Estrutura e Situação da Segurança da Internet no Brasil

Cristine Hoepers

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil - CERT.br

Núcleo de Informação e Coordenação do Ponto br - NIC.br
Comitê Gestor da Internet no Brasil - CGI.br

Agenda

- Estrutura do CGI.br, NIC.br e CERT.br
- Evolução do Tratamento de Incidentes no Brasil
- Missão do CERT.br e seu papel na segurança da Internet no Brasil
- Situação da segurança em números
  - Incidentes reportados ao CERT.br
  - Pesquisa nacional
  - Outros números
- Considerações finais

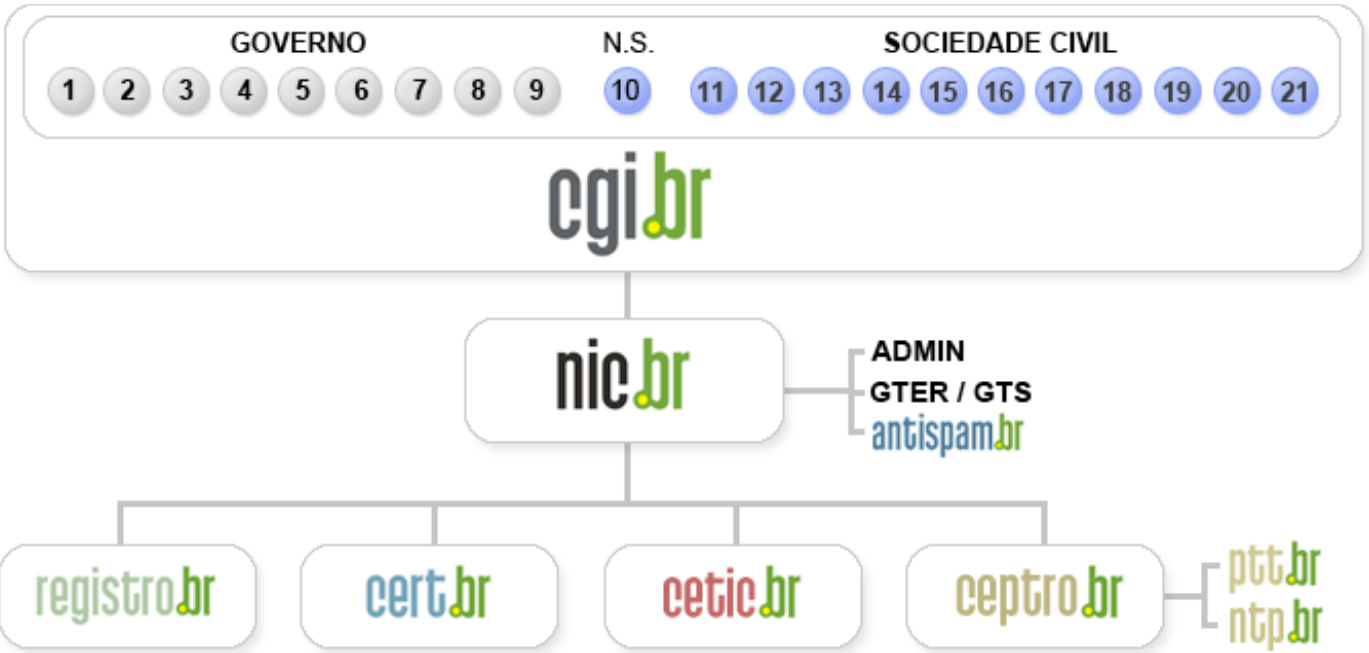
Comitê Gestor da Internet no Brasil – CGI.br

Dentre as atribuições definidas no Decreto Presidencial nº 4.829 destacam-se:

- **a proposição de normas e procedimentos relativos à regulamentação das atividades na internet;**
- **a recomendação de padrões e procedimentos técnicos operacionais para a internet no Brasil;**
- **o estabelecimento de diretrizes estratégicas relacionadas ao uso e desenvolvimento da internet no Brasil;**
- **a promoção de estudos e padrões técnicos para a segurança das redes e serviços no país;**
- **a coordenação da atribuição de endereços internet (IPs) e do registro de nomes de domínios usando <.br>;**
- **a coleta, organização e disseminação de informações sobre os serviços internet, incluindo indicadores e estatísticas.**

http://www.cgi.br/sobre-cg/

Estrutura do CGI.br e NIC.br



1 – Ministério da Ciência e Tecnologia (Coordenação)
2 – Ministério das Comunicações
3 – Casa Civil da Presidência da República
4 – Ministério da Defesa
5 – Ministério do Desenvolvimento, Indústria e Comércio Exterior
6 – Ministério do Planejamento, Orçamento e Gestão
7 – Agência Nacional de Telecomunicações (Anatel)
8 – Conselho Nacional de Desenvolvimento Científico e Tecnológico
9 – Fórum Nacional de Secretários Estaduais para Assuntos de C&T
10 – Representante de Notório Saber em assuntos de Internet

11 – provedores de acesso e conteúdo
12 – provedores de infra-estrutura de telecomunicações
13 – indústria de bens de informática, telecomunicações e software
14 – segmento das empresas usuárias de Internet
15-18 – representantes do terceiro setor
19-21 – representantes da comunidade científica e tecnológica

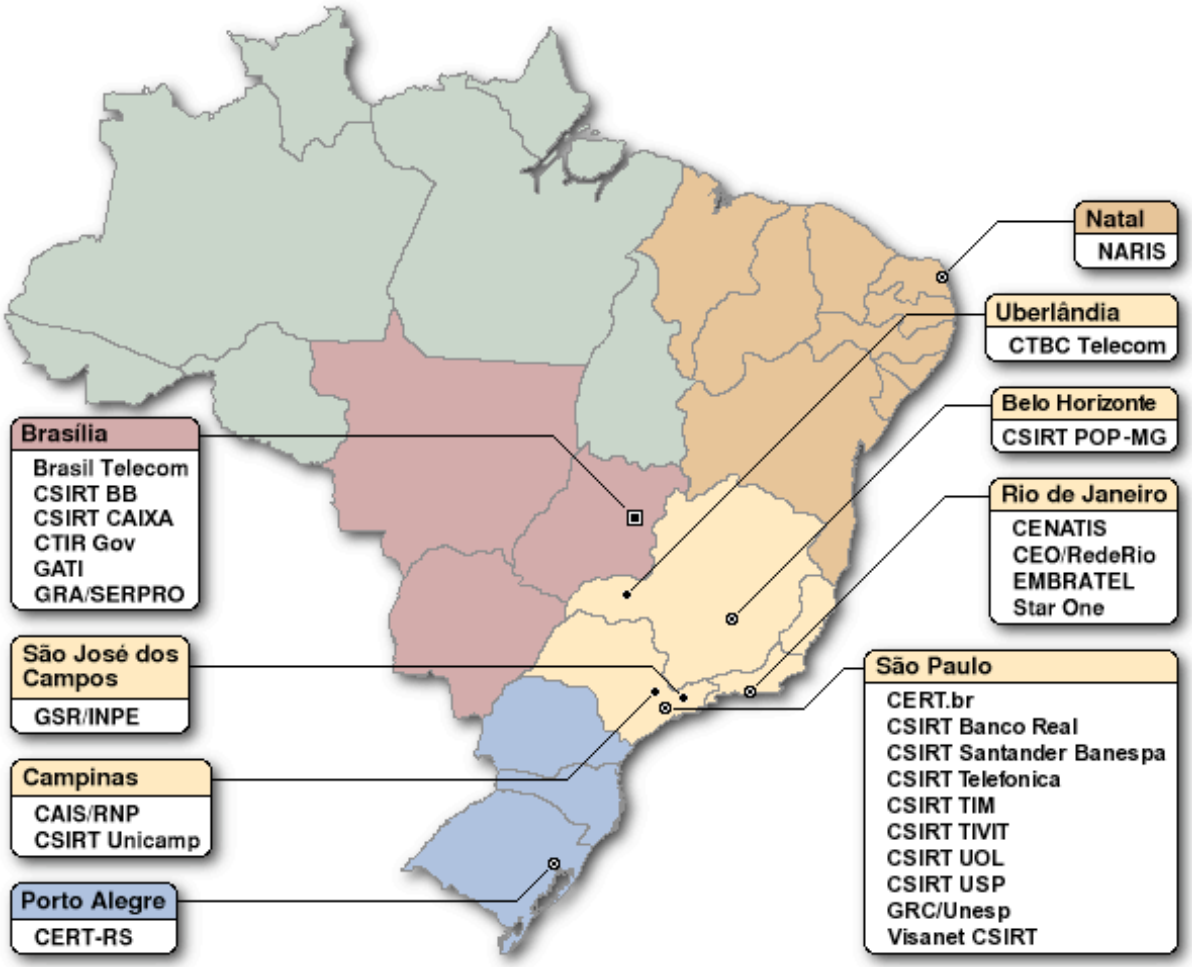
Evolução do Tratamento de Incidentes no Brasil (1/2)

- **Agosto/1996: o relatório "Rumo à Criação de uma Coordenadoria de Seguraça de Redes na Internet Brasil" é publicado pelo CGI.br[1]**
- **Junho/1997: o CGI.br cria o CERT.br (naquele tempo chamado NBSO – *NIC BR Security Office*), com base nas recomendações do relatório, como um grupo com responsabilidade nacional[2]**
- **Agosto/1997: a RNP cria seu próprio CSIRT (CAIS)[3], seguida pela rede acadêmica do Rio grande do Sul (CERT-RS)[4]**
- **1999: outras instituições, incluindo Universidades e Operadoras de Telecomunicações, iniciaram a formação de seus CSIRTs**
- **2003/2004 : grupo de trabalho para definição da estrutura de um CSIRT para a Administração Pública Federal**
- **2004: o CTIR Gov foi criado, com a Administração Pública Federal como seu público alvo[5]**

[1] http://www.nic.br/grupo/historico-gts.htm
[2] http://www.nic.br/grupo/gts.htm
[3] http://www.rnp.br/_arquivo/documentos/rel-rnp98.pdf
[4] http://www.cert-rs.tche.br/cert-rs.html
[5] http://www.ctir.gov.br

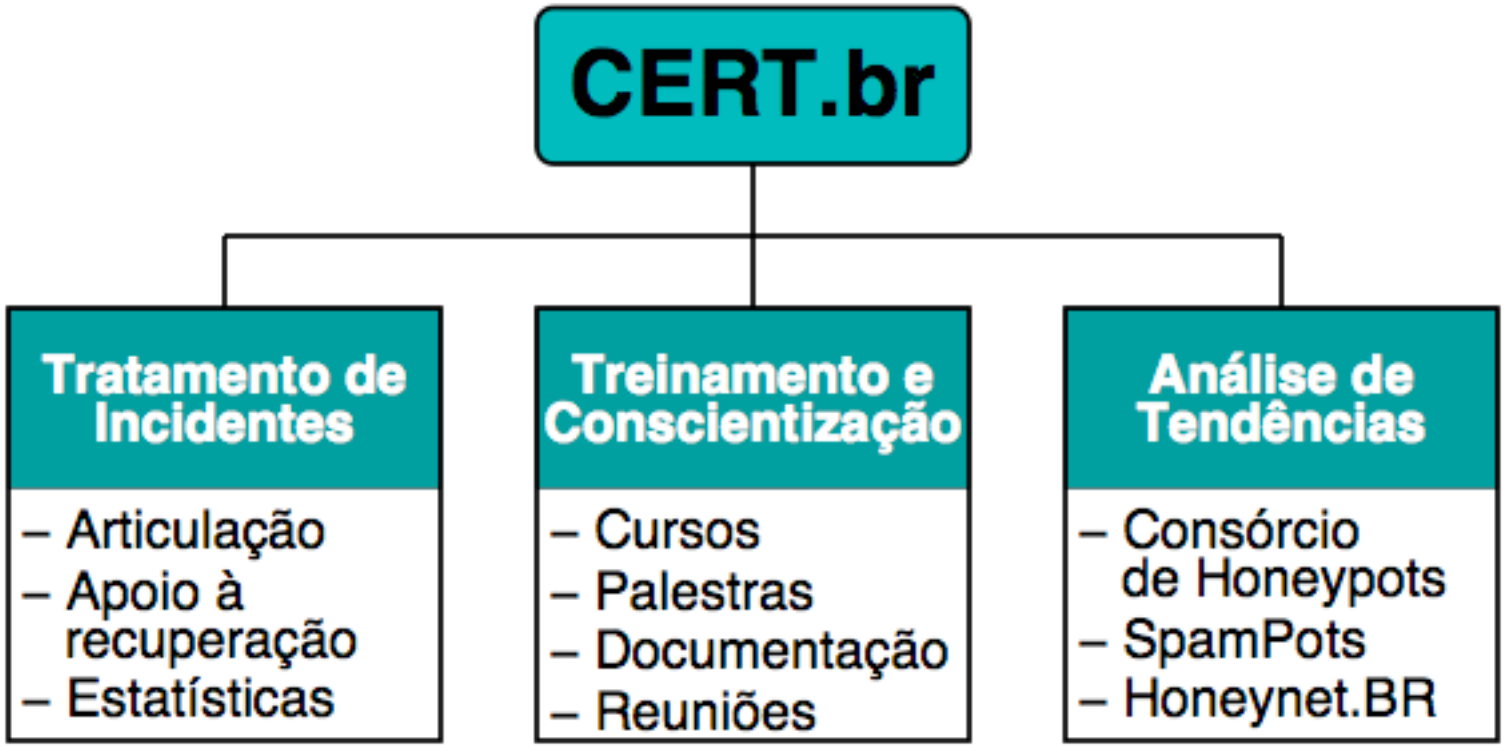
Grupos de Tratamento de Incidentes (CSIRTs/CERTs) no Brasil

