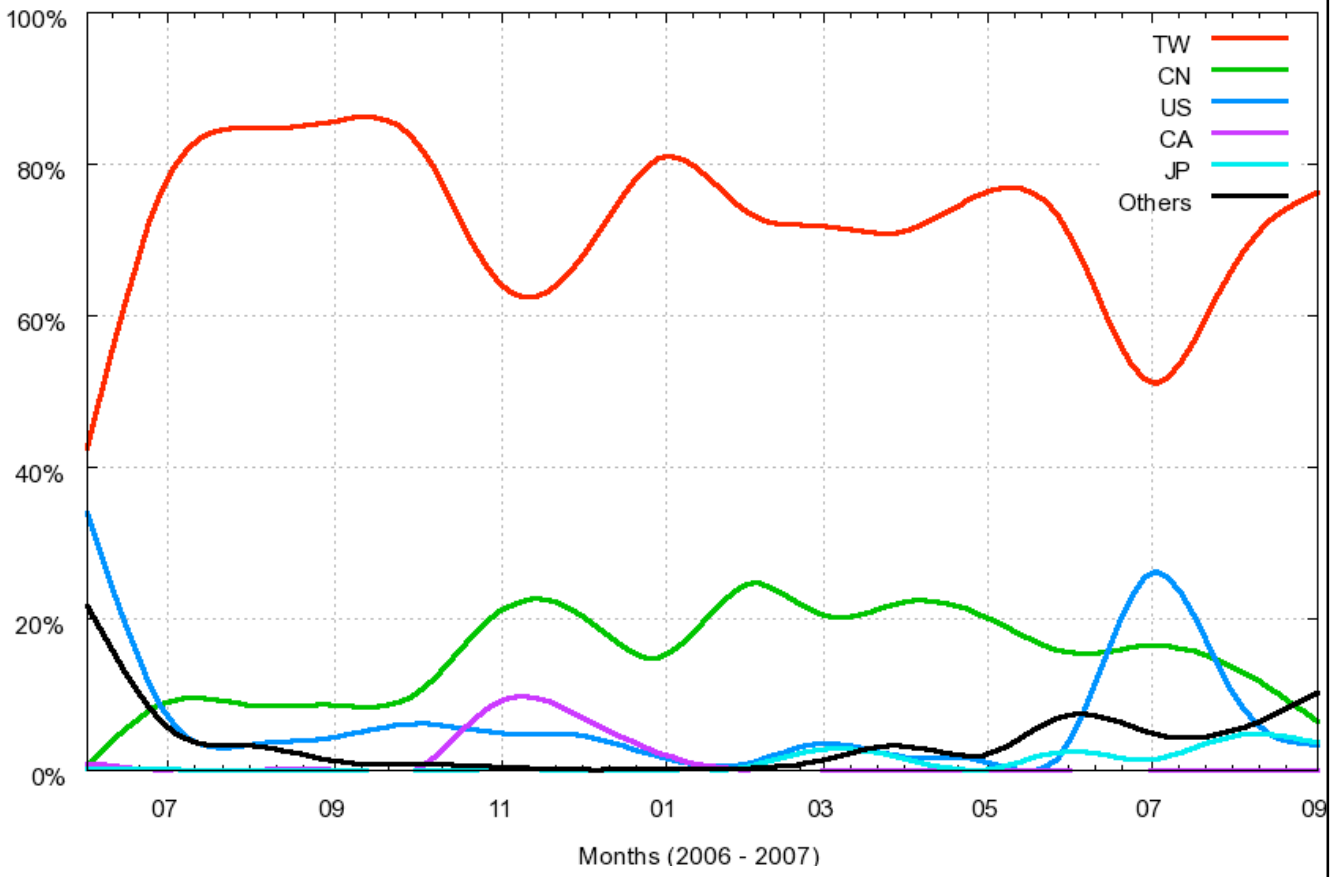
Total Data Collected in 466 Days of Operation

Data collected by 10 sensors	
E-mails captured (injected):	524.585.779
Potencial recipients	4.805.521.964
Average recipients/e-mail	≈ 9.1
Average captured e-mails/day	≈ 1.2 Million
Unique IPs that injected spam	216.888
Unique Autonomous Systems (AS)	3.006
Unique Country Codes (CCs)	165

Distribution by Country Code

#	CC	E-mails	%
01	TW	385,189,756	73.43
02	CN	82,884,642	15.80
03	US	29,764,293	5.67
04	CA	6,684,667	1.27
05	JP	5,381,192	1.03
06	HK	4,383,999	0.84
07	KR	4,093,365	0.78
08	UA	1,806,210	0.34
09	DE	934,417	0.18
10	BR	863,657	0.16
		Subtotal:	99.50

