Estado da Segurança da Internet no Brasil e sua Inserção no Panorama Nacional e Internacional de Governança da Internet

Cristine Hoepers

cristine@cert.br

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
Núcleo de Informação e Coordenação do Ponto BR
Comitê Gestor da Internet no Brasil

Agenda

- Contextualização: Governança da Internet no Brasil
- Quais são os problemas
  - Indicadores
  - Mitos
- O que está sendo feito
- Desafios

Governança da Internet no Brasil

Comitê Gestor da Internet no Brasil – CGI.br

- 1989 – Criação e delegação do código de país (ccTLD) ".br" à FAPESP
- 1991 – Primeira conexão TCP/IP brasileira, realizada entre a FAPESP e a *ESNet*
- 1995 – Portaria Interministerial MC/MCT nº 147, de 31 de maio, cria o CGI.br
  - coordenar e integrar todas as iniciativas de serviços Internet no país, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados
- 1995 – Criação do Registro.br
- 1997 – Criação do CERT.br (à época NBSO)
- 2005 – Criação do NIC.br, entidade sem fins lucrativos para executar as diretrizes do CGI.br e prestar serviços para a estabilidade e segurança da Internet no Brasil

http://www.nic.br/imprensa/releases/2010/rl-2010-12.htm

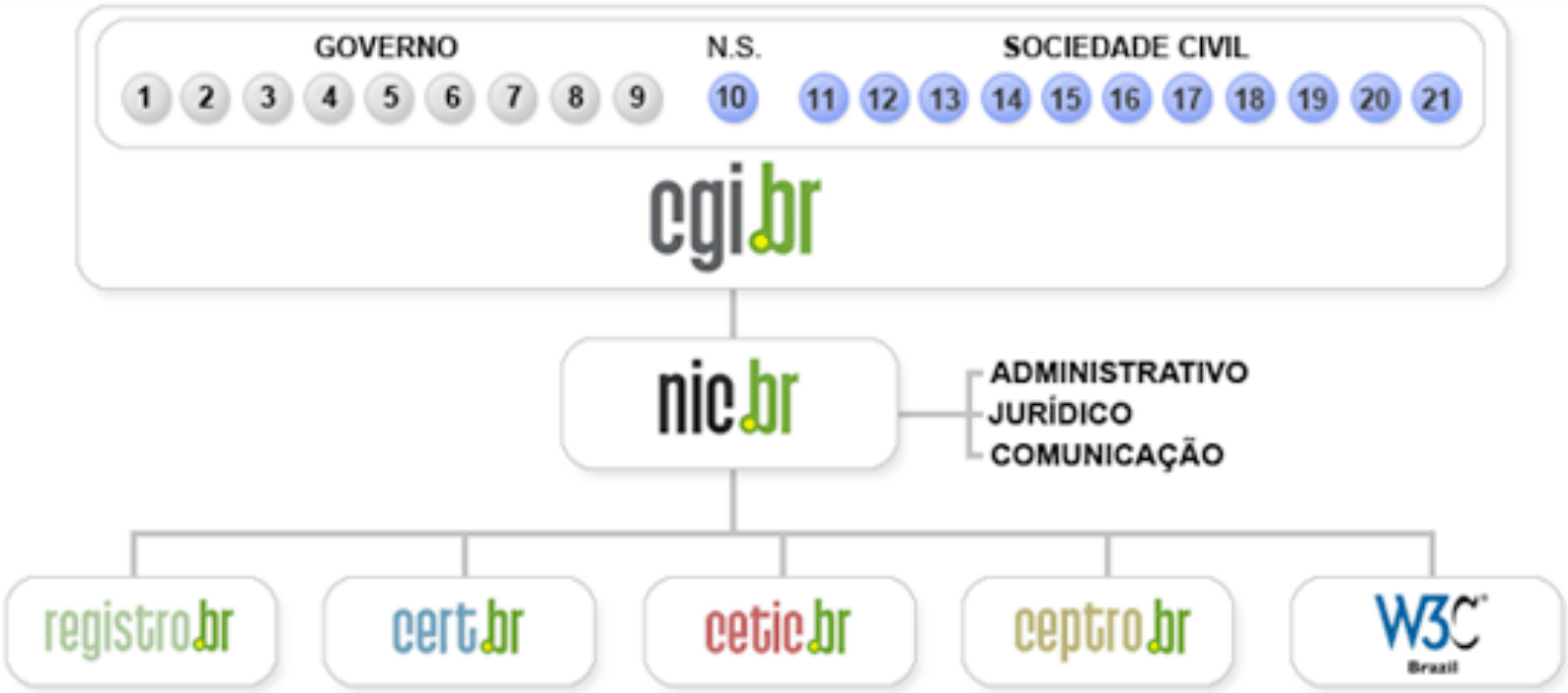
Comitê Gestor da Internet no Brasil – CGI.br