Sector	CSIRTs
Resposabilidade Nacional	CERT.br
Redes de Governo	CTIR Gov, GATI, GRA/SERPRO
Setor Financeiro	CSIRT BB, CSIRT CAIXA, CSIRT Banco Real, CSIRT Santander Banespa, Visanet CSIRT
Telecom/ISP	Brasil Telecom, CTBC Telecom, EMBRATEL, StarOne, CSIRT Telefonica, CSIRT TIM, CSIRT UOL
Redes Acadêmicas e de Pesquisa	GSR/INPE, CAIS/RNP, CSIRT Unicamp, CERT-RS, NARIS, CSIRT POP-MG, CENATIS, CEO/RedeRio, CSIRT USP, GRC.UNESP
Outsourcing	CSIRT TIVIT



http://www.cert.br/contato-br.html

Atividades do CERT.br



Parcerias Internacionais:

FIRST Improving Security Together MEMBER

Anti-Phishing Working Group APWG

SEIPartner CERT Courses

The Honeynet PROJECT®

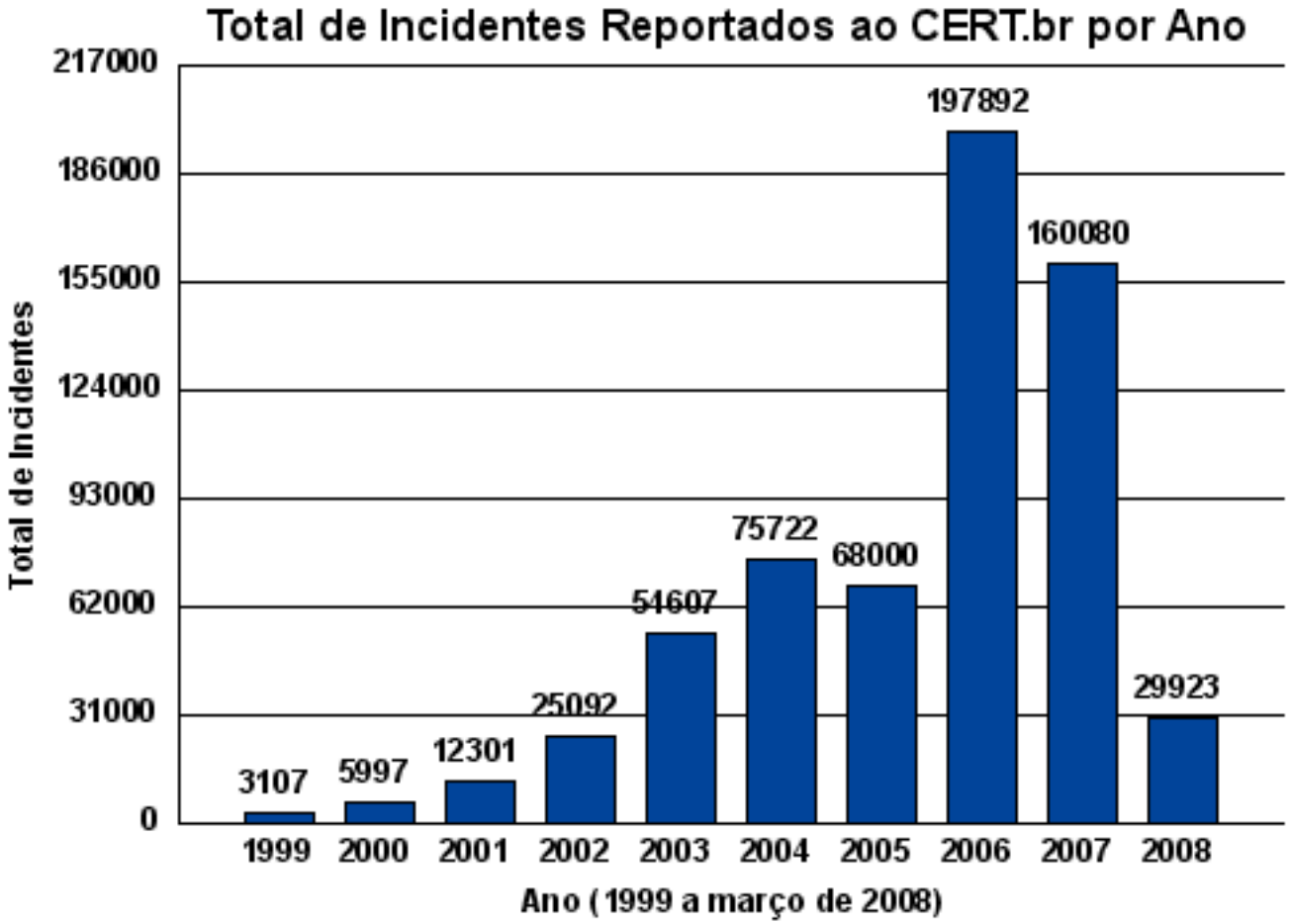
Apoio e Treinamento para Novos CSIRTs

- **Auxílio no estabelecimento das atividades**
  - **Reuniões, palestras, treinamentos, etc**
- ***SEI/CMU Partner* desde 2004, licenciado para ministrar os cursos do *CERT® Program* no Brasil:**
  - **http://www.cert.br/cursos/**
    - ***Information Security for Technical Staff***
    - ***Overview of Creating and Managing Computer Security Incident Response Teams***
    - ***Fundamentals of Incident Handling***
    - ***Advanced Incident Handling for Technical Staff***
  - **240+ profissionais treinados**

Tratamento de Incidentes

- **Articulação das ações para o tratamento de incidentes envolvendo redes brasileiras**
  - **Contato nacional para notificação de incidentes de segurança**
  - **Manutenção de estatísticas sobre as notificações de incidentes recebidas**
    - **http://www.cert.br/stats/incidentes/**
    - **http://www.cert.br/stats/spam/**
  - **Desenvolvimento de documentos de boas práticas para usuários e administradores de redes**
    - **Práticas de Segurança para Administradores de Redes Internet http://www.cert.br/seg-adm-redes/**
    - **Cartilha de Segurança para Internet http://cartilha.cert.br/**

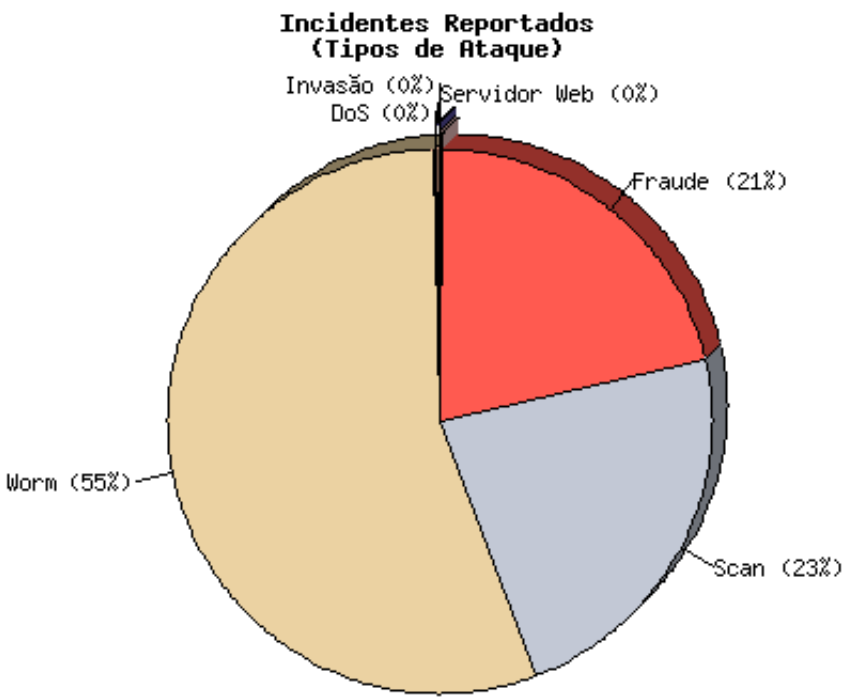
Incidentes Reportados ao CERT.br



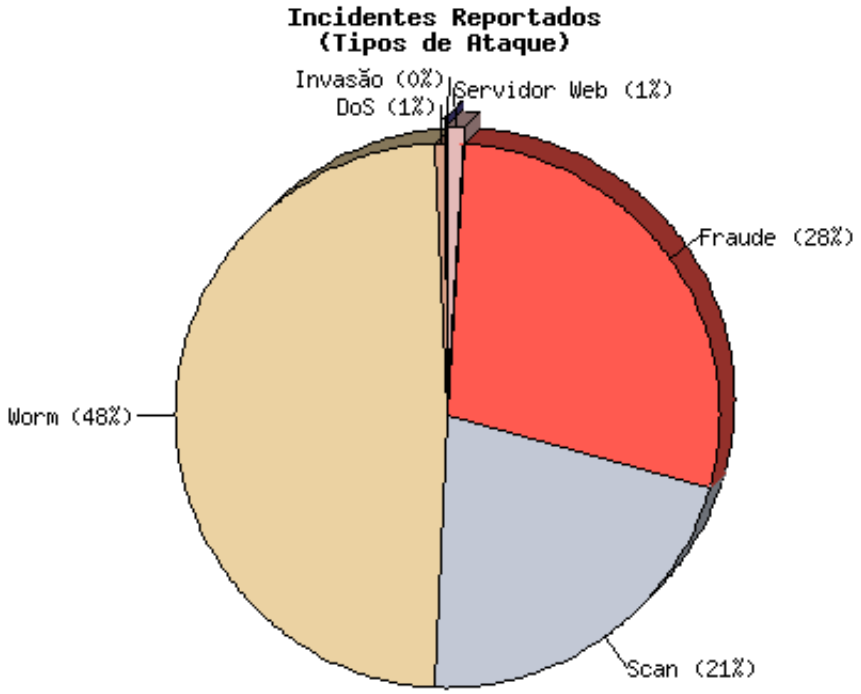
http://www.cert.br/stats/incidentes/

Incidentes Reportados ao CERT.br – Tipos (1/2)

2006



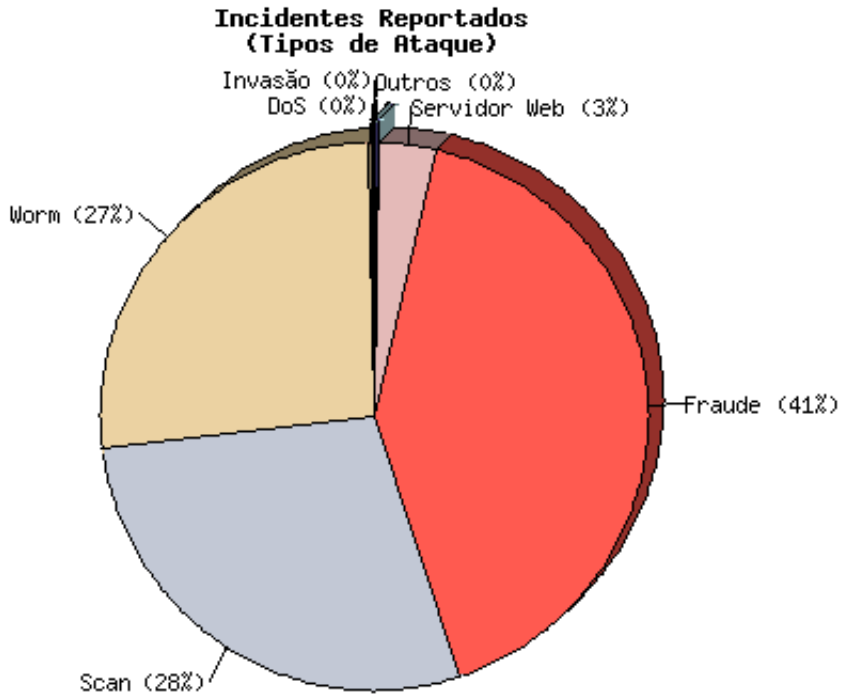
2007



http://www.cert.br/stats/incidentes/

Incidentes Reportados ao CERT.br – Tipos (2/2)