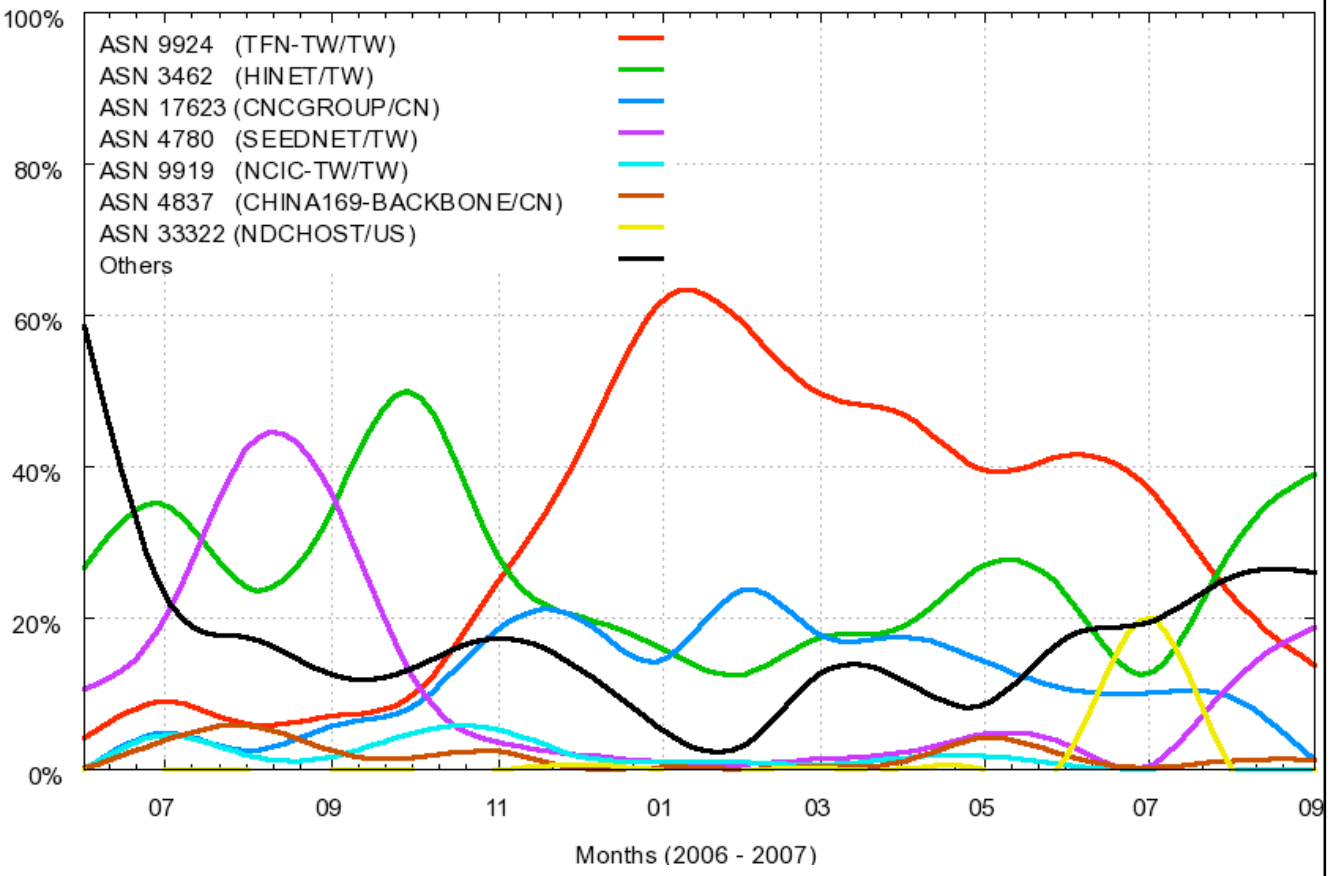
Percentage of Emails Received – Over the Period



Distribution by Autonomous System

#	AS	CC	%
01	TFN-TW	TW	32.60
02	HINET	TW	25.04
03	CNCGROUP	CN	12.43
04	SEEDNET	TW	10.38
05	NCIC-TW	TW	1.75
06	CHINA169	CN	1.72
07	NDCHOST	US	1.59
08	CHINANET	CN	1.39
09	EXTRALAN	TW	1.29
10	LOOKAS	CA	1.07
			89.26

Percentage of Emails Received – Over the Period



TCP Ports Abused Over the Period

#	TCP Port	Protocol	Usual Service	%
01	1080	SOCKS	socks	37.31
02	8080	HTTP	alternate http	34.79
03	80	HTTP	http	10.92
04	3128	HTTP	Squid	6.17
05	8000	HTTP	alternate http	2.76
06	6588	HTTP	AnalogX	2.29
07	25	SMTP	smtp	1.46
08	4480	HTTP	Proxy+	1.38
09	3127	SOCKS	MyDoom Backdoor	1.00
10	3382	HTTP	Sobig.f Backdoor	0.96
11	81	HTTP	alternate http	0.96

Requests to the HTTP and SOCKS Modules

Number of requests received by the modules, divided according to outbound requested connection type:

HTTP		
Type	Requests	%
connect to 25/TCP	**89,496,969**	**97.62**
connect to others	106,615	0.12
get	225,802	0.25
errors	1,847,869	2.01
total	91,677,255	100.00

SOCKS		
Type	Requests	%
connect to 25/TCP	**46,776,884**	**87.31**
connect to others	1,055,081	1.97
errors	5,741,908	10,72
total	53,573,873	100.00

Among the Activities Observed...