Dentre as atribuições definidas no Decreto Presidencial nº 4.829, de 03 de setembro de 2003, 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.**
- **ser representado nos fóruns técnicos nacionais e internacionais relativos à Internet;**

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 – Cons. Nacional de Desenvolvimento Científico e Tecnológico
9 – Fórum Nac. 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

Órgãos Internacionais de Governança

- **ICANN – *Internet Corporation for Assigned Names and Numbers***

  Diretor Presidente do NIC.br foi membro do Board por 2 mandatos
  - **GAC – *Governmental Advisory Committee***

    Representação conjunta com o MRE
  - **ccNSO – *Country Code Names Supporting Organisation***
  - **SSAC – *Security and Stability Advisory Committee***

    Diretor de Tecnologia do NIC.br é membro do Conselho
  - **ASO – *Address Supporting Organization***

    Diretor Executivo do CGI.br é membro representando a região da América Latina
- **IANA – Internet Assigned Numbers Authority**
  - Coordena os Servidores raiz DNS e a alocação de blocos de endereçamento IPv4 e IPv6
- **LACNIC – Registro de Endereços da Internet para a América Latina e o Caribe**
  - Diretor Executivo do CGI.br é membro da diretoria
- **IGF – *Internet Governance Forum* –** participação em todas as áreas
- **IETF – Internet Engineering Task Force**
  - **Padroniza e define todos os padrões e protocolos Internet**

CERT.br

Treinamento e Conscientização

- Cursos
- Palestras
- Documentação
- Reuniões

Tratamento de Incidents

- Articulação
- Apoio à recuperação
- Estatísticas

Análise de Tendências

- *Honeypots* Distribuídos
- SpamPots

SEIPartner CERT Courses

FIRST Improving Security Together MEMBER

APWG RESEARCH PARTNER www.antiphishing.org

The Honeynet PROJECT®

Criado em 1997 para:

- Ser um ponto de contato nacional para notificação de incidentes de segurança
- Prover a coordenação e o apoio necessários no processo de resposta a incidentes
- Estabelecer um trabalho colaborativo com outras entidades, como os operadores da justiça, provedores de acesso e serviços e backbones
- Auxiliar novos CSIRTs a estabelecerem suas atividades
- Aumentar a conscientização sobre a necessidade de segurança na Internet