2008 – 1º trimestre



Totais da categoria tentativas de fraude:

2004:	**4.015**	**(05%)**
2005:	**27.292**	**(40%)**
2006:	**41.776**	**(21%)**
2007:	**45.298**	**(28%)**
2008:	**12.352**	**(41%)**

Características das tentativas de fraude:

Spams

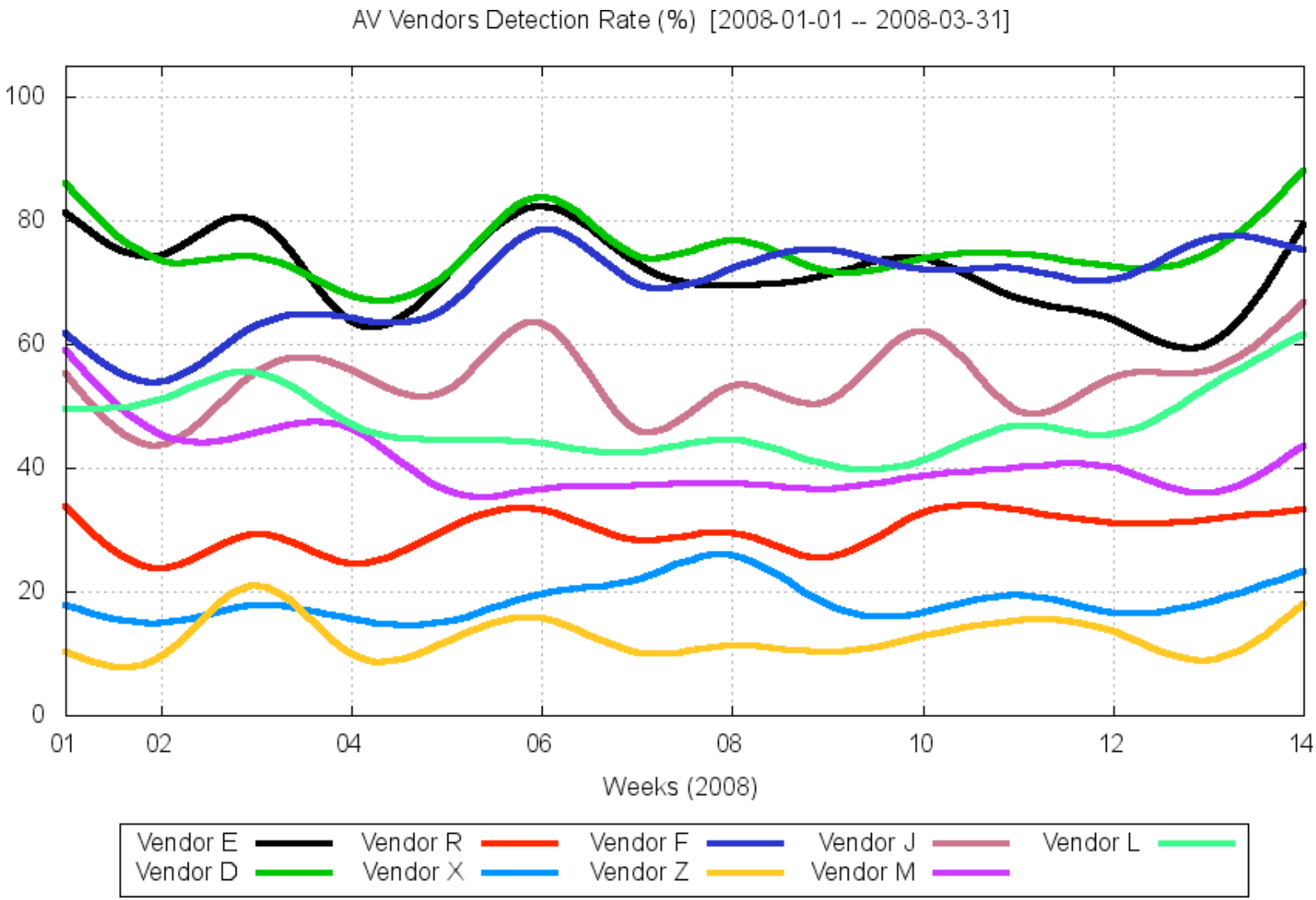
- **Em nome das mais variadas instituições e com tópicos diversos**
- **Com *links* para códigos maliciosos (cavalos de tróia)**

http://www.cert.br/stats/incidentes/

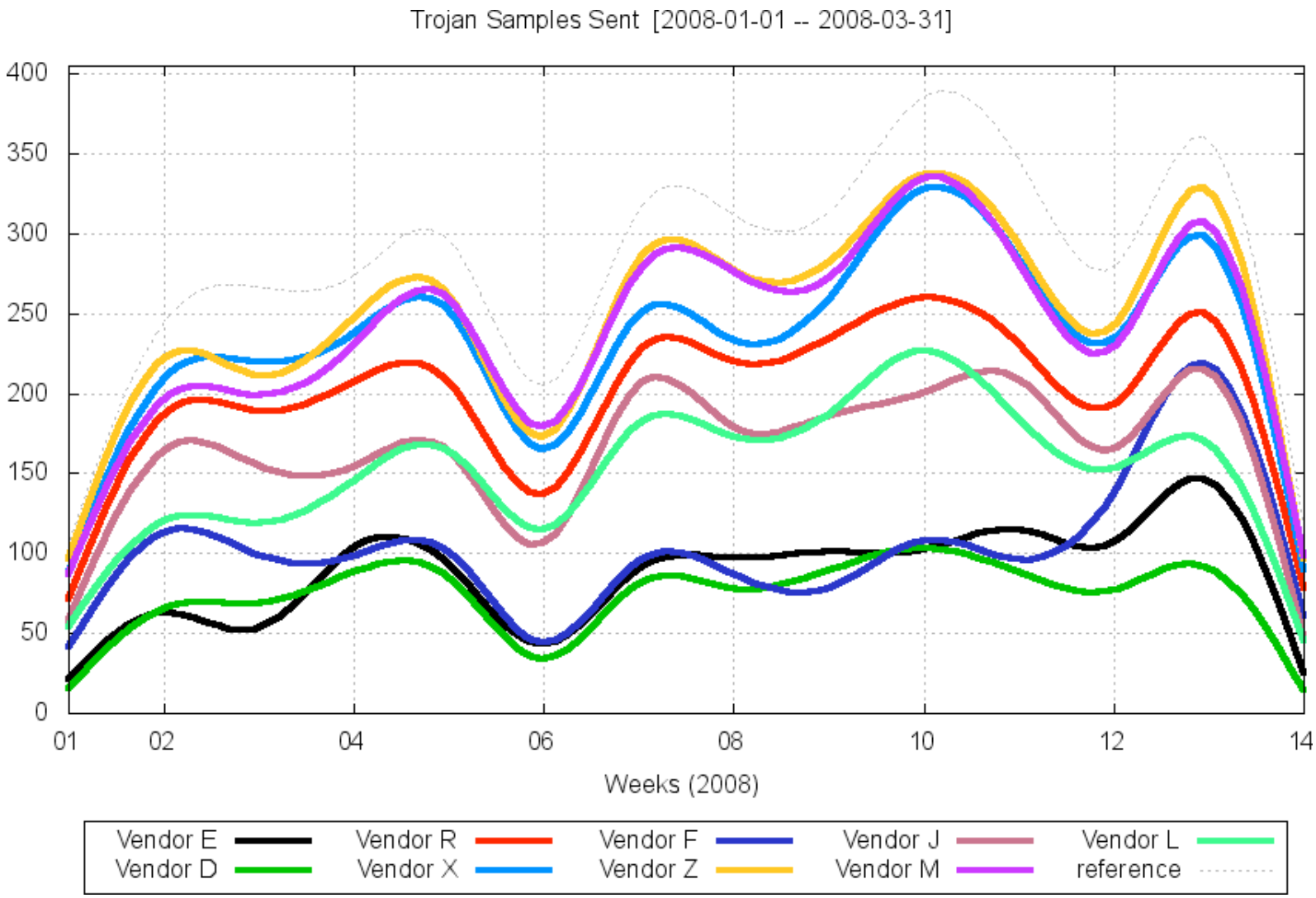
1º Trimestre/2008: Detalhes dos Códigos e URLs

Assinaturas de antivírus ("famílias")	47
Assinaturas de antivírus (únicas)	1.344
Blocos CIDR	701
Contatos de domínios/redes	718
Domínios	1.803
Extensões de arquivos usadas	64
Endereços IP únicos	1.298
Países de origem	58
Nomes de arquivos	2.696
URLs únicas	4.718
Códigos maliciosos únicos (hashes criptográficos únicos)	3.823

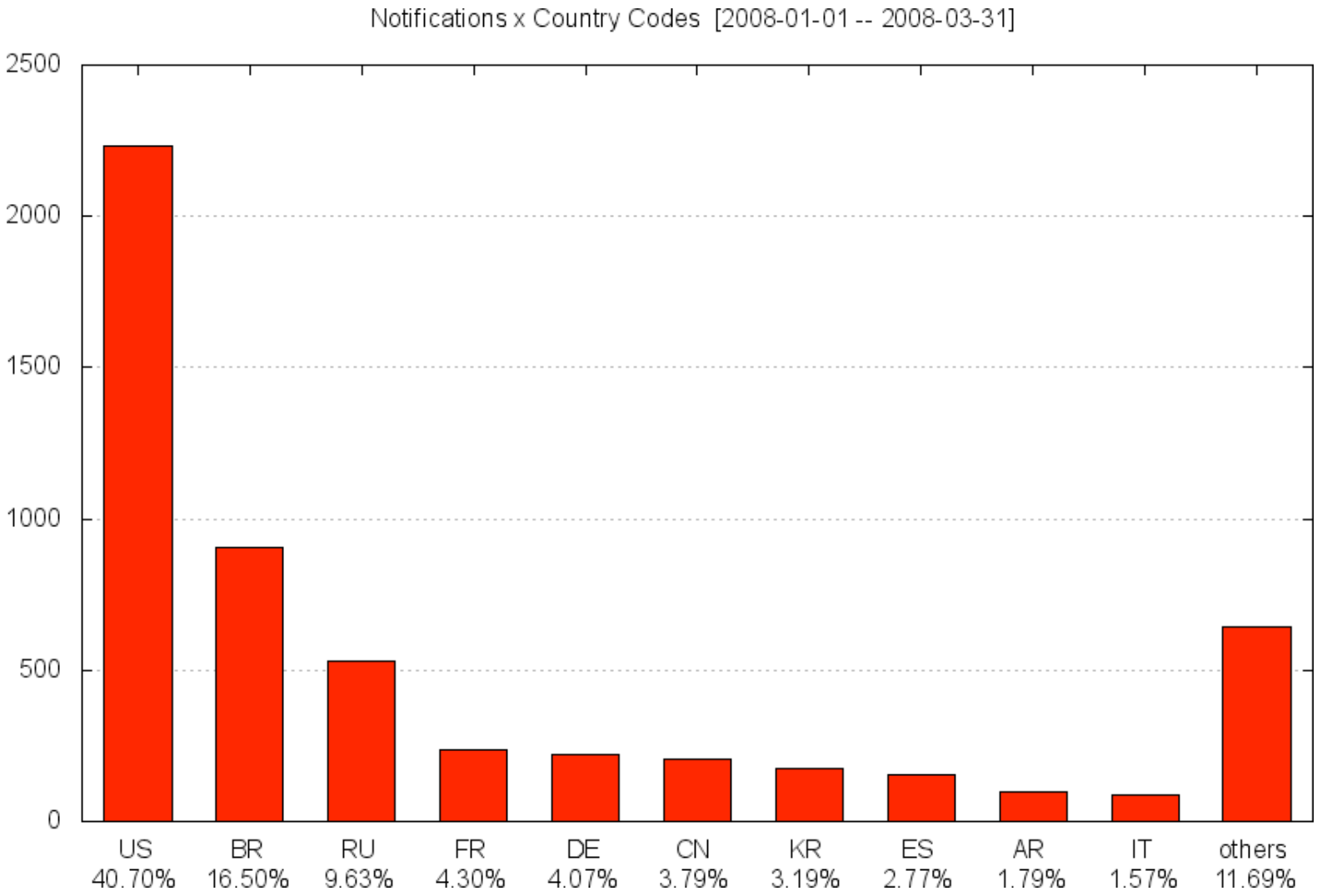
1º Trimestre/2008: Eficiência dos Antivírus