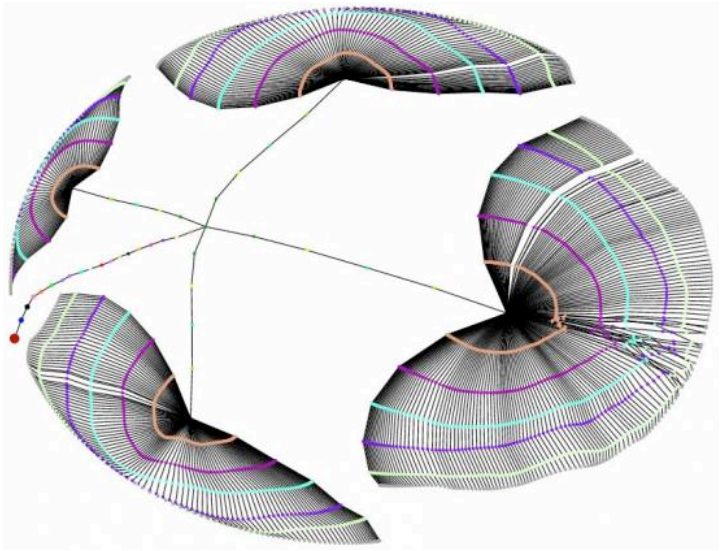
- Main results:
  - 99.84% of connections originated from abroad
  - Spammers used all the upload bandwidth available
  - More than 90% of spams targetted networks in other countries

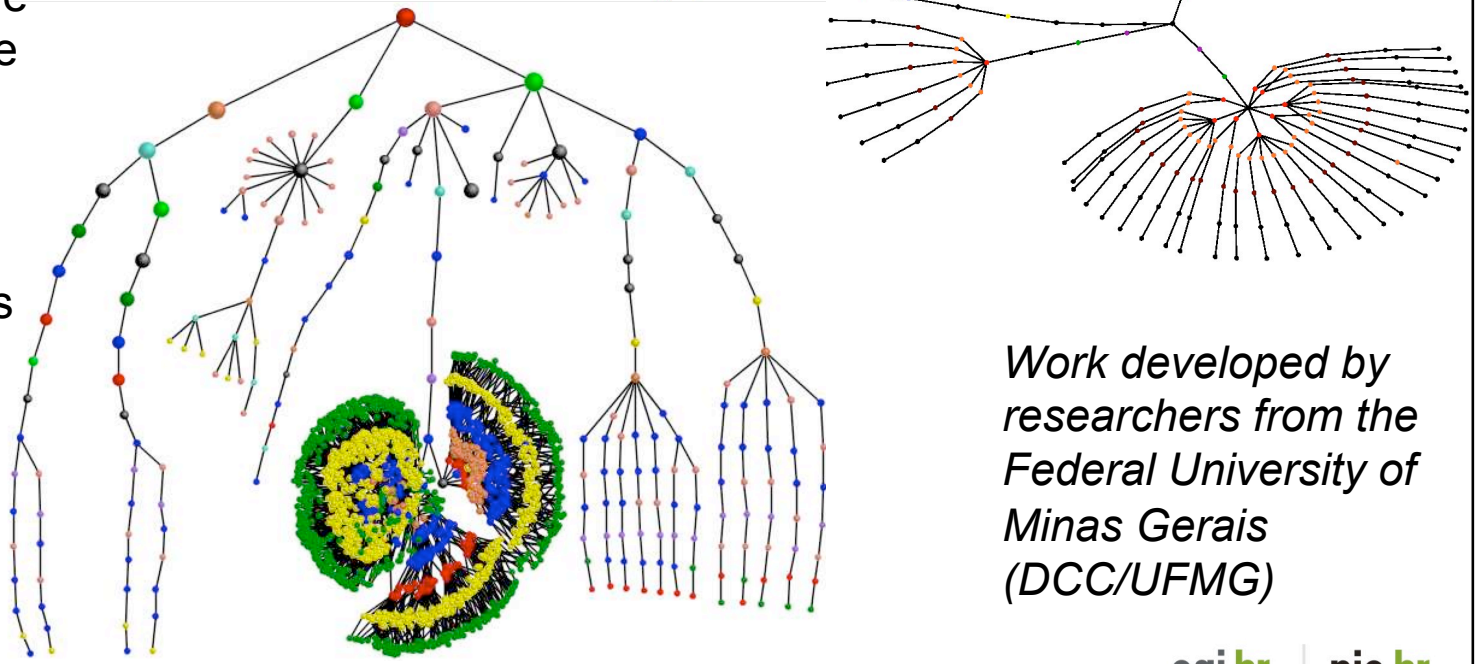
- Among the outgoing activity that was not aimed at port 25/TCP:
  - attempts to connect to Yahoo! servers using the Yahoo! Messenger Protocol, via the abuse of SOCKS proxies

Current Anti-spam Activities

Data Mining: Characterization of Spam Campaigns

- Frequent Pattern Tree showing different spam campaigns
  - node's color represents a different feature that varied among the messages at that level
  - diameter of the node is proportional to the log of the frequency of the characteristic in the campaign
- Some characteristics taken into account:
  - Common keywords
  - Message layout
  - Language
  - Encoding type
  - Similar URLs
  - Services abused