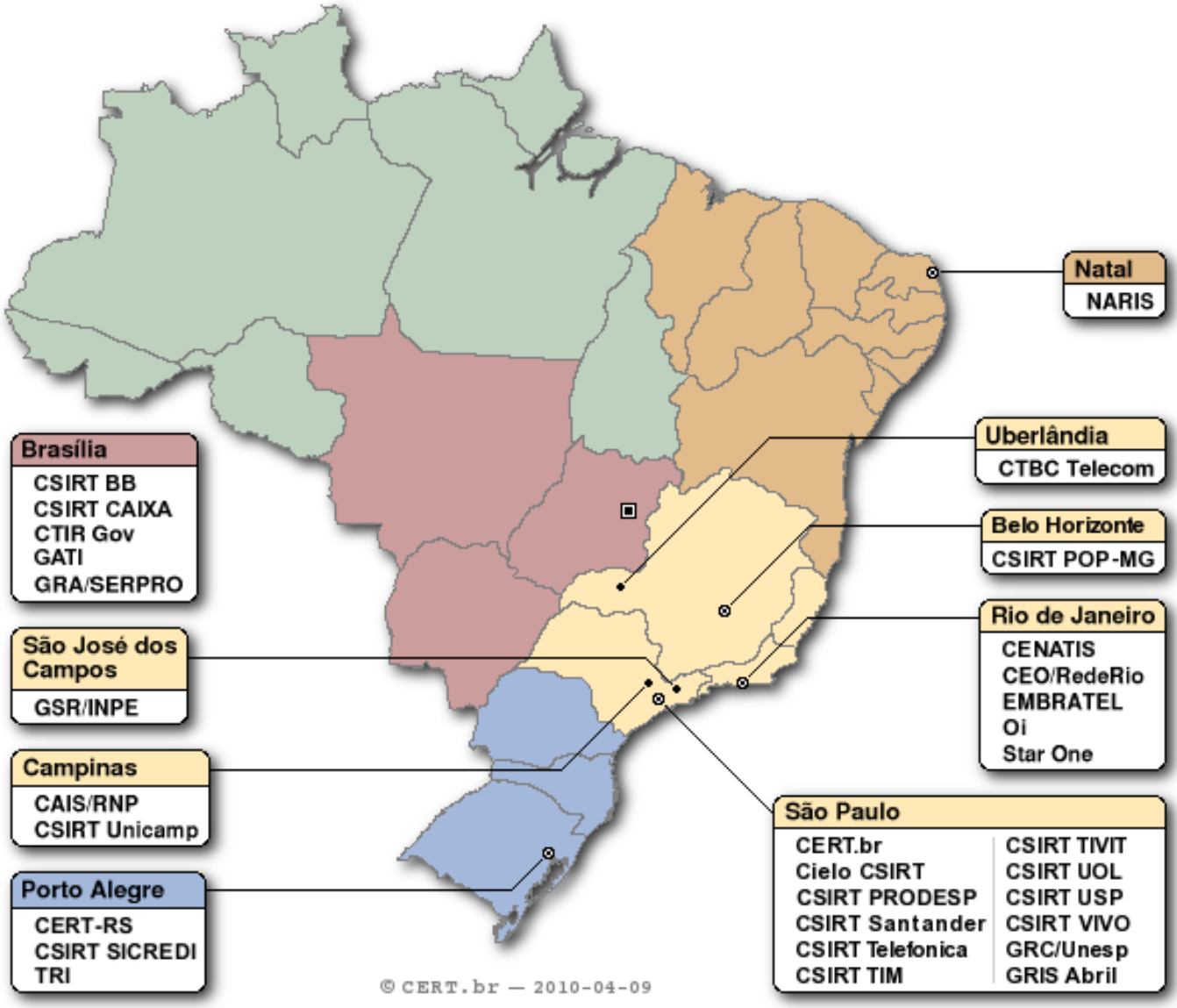
Evolução do Tratamento de Incidentes no Brasil

- 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 (à época 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 no Brasil

Público Alvo	CSIRTs
Qualquer rede no Brasil	CERT.br
Redes de Governo	CTIR Gov, GATI, GRA/SERPRO, CSIRT PRODESP
Setor Financeiro	CSIRT BB, CSIRT CAIXA, CSIRT Sicredi, CSIRT Santander, Cielo CSIRT
Telecom/ISP	CTBC Telecom, EMBRATEL, StarOne, Oi, CSIRT Telefonica, CSIRT TIM, CSIRT UOL, CSIRT VIVO
Redes Acadêmicas e de Pesquisa	GSR/INPE, CAIS/RNP, CSIRT Unicamp, CERT-RS, NARIS, CSIRT POP-MG, CENATIS, CEO/RedeRio, CSIRT USP, GRC/Unesp, TRI
Outros	CSIRT TIVIT, GRIS Abril