1º Trimestre/2008: Exemplares Enviados



1º Trimestre/2008: Países Hospedando os Códigos



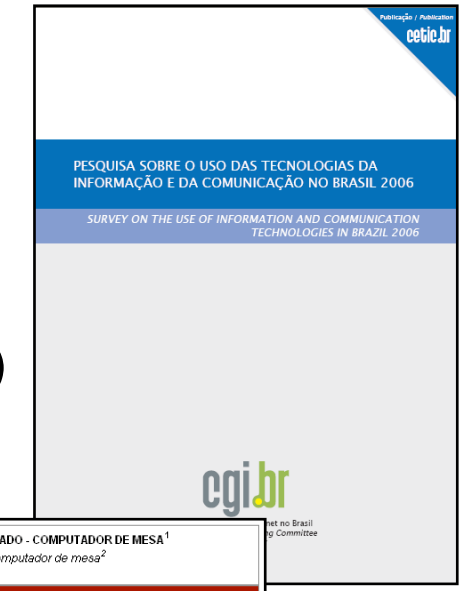
Pesquisas: TIC Domicílios e TIC Empresas

Investigam a disponibilidade e uso da internet,
incluindo questões específicas sobre:

- *governo eletrônico*
- *comércio eletrônico*
- *segurança*
- *habilidades*
- *barreiras de acesso, entre outros*

- **ANUAL (desde 2005) e NACIONAL**
- **Comparabilidade internacional (modelo Eurostat/OECD)**
- **Entrevistas presenciais (domiciliar) e por telefone (empresas)**

➢ **Disponíveis em www.cetic.br**

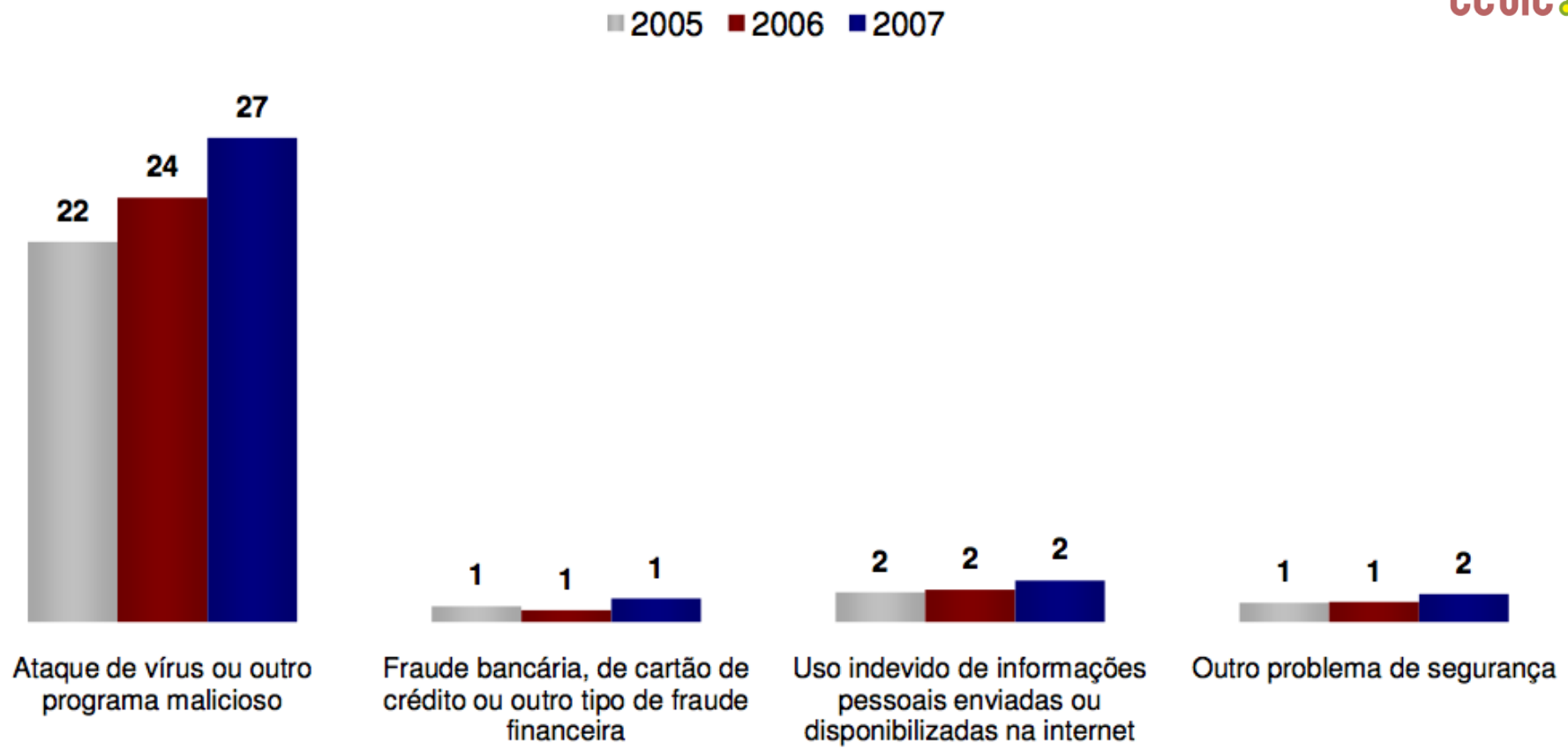


A3 - TIPO DE SISTEMA OPERACIONAL UTILIZADO - COMPUTADOR DE MESA[1]
Percentual sobre o total de domicílios com computador de mesa[2]

Percentual (%)		Computador de mesa				
		Microsoft/Windows	Linux	Macintosh	Outros	Não sabe
Total		85,45	1,45	0,22	1,14	11,73
REGIÕES DO PAÍS	NORTE/NORDESTE	90,04	2,15	-	0,43	7,38
	SUDESTE	82,25	1,14	0,32	1,33	14,96
	SUL	92,40	1,25	-	1,06	5,29
	CENTRO-OESTE	82,75	1,86	0,40	0,40	14,59
CLASSE SOCIAL[3]	A	95,49	0,18	-	-	4,33
	B	86,77	1,24	0,20	1,05	10,74
	C	84,68	1,95	0,31	1,32	11,74
	DE	70,71	1,14	-	1,78	26,36

Domicílios: Problemas de Segurança Encontrados

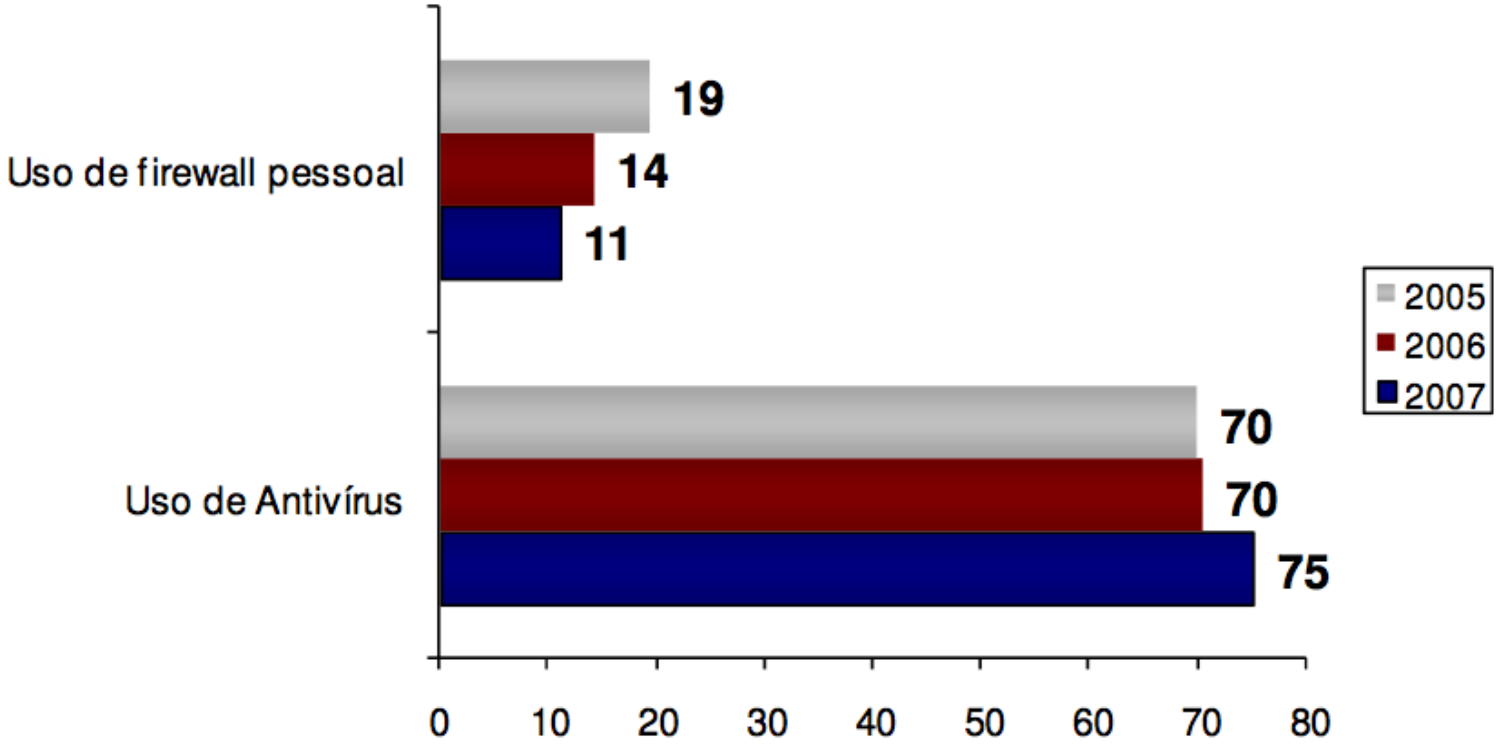
Percentual sobre o total de usuários de Internet



Base 2005: 2.085 entrevistados que usaram internet nos últimos três meses.
Base 2006: 2.924 entrevistados que usaram internet nos últimos três meses.
Base 2007: 5.823 entrevistados que usaram internet nos últimos três meses