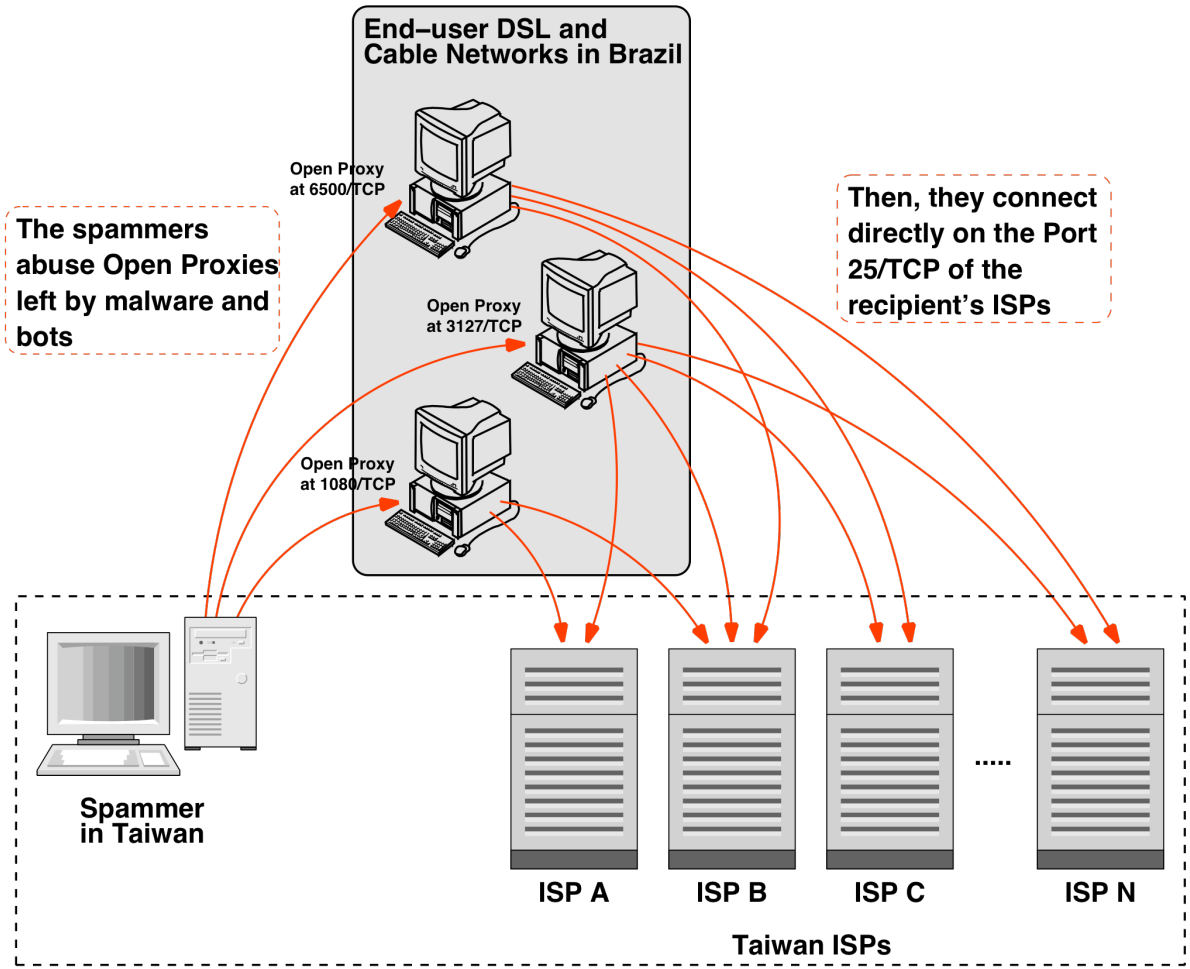


Work developed by researchers from the Federal University of Minas Gerais (DCC/UFMG)

Collaboration with TW Authorities

- MoU with TW NCC (National Communications Commission), TWCERT/CC and TWIA (Taiwan Internet Association)
  - Send data weekly about spam coming from and returning to Taiwan
  - They are identifying and shuting down spammers operations
  - We are discussing the implementation of a sensor in Taiwan

How spammers from Taiwan abuse the DSL and Cable Networks in Brazil



Collaboration with JP Authorities

- In the past few months the activities seen changed
  - IPs assigned to Philipines are attempting to send spam to mobile phones in Japan
- JPCERT/CC and the Japanese Embassy in Brazil contacted us regarding "spam coming from Brazil"
  - the data being collected at the active sensors is being sent to them so they can pursue their investigations
  - They are sharing a case study on the success of Port 25 Management adoption in Japan, regarding the abuse of Japanese networks for sending spam

Understanding the Abuse of Worldwide Distributed Networks for sending Spam: SpamPots Project