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

Indicadores, Problemas e Mitos sobre Segurança na Internet

Ataques mais Freqüentes em 2009

- Contra usuários finais
  - fraudes, *phishing*, *bots*, *spyware*, etc
  - motivação financeira
  - abuso de *proxies*, na maioria instalados por *bots*
- De força bruta contra serviços de rede
  - SSH, FTP, Telnet, VNC, etc
- Não tão freqüentes, mas com grande impacto por serem contra a infra-estrutura crítica da Internet
  - ataques contra servidores DNS
  - contra protocolos de roteamento como o BGP
- Com rápido crescimento nos últimos meses
  - ataques a aplicações Web vulneráveis

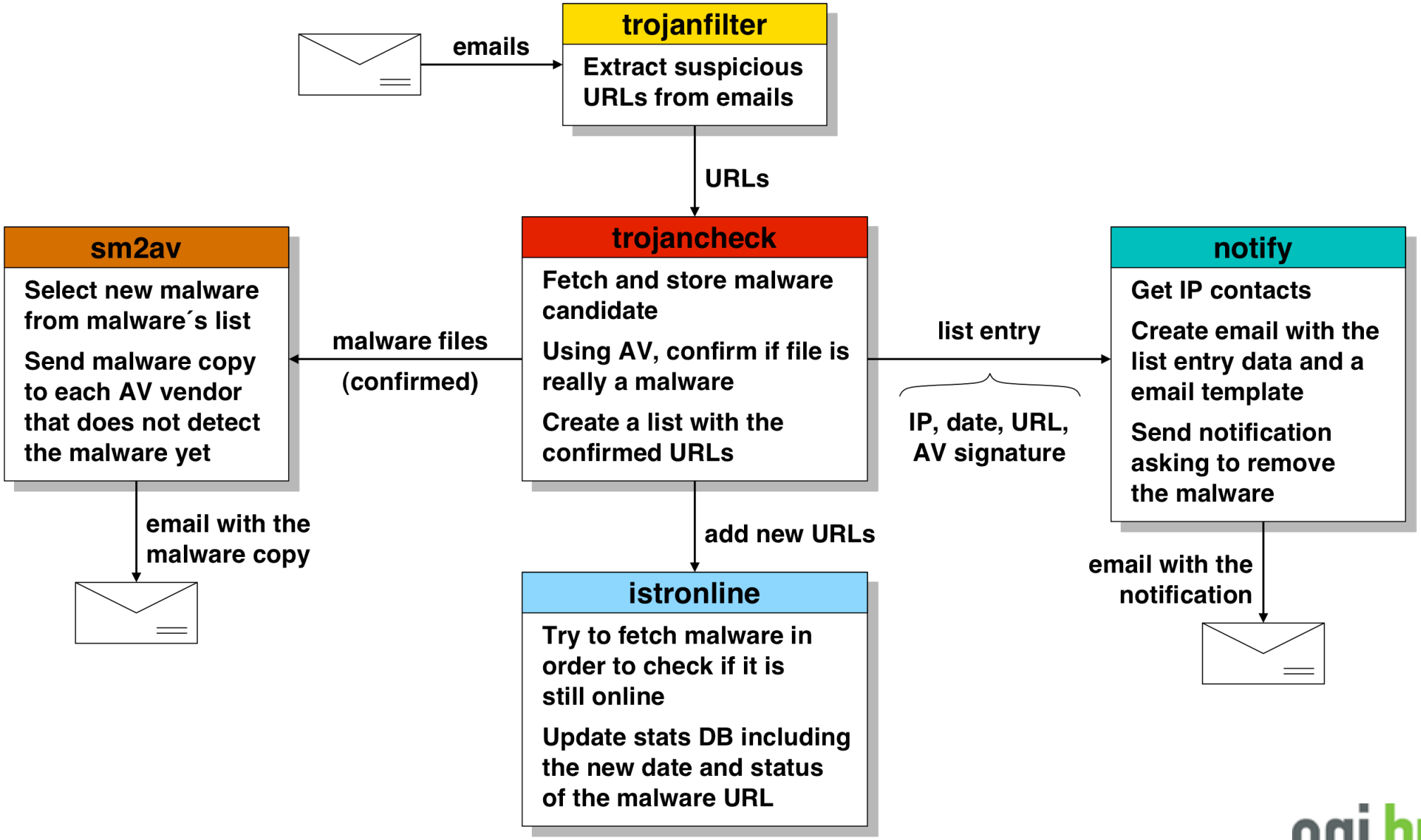
Ataques a Usuários Finais

- Fruto da mudança no enfoque dos atacantes
  - Por que atacar um servidor protegido se é mais fácil e "rentável" atacar um usuário?