Domicílios: Medidas de Segurança Adotadas

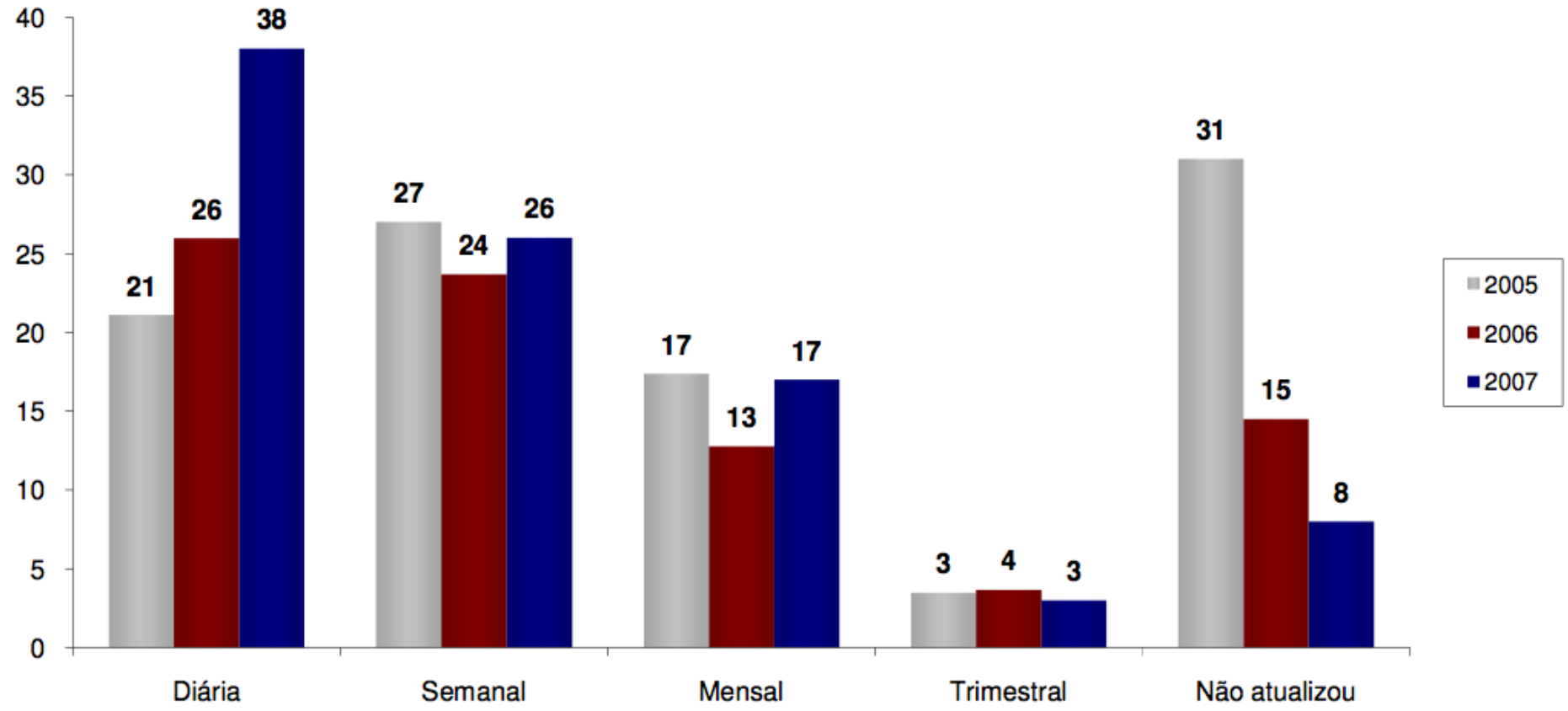
Percentual sobre o total de usuários de Internet que possuem computador



Base 2005: 1.020 entrevistados que usaram internet nos últimos três meses e possuem computador no seu domicílio.
Base 2006: 1.444 entrevistados que usaram internet nos últimos três meses e possuem computador no seu domicílio.
Base 2007: 2.808 entrevistados que usaram a internet nos últimos três meses e possuem computadores no seu domicílio.

Domicílios: Freqüência de Atualização do Antivírus

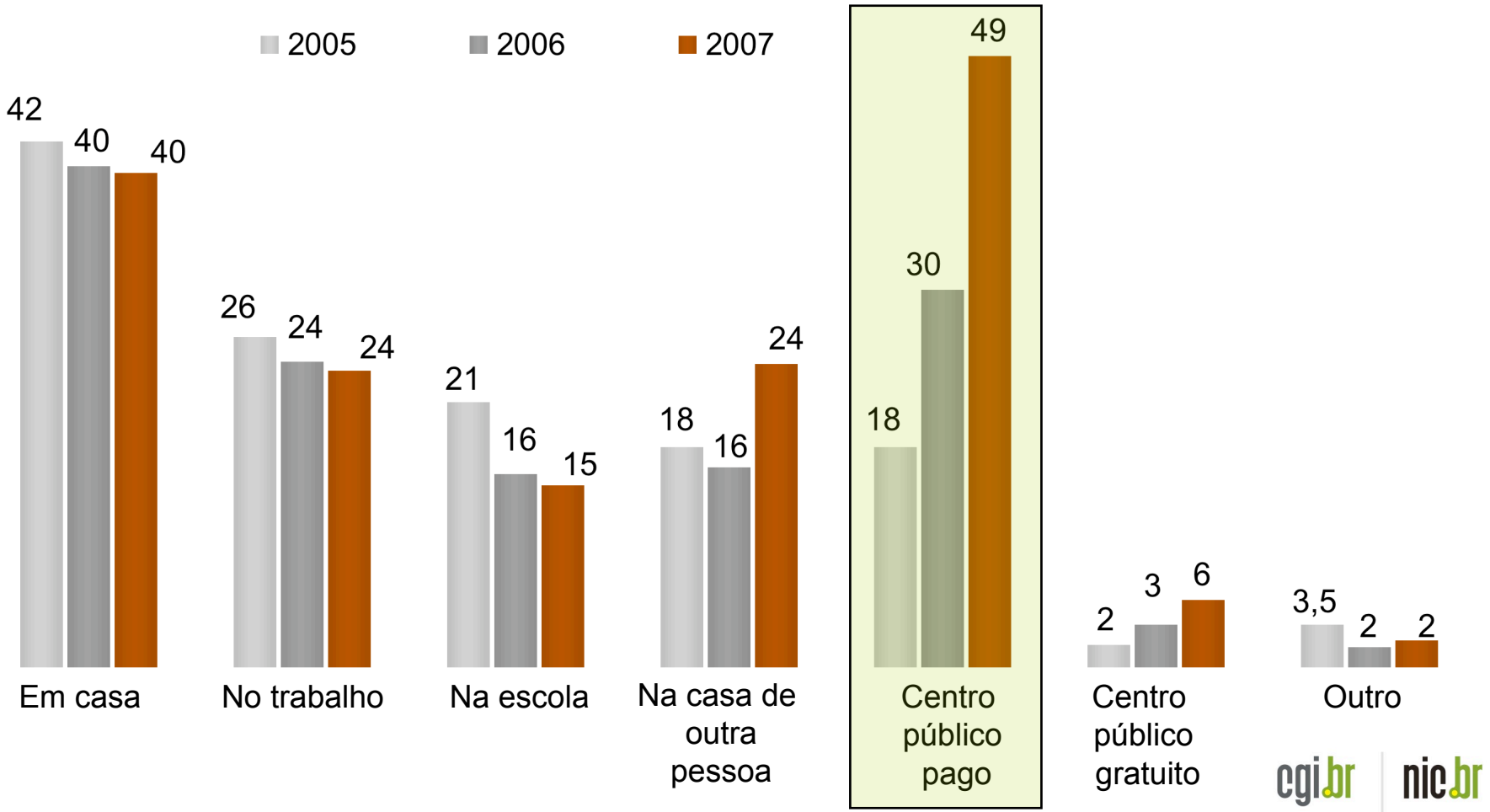
Percentual sobre o total de usuários de Internet que possuem computador e utilizaram antivírus



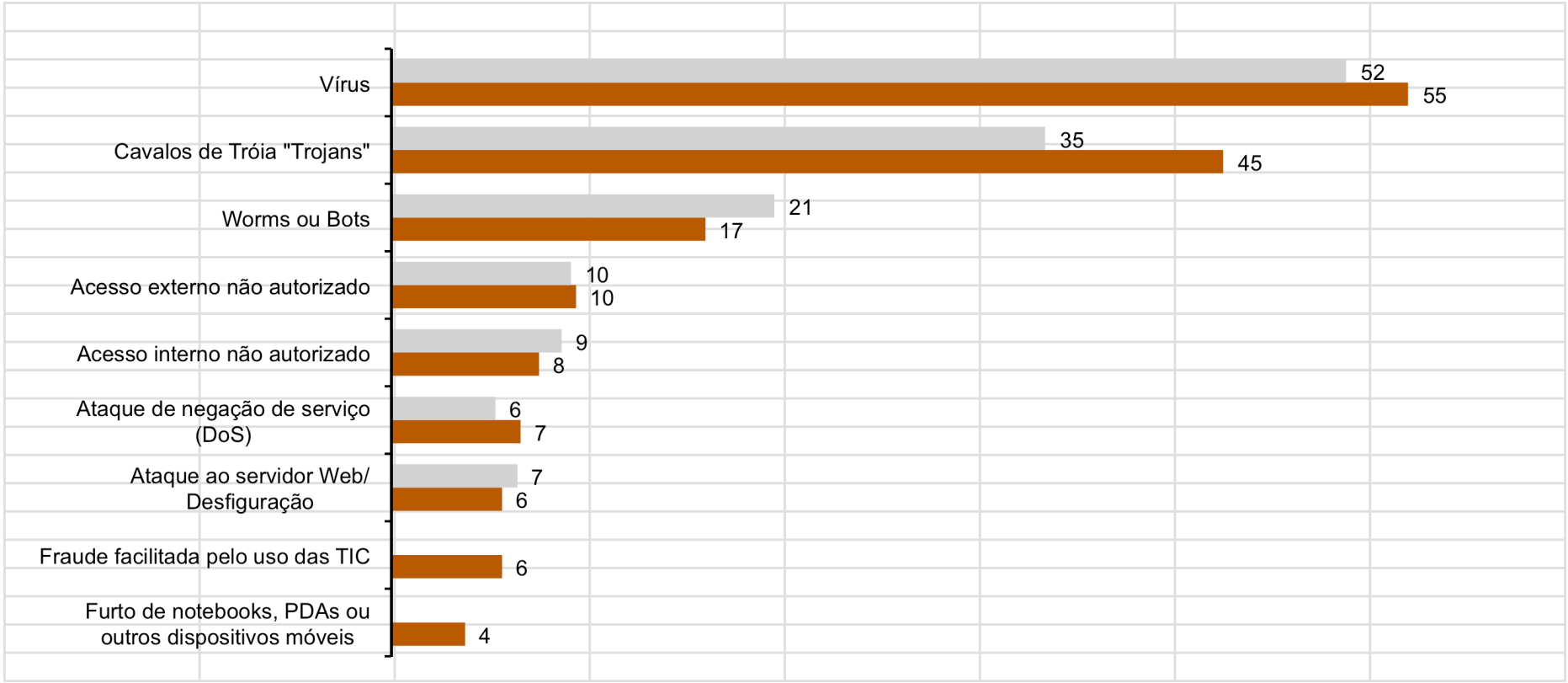
Base 2005: 1.020 entrevistados que usaram internet nos últimos três meses que possuem computador no domicílio e utilizaram antivírus.
Base 2006: 1.444 entrevistados que usaram internet nos últimos três meses que possuem computador no domicílio e utilizaram antivírus.
Base: 2007: 2.808 entrevistados que usaram internet nos últimos três meses que possuem computador no domicílio e utilizaram antivírus.

Domicílios: Local de Acesso à Internet

Percentual sobre o total de usuários de Internet



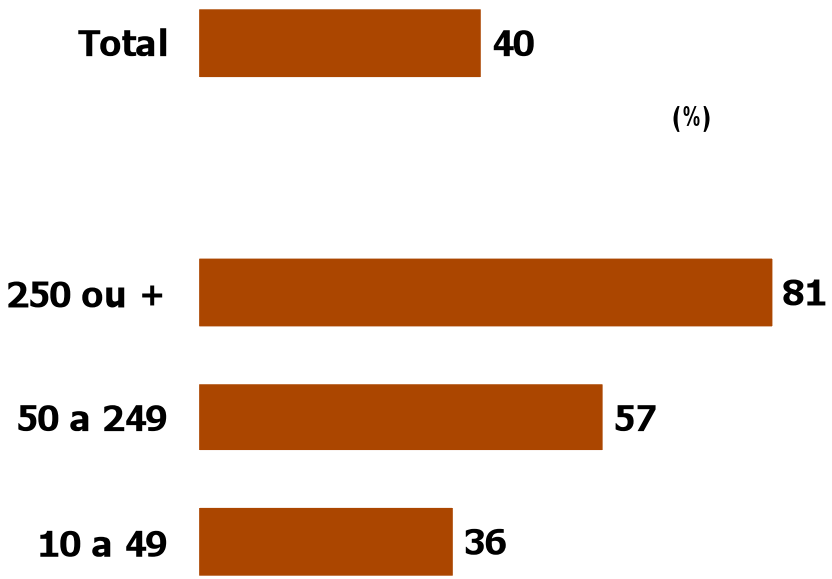
Empresas: Problemas de Segurança Identificados



Base 2006: 2.437 empresas com acesso à internet, com 10 funcionários ou mais, que constituem os seguintes segmentos da CNAE: seção D, F, G, I, K e grupos 55.1, 55.2, 92.1 e 92.2.

Base 2007: 2110 empresas, com acesso à internet, com 10 ou mais funcionários, que constituem os seguintes segmentos da CNAE 1.0: seção D, F, G, H, I, K e seção O sem divisões 90 e 91.