2nd Phase

Deployment of spampots' sensors worldwide

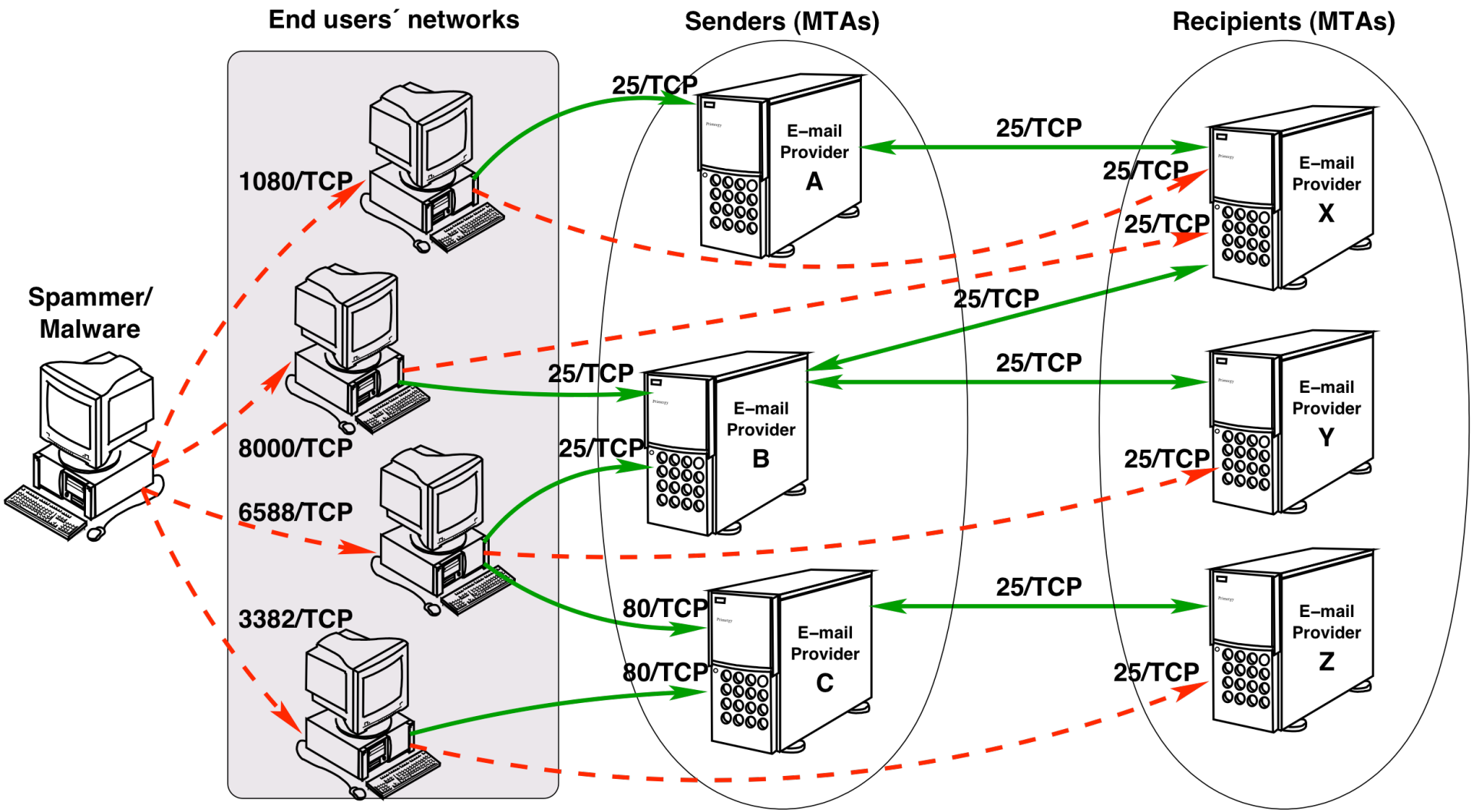
- Global view of the data
- Help other networks to understand and prevent being abused by spammers
- Better understand the abuse of the Internet infrastructure by spammers
- Use the spam collected to improve antispam filters
- Develop better ways to
  - identify phishing and malware
  - identify botnets via the abuse of open proxies and relays
- Provide data to trusted parties
  - help the constituency to identify infected machines
  - identify malware and scams targeting their constituency

We are Looking for Partners Interested in...

- Receiving data
  - spams, URLs, IPs abusing the sensors, etc
- Hosting a sensor
- Helping to improve the technology
  - Analysis, capture, collection, correlation with other data sources, etc
- All partners will have access to all data if they want
- We are currently working with networks in the following countries/economies: AU, UY, PL, TW, HK and JP.