- fraudes, *phishings*, *bots*, *spyware*, *crimeware,* etc
- Motivação financeira

Características das tentativas de fraude mais notificadas ao CERT.br:

- Eventuais violações de direitos autorais
- Fraude com objetivos financeiros
  - majoritariamente envolve *spams*
    - em nome das mais variadas instituições e com tópicos diversos
    - com *links* (URLs) para códigos maliciosos (cavalos de tróia)
  - páginas falsas estão voltando a ter números significativos
  - *drive-by downloads* sendo usados intensamente no Brasil
    - casos publicados na mídia em 2009 incluem: *sites* principais da Vivo, da Oi e da Ambev

Acompanhamento e Notificação de Códigos Maliciosos que afetam o Brasil



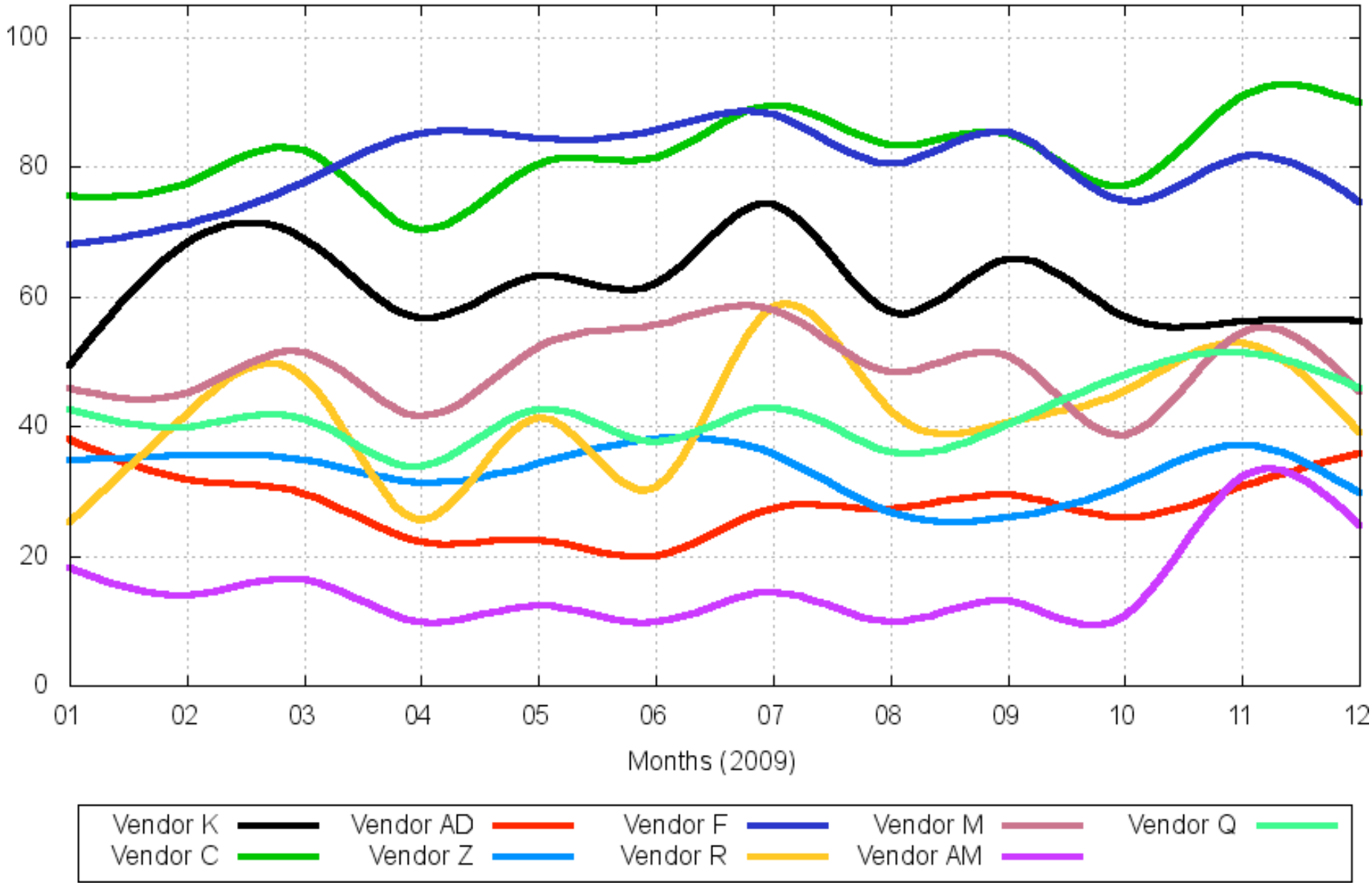
Códigos Maliciosos que Afetam Usuários do Brasil