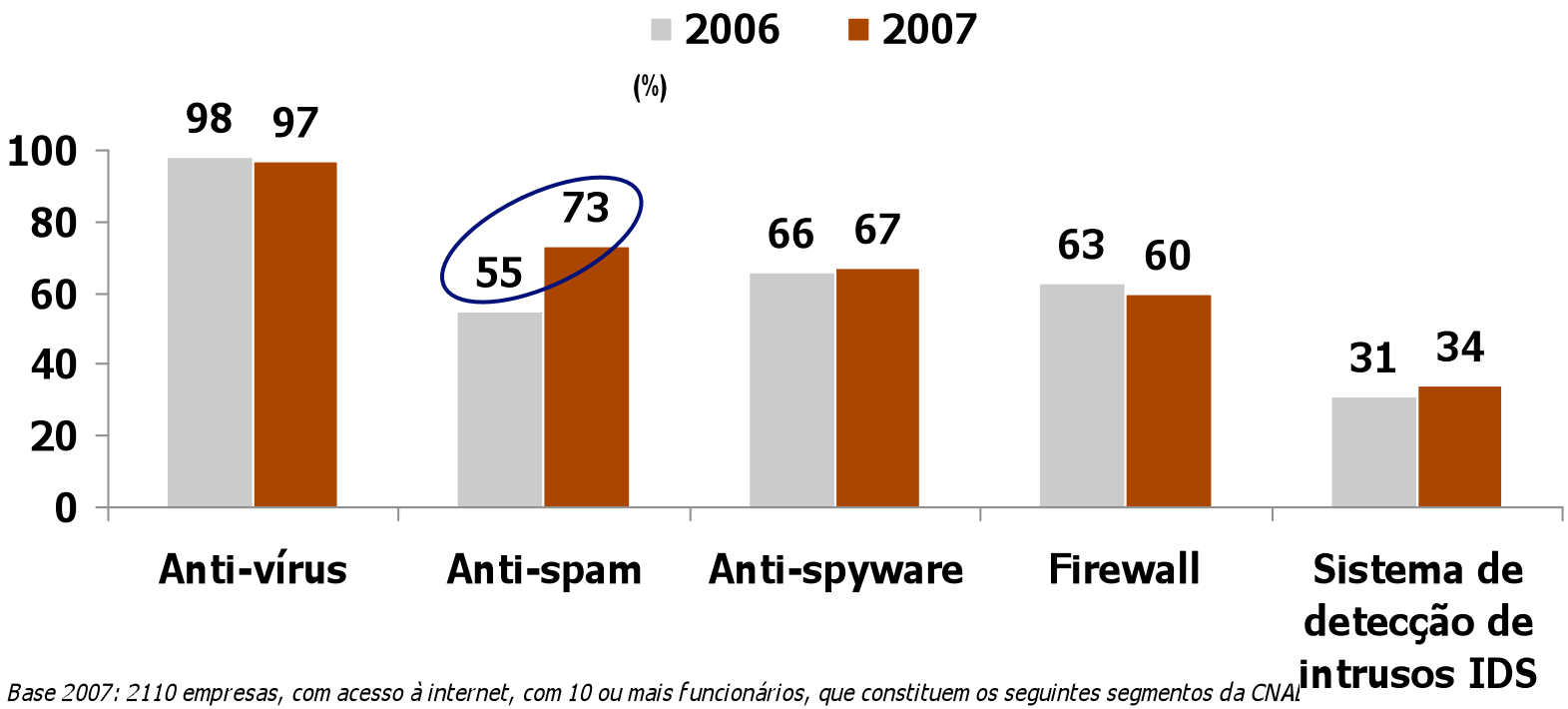
Empresas: Política de Segurança ou de Uso Aceitável



Base 2007: 2110 empresas com acesso à internet, com 10 ou mais funcionários, que constituem os seguintes segmentos da CNAE 1.0: seção D, F, G, H, I, K e seção O sem divisões 90 e 91.

Percentual de empresas com política de segurança aumenta de acordo com o porte: 81% nas que têm a partir de 250 funcionários

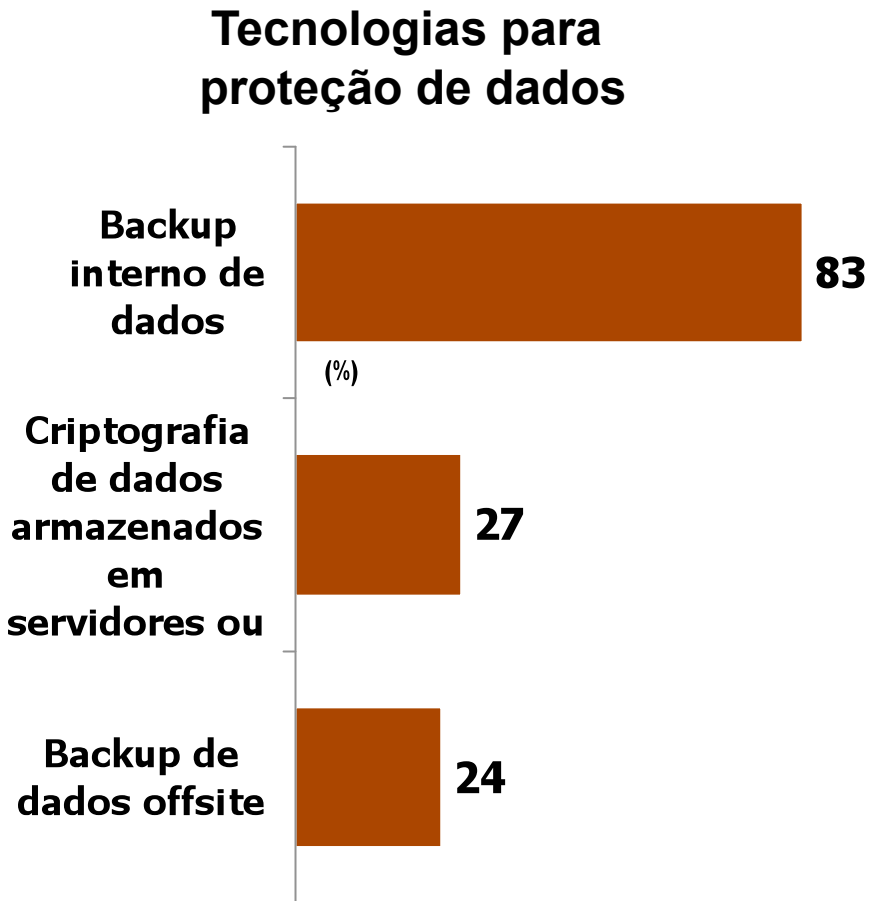
Empresas: Tecnologias de segurança adotadas

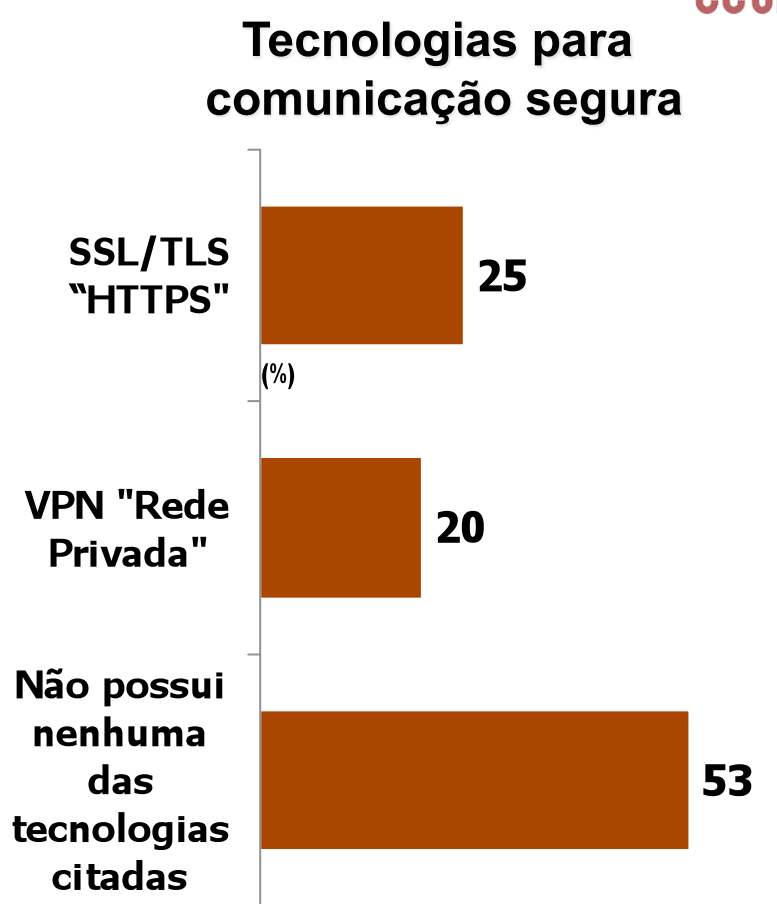


Base 2007: 2110 empresas, com acesso à internet, com 10 ou mais funcionários, que constituem os seguintes segmentos da CNAE 1.0: seção D, F, G, H, I, K e seção O sem divisões 90 e 91.

Uso das tecnologias de segurança se mantém constante à exceção do Anti-spam que cresceu 18 p.p.

Empresas: Tecnologias Adotadas





Base 2007: 2110 empresas com acesso à internet, com 10 ou mais funcionários, que constituem os seguintes segmentos da CNAE 1.0: seção D, F, G, H, I, K e seção O sem divisões 90 e 91.

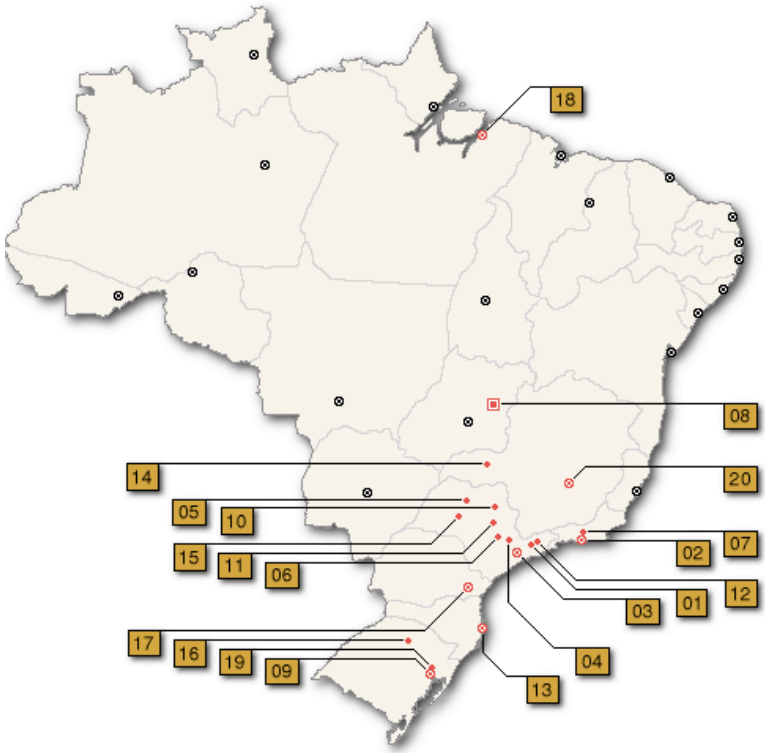
Análise de Tendências e *Early Warning*

Consórcio Brasileiro de *Honeypots*

Projeto *Honeypots* Distribuídos

Objetivo: aumentar a capacidade de detecção de incidentes, correlação de eventos e determinação de tendências de ataques no espaço Internet brasileiro

- **37 instituições, entre academia, governo, indústria e instituições financeiras**
- **Baseado em trabalho voluntário**
- **http://www.honeypots-alliance.org.br/**