Preventing the Abuse: Port 25 Management

Current Scenario: The Abuse

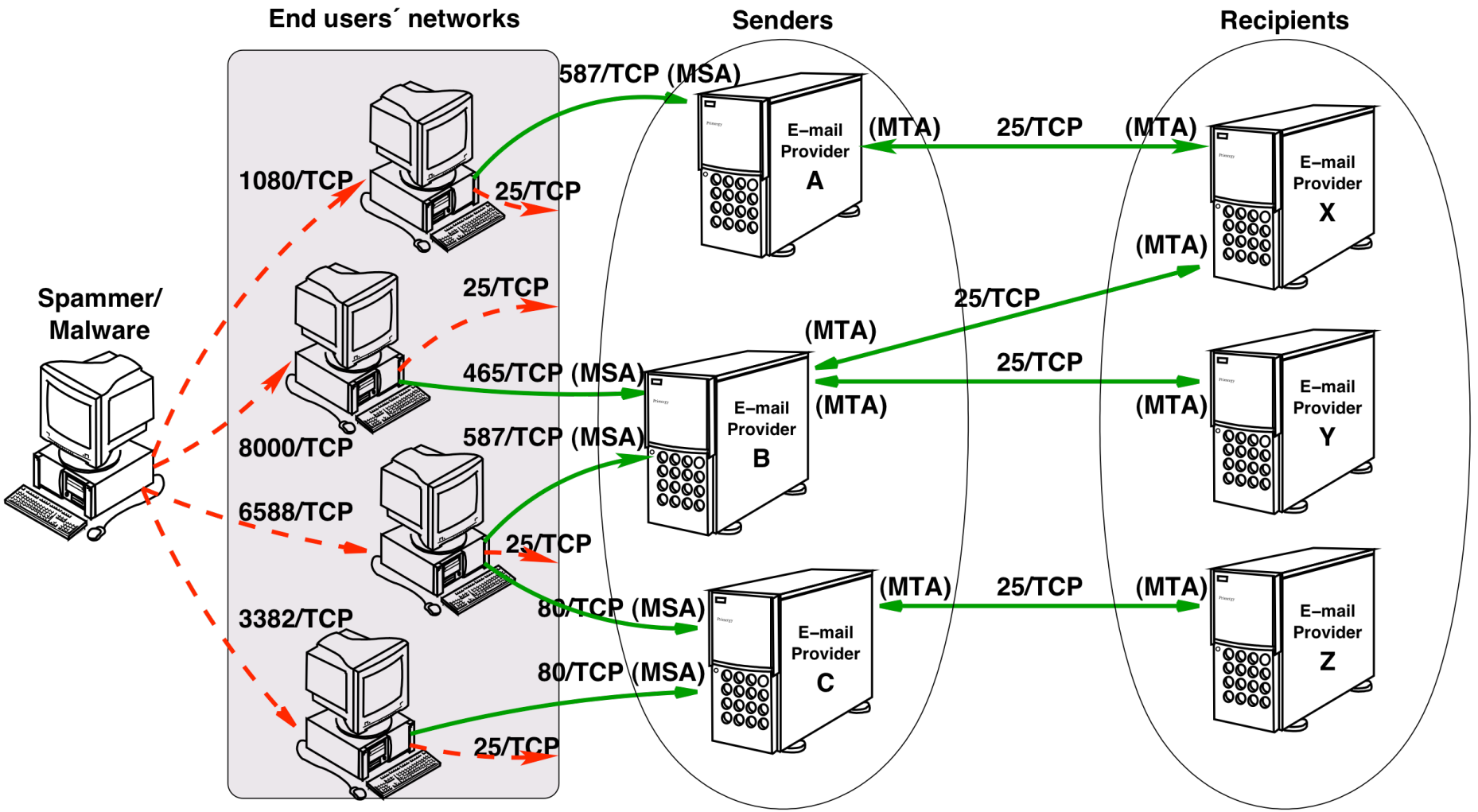


Port 25 Management

Differentiate client-server email submission from the email transmission among servers

- The adoption of port 25 management need to be articulated among competing sectors
  - Email providers
    - deploy message submission, typically on port 587/TCP (RFC 4409), and deploy SMTP authentication
  - Broadband/dial-up providers (for end users)
    - prevent email direct delivery (filtering outgoing traffic targetting port 25/TCP)

Port 25 Management: Impact



Port 25 Management: Benefits

- Network provider IP blocks excluded from block lists
- Less end user complaints
- Makes the abuse of the Internet infrastructure for malicious activities (fraud, identity theft, etc) harder
- Enhances the ability of tracking abuse cases
- Acts on the submission, before the message gets in the email infrastructure
- Reduces the international bandwidth consumption by spammers
- Reduces operational costs
  - Spam was pointed out as the main responsible for consuming the largest amount of operational resources on “2008 Worldwide Infrastructure Security Report” (http://www.arbornetworks.com/report)

Port 25 Management: Adoption & Challenges

- Adoption
  - Wolrdwide
    http://www.antispam.br/admin/porta25/adocao/
  - Brazil
    Sercomtel (Londrina/PR)

- CGI.br's Resolution CGI.br/RES/2009/001/P
  http://www.cgi.br/regulamentacao/resolucao2009-001.htm

- Challenges
  - Increase on the load of provider's user support
  - Network providers need to differentiate between end user and business connections
  - Exception handling (outdated/legacy software)

Port 25 Management on Antispam.br

User Awareness

Antispam.br Website - Malicious Code Through E-mail

Antispam.br ::

http://www.antispam.br/tipos/malware/

Comitê Gestor da Internet no Brasil

Sobre o NIC.br | Indicadores | Antispam.br | PTT.br

nic.br — Núcleo de Informação e Coordenação

cgi.br — Registro CERT.br

Início - Administradores de redes - Estatísticas - Sobre o Antispam.br

antispam.br

- O que é spam?
- Problemas causados pelo spam
- Origem e curiosidades
- Tipos de spam
- Como identificar
- Prevenção
- Boas práticas
- Dicas
- Como reclamar
- FAQ
- Links
- Glossário
- Créditos
- Mapa do site

Busca

ok

NIC.br | Antispam.br | CERT.br | Registro.br

Tipos de spam

Voltar

Códigos maliciosos

São programas que executam ações maliciosas em um computador. Diversos tipos de códigos maliciosos são inseridos em *e-mails*, contendo textos que se valem de métodos de engenharia social para convencer o usuário a executar o código malicioso em anexo. Em geral, estes códigos também são utilizados em **spams enviados por fraudadores**.

Dentre os códigos mais comuns enviados via spam, pode-se citar as seguintes categorias:

- **Backdoor:** Programa que permite a um invasor retornar a um computador comprometido. Normalmente este programa é colocado de forma a não ser notado.
- **Spyware:** Termo utilizado para se referir a uma grande categoria de software que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros. Podem ser utilizados de forma legítima, mas, na maioria das vezes, são utilizados de forma dissimulada, não autorizada e maliciosa.
- **Keylogger:** Programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador. Normalmente, a ativação do keylogger é condicionada a uma ação prévia do usuário, como por exemplo, após o acesso a um site de comércio eletrônico ou Internet Banking, para a captura de senhas bancárias ou números de cartões de crédito.
- **Screenlogger:** Forma avançada de keylogger, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou armazenar a região que circunda a posição onde o mouse é clicado.
- **Cavalo de tróia:** Programa, normalmente recebido como um "presente" (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo, etc), que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.