	2006	2007	2008	2009	2010
URLs únicas	25.087	19.981	17.376	10.864	2.798
Exemplares únicos	19.148	16.946	14.256	8.151	1.870
Antivírus: Assinaturas únicas	1.988	3.032	6.085	4.101	1.387
Antivírus: Famílias de assinaturas	140	109	63	93	51
Extenões de arquivos	73	112	112	100	46
Domínios envolvidos na hospedagem	5.587	7.795	5.916	4.447	1.311
Endereços IP	3.859	4.415	3.921	3.233	996
Códigos de País	75	83	78	76	53
Notificações enviadas pelo CERT.br	18.839	17.483	15.499	9.935	2.236

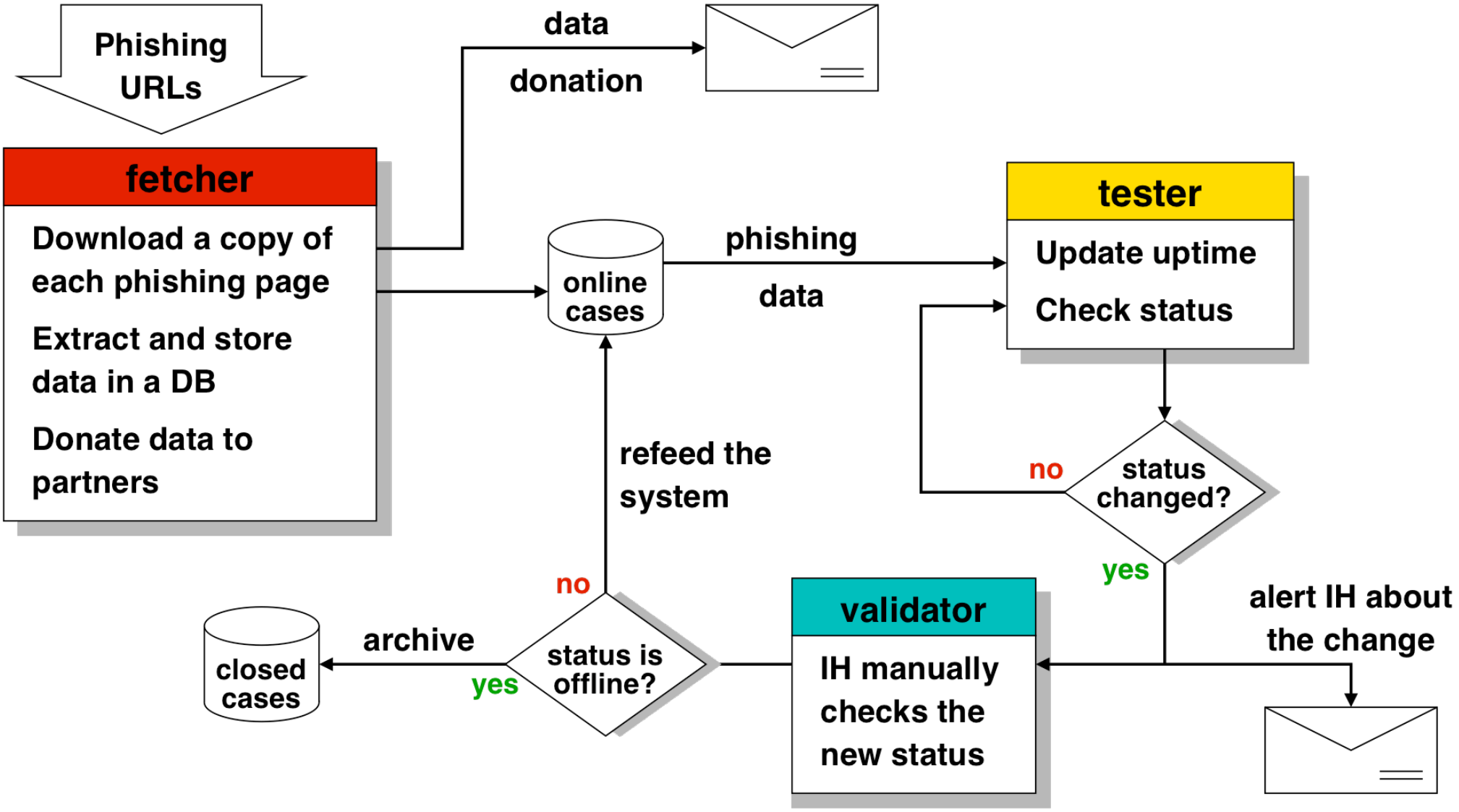
As estatísticas:

- **Incluem** *keyloggers*, *screenloggers*, *trojan downloaders*
- **Não inlcuem** *worms*, *bots* e *botnets*

Eficiência dos *Softwares* Antivírus



Acompanhamento e Notificação de Páginas Falsas (*Phishings*) que afetam ou estão hospedadas no Brasil



Casos de *Phishing* e Tempo *Online*

2009-03-23 – 2009-12-31:	
Número de casos	3.332
Bancos do Brasil	1.916
Outras Instituições	1.416
URLs únicas	3.215
Domínios	1.619
Endereços IP	1.344
Tempo online:	
≤ 15 min.	24
≤ 1 hora	324
≤ 6 horas	765
≤ 12 horas	259
≤ 1 dia	361
≤ 1 semana	1.100
> 1 semana	499
Média:	4d 07h 12m
Máximo:	218d 05h 26m

2010-01-01 – 2010-04-30:	
Número de casos	1.968
Bancos do Brasil	1.412
Outras Instituições	556
URLs únicas	1.933
Domínios	1.343
Endereços IP	1.182
Tempo online:	
≤ 15 min.	12
≤ 1 hora	237
≤ 6 horas	442
≤ 12 horas	129
≤ 1 dia	215
≤ 1 semana	594
> 1 semana	339
Média:	4d 15h 06m
Máximo:	119d 23h 59m