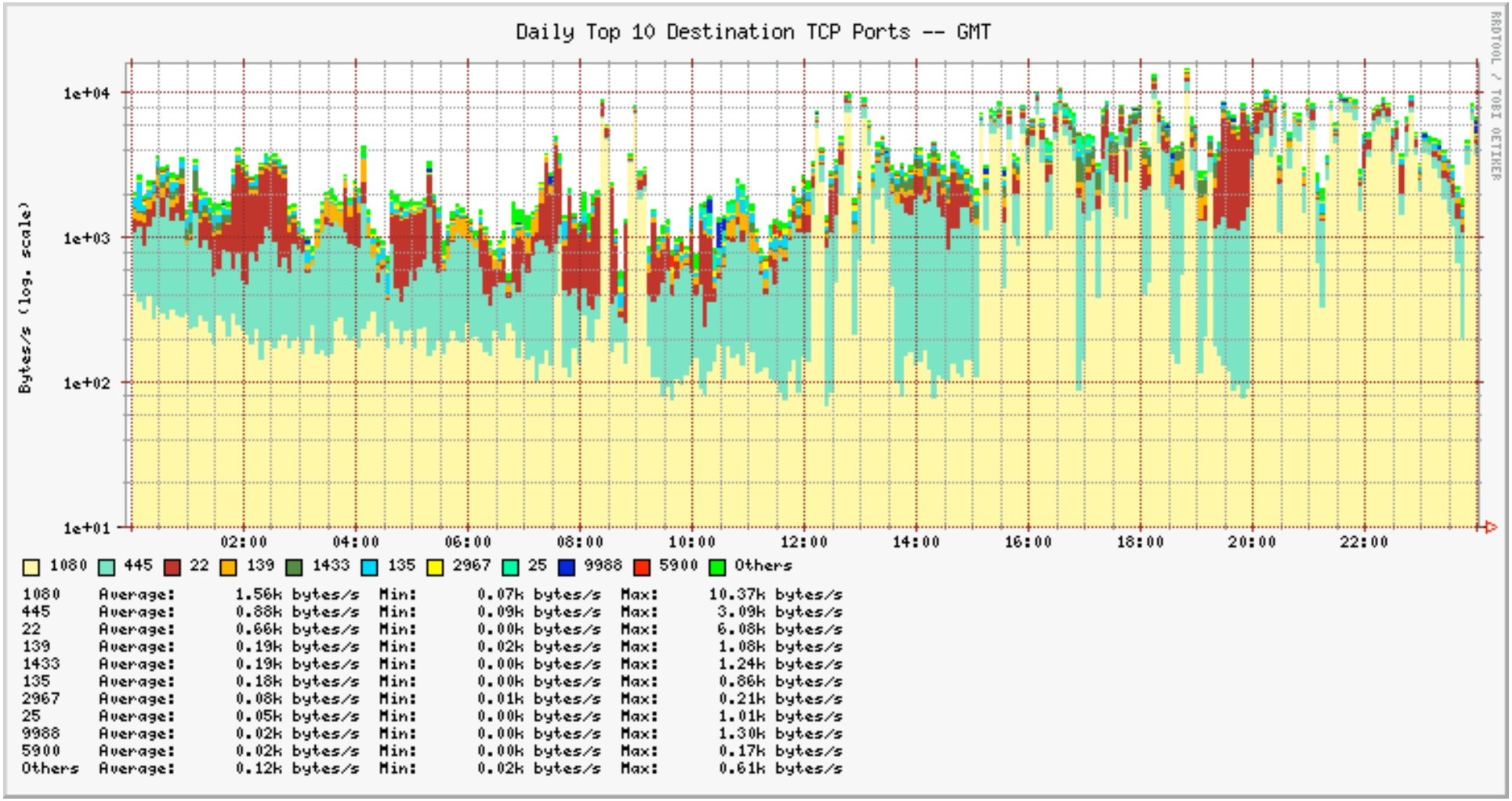


Utilização dos dados coletados para:

- **Notificação das redes originadoras dos ataques**
- **Geração de estatísticas públicas**

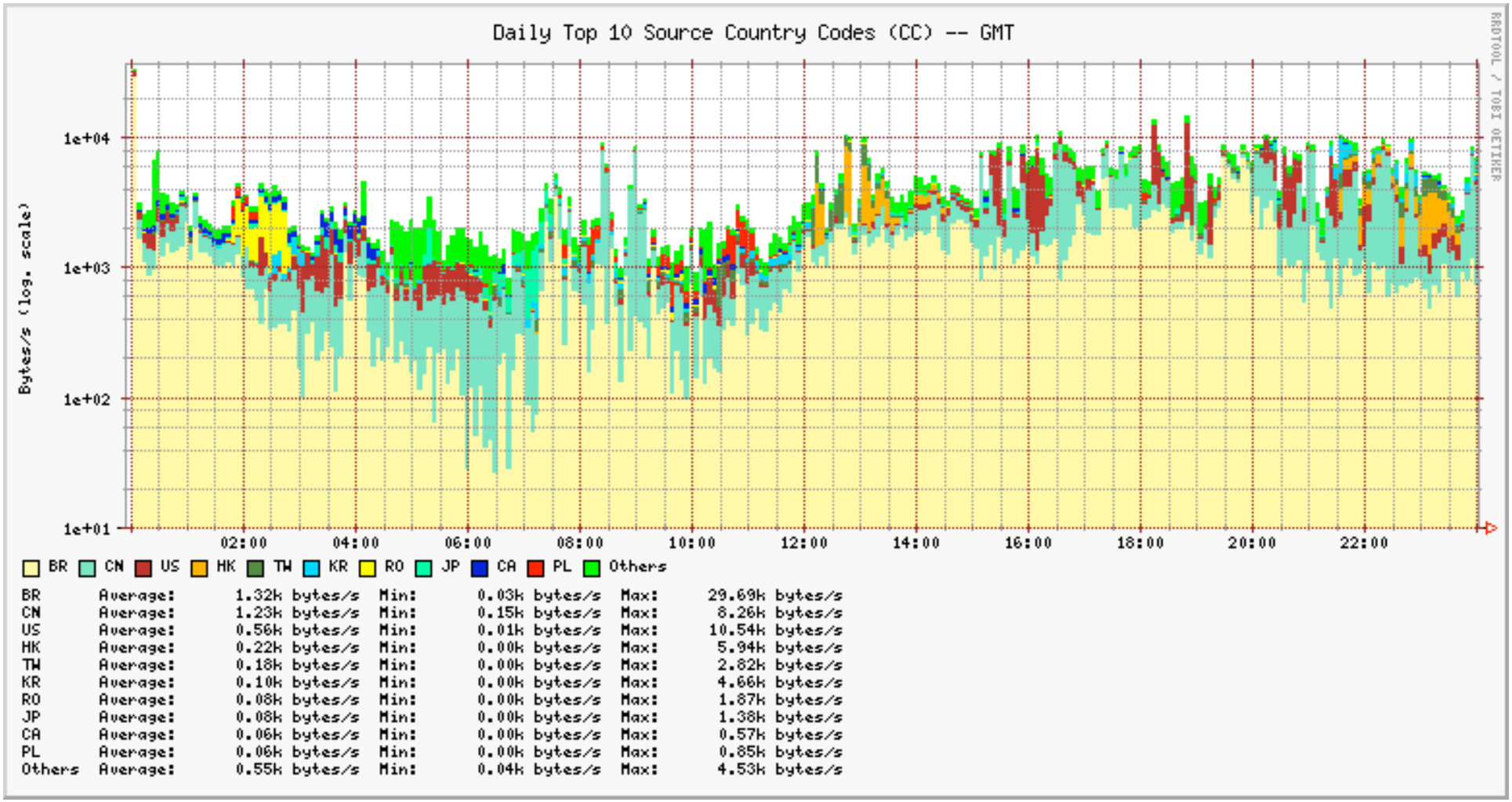
Estatísticas Públicas dos Ataques Registrados (1/2)

Portas TCP mais procuradas – 27/05/2008



Estatísticas Públicas dos Ataques Registrados (2/2)

Países de origem do tráfego – 27/05/2008

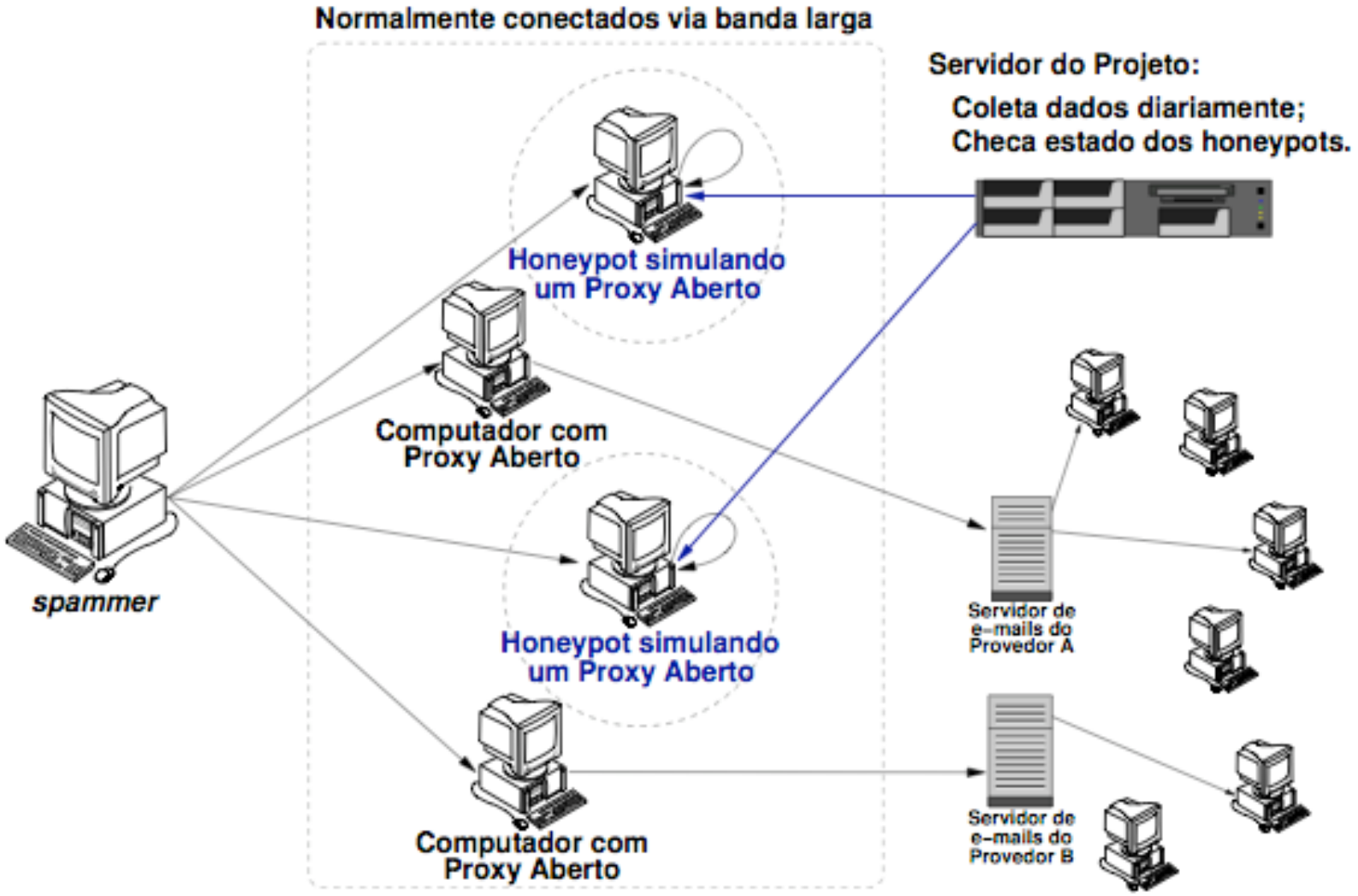


O Projeto SpamPots

- **Implementado pelo CERT.br**
- **Financiado pelo NIC.br/CGI.br**
  - **Como parte dos trabalhos da Comissão Anti-Spam**
  - **Para gerar métricas sobre o abuso de máquinas de usuários finais para o envio de *spam***
- **Implantação de 10 *honeypots** de baixa-interatividade, simulando ser *proxies* abertos e capturando *spam***
  - **Em 5 operadoras de banda-larga**
    - **2 cabo e 3 ADSL**
    - **1 residencial e 1 empresarial em cada**

* *Honeypot* é um tipo de sensor usado para simular serviços e registrar as atividades maliciosas.
Fonte: http://www.cert.br/docs/whitepapers/honeypots-honeynets/