Antispam.br Website - Fraud, Phishing, Scam, etc

Antispam.br ::

http://www.antispam.br/tipos/fraudes/

Comitê Gestor da Internet no Brasil

Sobre o NIC.br | Indicadores | Antispam.br | PTT.br

nic.br Núcleo de Informação e Coordenação

cgi.br Registro CERT.br

Início - Administradores de redes - Estatísticas - Sobre o Antispam.br

antispam.br

- O que é spam?
- Problemas causados pelo spam
- Origem e curiosidades
- Tipos de spam
- Como identificar
- Prevenção
- Boas práticas
- Dicas
- Como reclamar
- FAQ
- Links
- Glossário
- Créditos
- Mapa do site

Busca

ok

NIC.br Antispam.br CERT.br Registro.br

Tipos de spam

Voltar

Fraudes

Normalmente, não é uma tarefa simples atacar e fraudar dados em um servidor de uma instituição bancária ou comercial. Então, atacantes têm concentrado seus esforços na exploração de fragilidades dos usuários, para realizar fraudes comerciais e bancárias através da Internet.

Para obter vantagens, os fraudadores têm utilizado amplamente *e-mails* com discursos que, na maioria dos casos, envolvem engenharia social e que tentam persuadir o usuário a fornecer seus dados pessoais e financeiros. Em muitos casos, o usuário é induzido a instalar algum código malicioso ou acessar uma página fraudulenta, para que dados pessoais e sensíveis, como senhas bancárias e números de cartões de crédito, possam ser furtados. Desta forma, é muito importante que usuários de Internet tenham certos cuidados com os *e-mails* que recebem e ao utilizarem serviços de comércio eletrônico ou *Internet Banking*.

Sumário

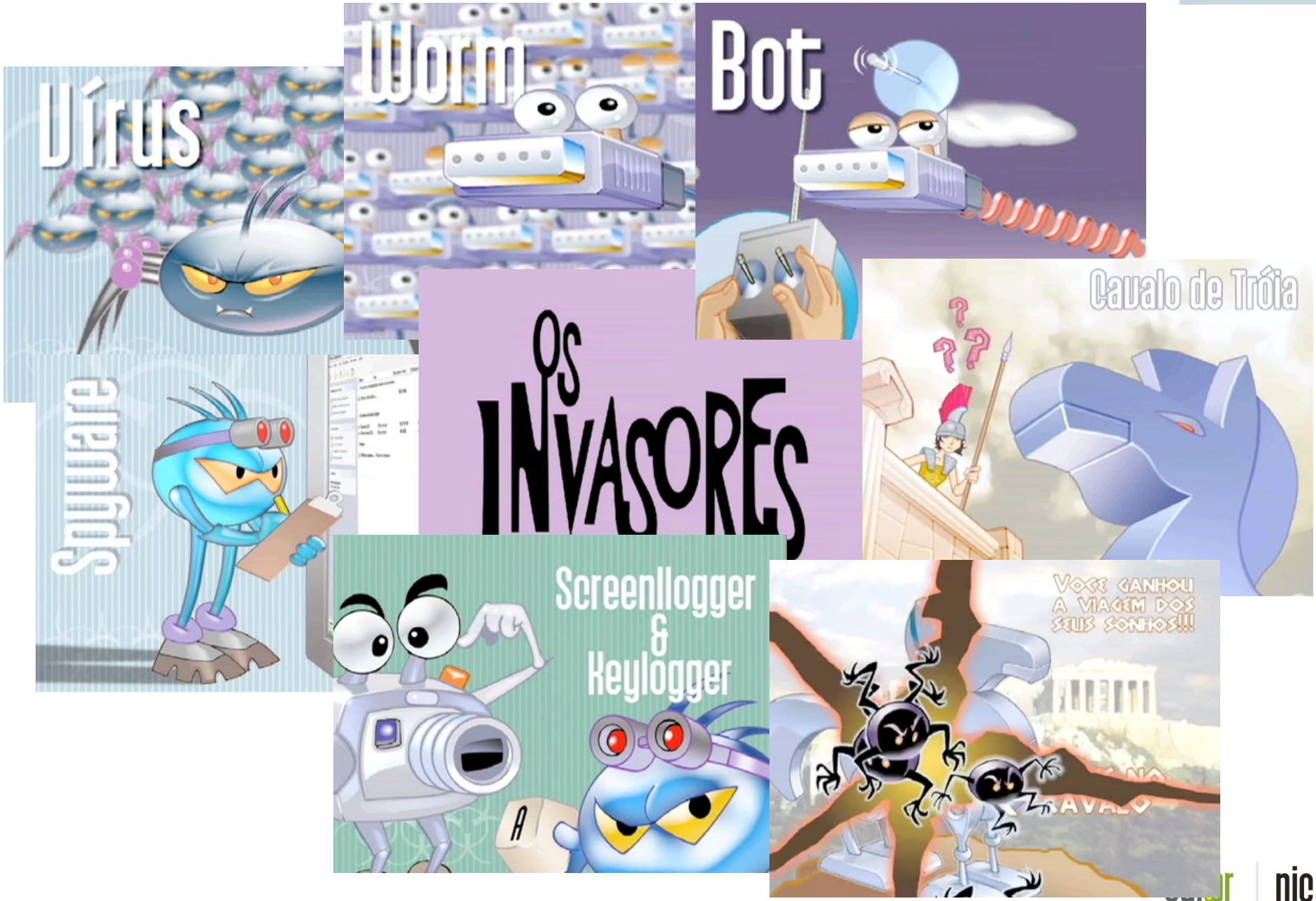
Golpes (*Scams*)