Localização dos Sensores



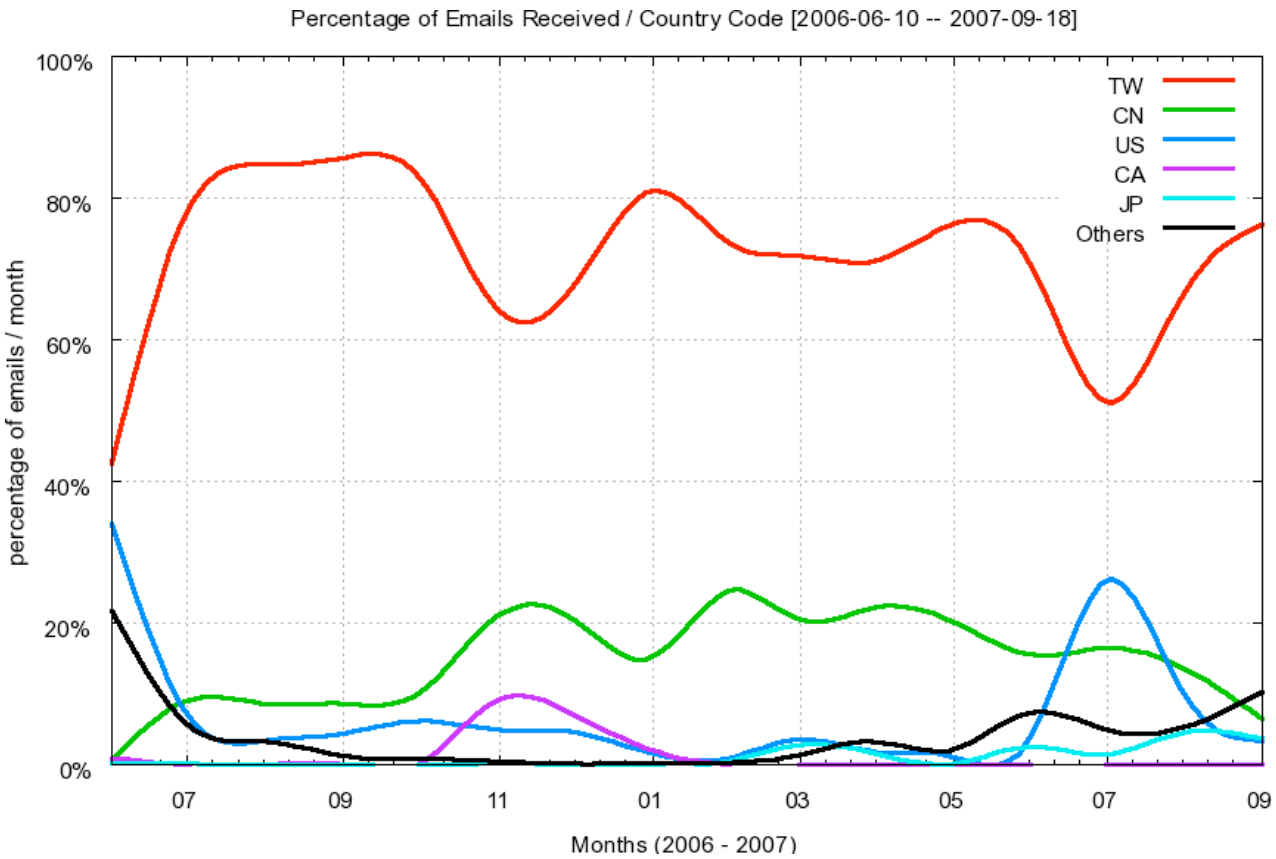
Dados Totais Coletados pelos 10 sensores

Período: 10 de junho de 2006 a 18 de setembro de 2007
Dias: 466

E-mails capturados:	**524.585.779**
Potenciais Destinatários:	**4.805.521.964**
Média de destinatários/e-mail:	**≈ 9.1**
Média de emails/dia:	**≈ 1.2 Milhões**
IPs únicos que conectaram nos sensores:	**216.888**
***Autonomous Systems* (AS) únicos:**	**3.006**
Códigos de País (CCs) únicos:	**165**

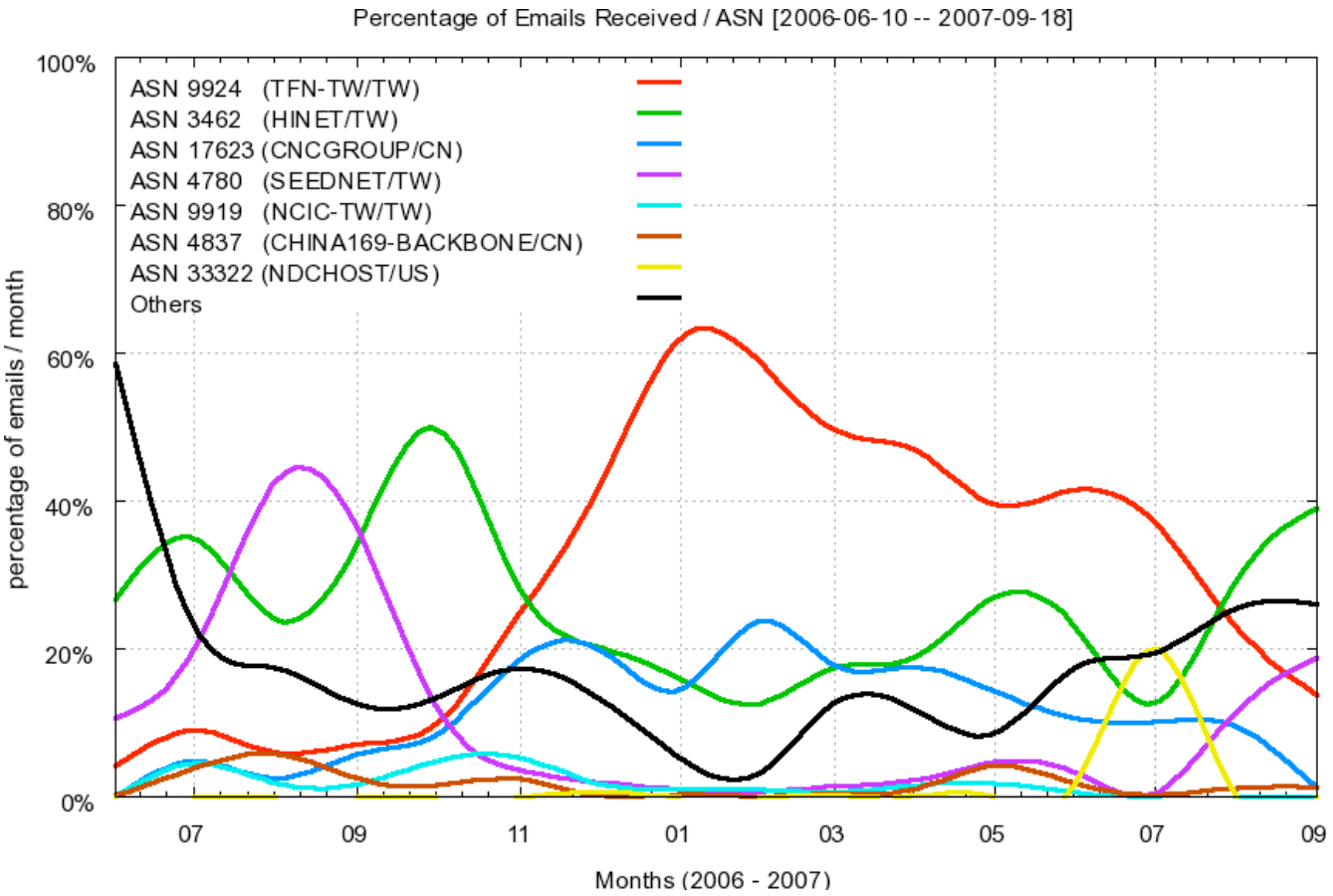
Países que Injetaram Mais *Spams*

#	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
		Sub-total:	99.50



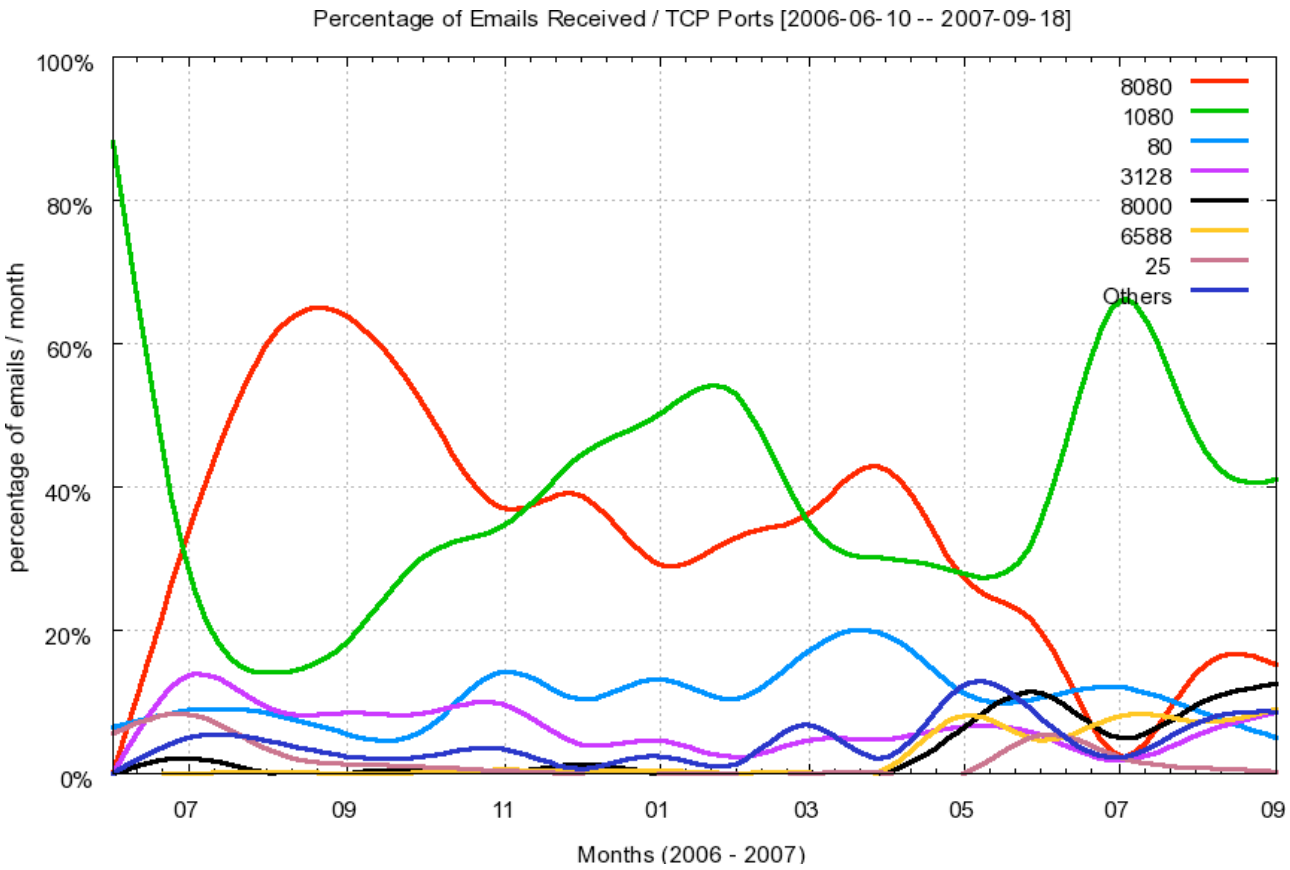
Autonomous Systems que Injetaram Mais Spams

#	Nome do 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
	Sub-Total:		89.26



Portas e Serviços Mais Abusados

#	Porta	Protocolo	Serviço	%
01	1080	SOCKS	socks	37.31
02	8080	HTTP	http	34.79
03	80	HTTP	http	10.92
04	3128	HTTP	Squid	6.17
05	8000	HTTP	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	1.00
10	3382	HTTP	Sobig.f	0.96
11	81	HTTP	http	0.96



Considerações Finais

- **Cenário atual**
  - ***Softwares* com muitas vulnerabilidades**
  - **Pressão econômica para lançar, mesmo com problemas**
- **Só haverá melhorias quando**
  - **O processo de desenvolvimento de *software* incluir**
    - **Levantamento de requisitos de segurança**
    - **Testes que incluam casos de abuso (e não somente casos de uso)**
  - ***Secure Software Development* se tornar parte da formação de projetistas e programadores**
  - **Provedores e operadoras forem mais pró-ativos**

Links Relacionados

- CGI.br - Comitê Gestor da Internet no Brasil
  http://www.cgi.br/
- NIC.br - Núcleo de Informação e Coordenação do Ponto br
  http://www.nic.br/
- CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
  http://www.cert.br/
- Mais sobre o Projeto SpamPots
  http://www.cert.br/docs/whitepapers/spampots/