Cartoons

- 4 videos – ≈ 4 minutes each
  - The Internet
  - The Intruders
  - Spam
  - The Defense
  - Freely available on the Internet
  - In several formats and resolutions
- English version (subtitles) already available: **http://www.antispam.br/videos/english/**
- English (voice-over and written texts) to be released very soon
- Q-CERT interested in making an Arabic voice-over

Video 1: The Internet

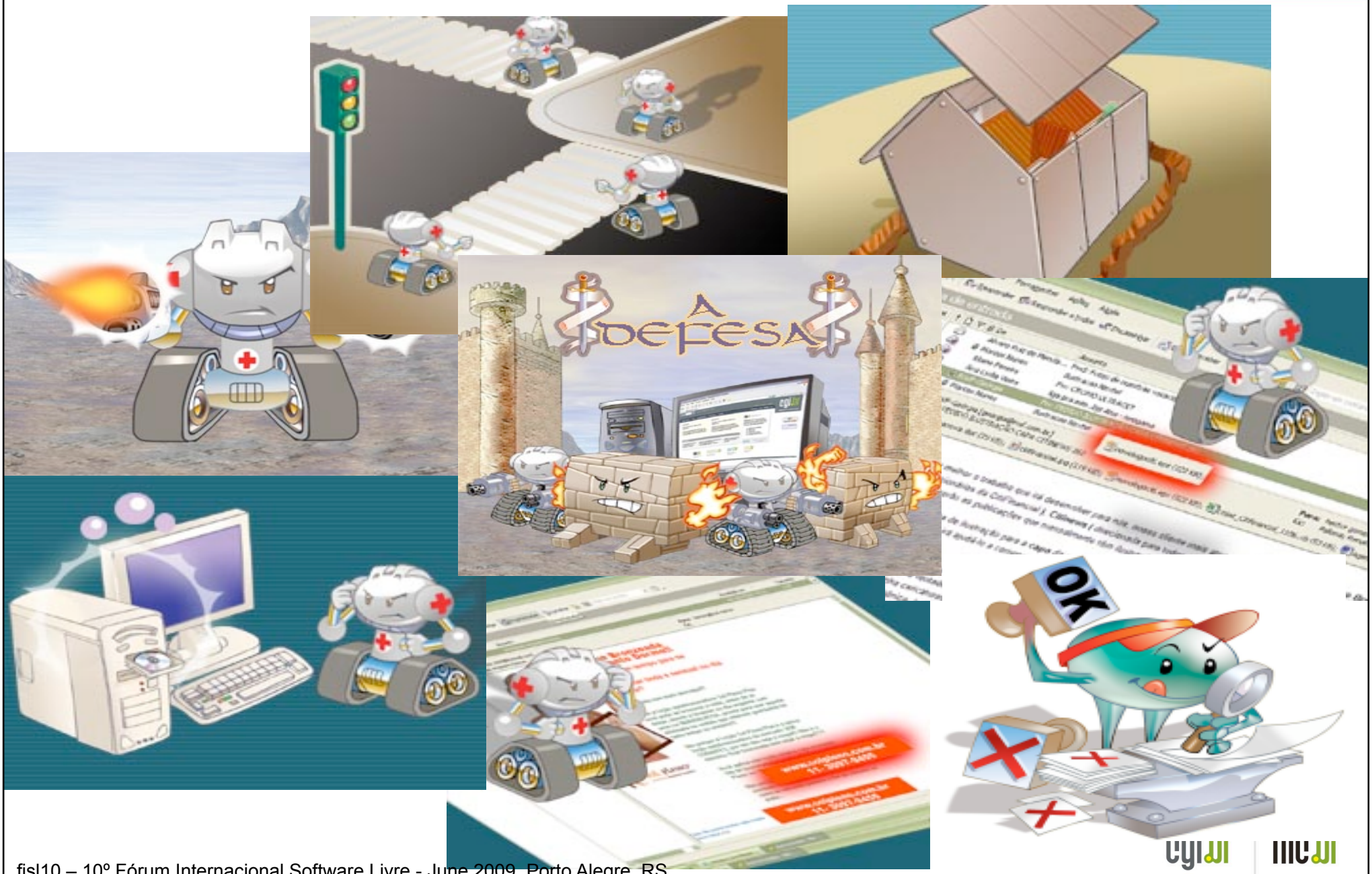
Video 2: The Intruders



Video 3: Spam


SPAM
SPIT ou SPIM
Spaum (online)
Localizar um contato...
Você tem 5 solicitações....
Oscar- Freelas para redator....
Robert- La donna é mobile...
Rodrigon-
SUPER SOFT
10,00

Video 4: The Defense



Stickers with the Characters

Additional References

- This presentation (next week)
  http://www.cert.br/docs/presentations/

- CERT.br
  Computer Emergency Response Team Brazil
  http://www.cert.br/

- Antispam.br
  http://www.antispam.br/