Casos de *Phishing* por País de Hospedagem

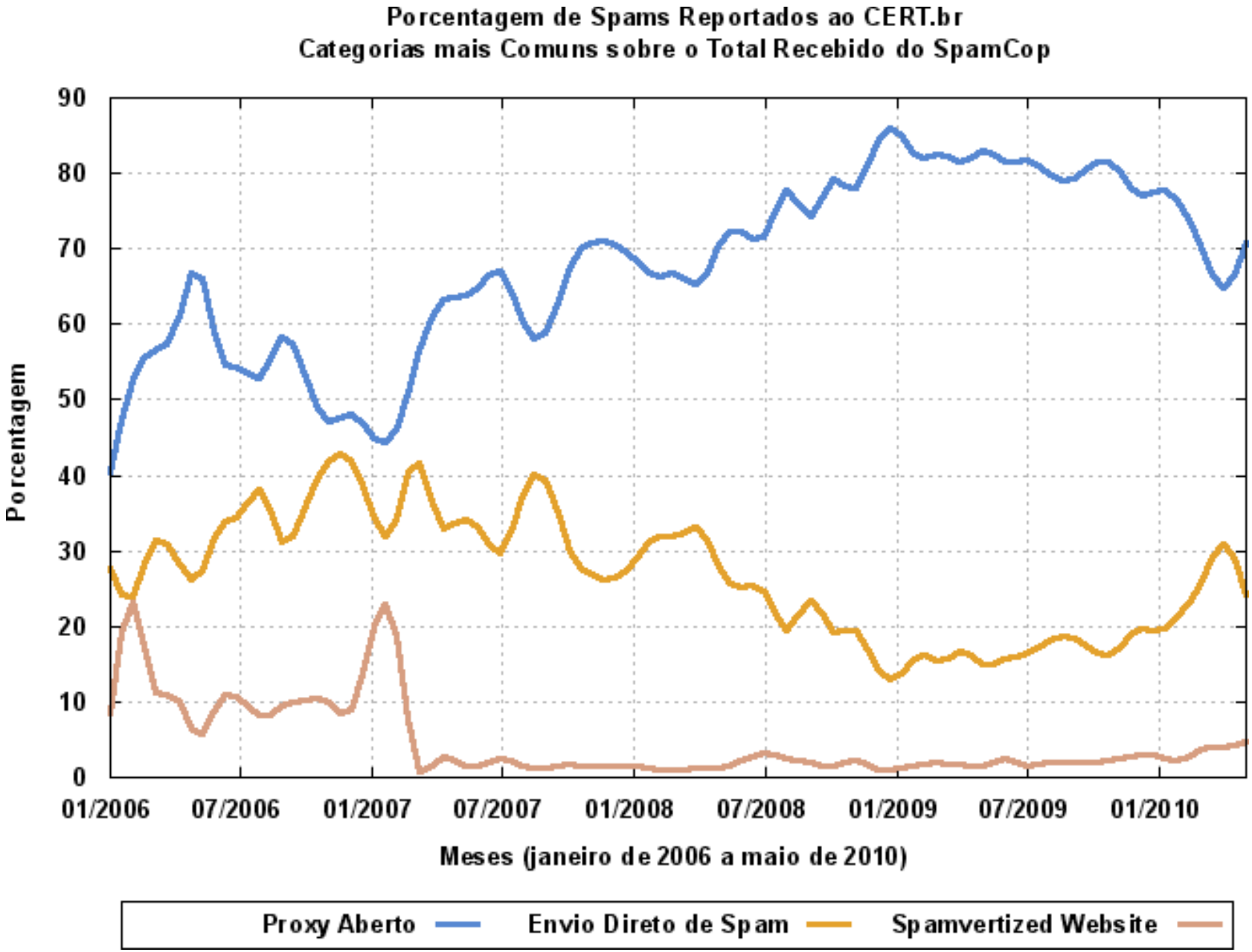
2009-03-23 – 2009-12-31

Pos.	País	Casos	%
01	Brasil	1.853	55,61
02	EUA	897	29,26
03	Alemanha	81	2,43
04	Panamá	69	2,07
05	Canadá	43	1,29
06	França	40	1,20
07	Inglaterra	39	1,17
08	China	38	1,14
09	Coréia	35	1,05
10	Austrália	26	0,78

2010-01-01 – 2010-04-30

Pos.	País	Casos	%
01	Brasil	714	36,28
02	EUA	618	31,40
03	Alemanha	97	4,93
04	Inglaterra	56	2,85
05	Itália	55	2,79
06	França	54	2,74
07	China	35	1,78
08	Holanda	32	1,63
09	Canadá	28	1,42
10	Austrália	26	1,32

Abuso de Proxies em PCs Infectados



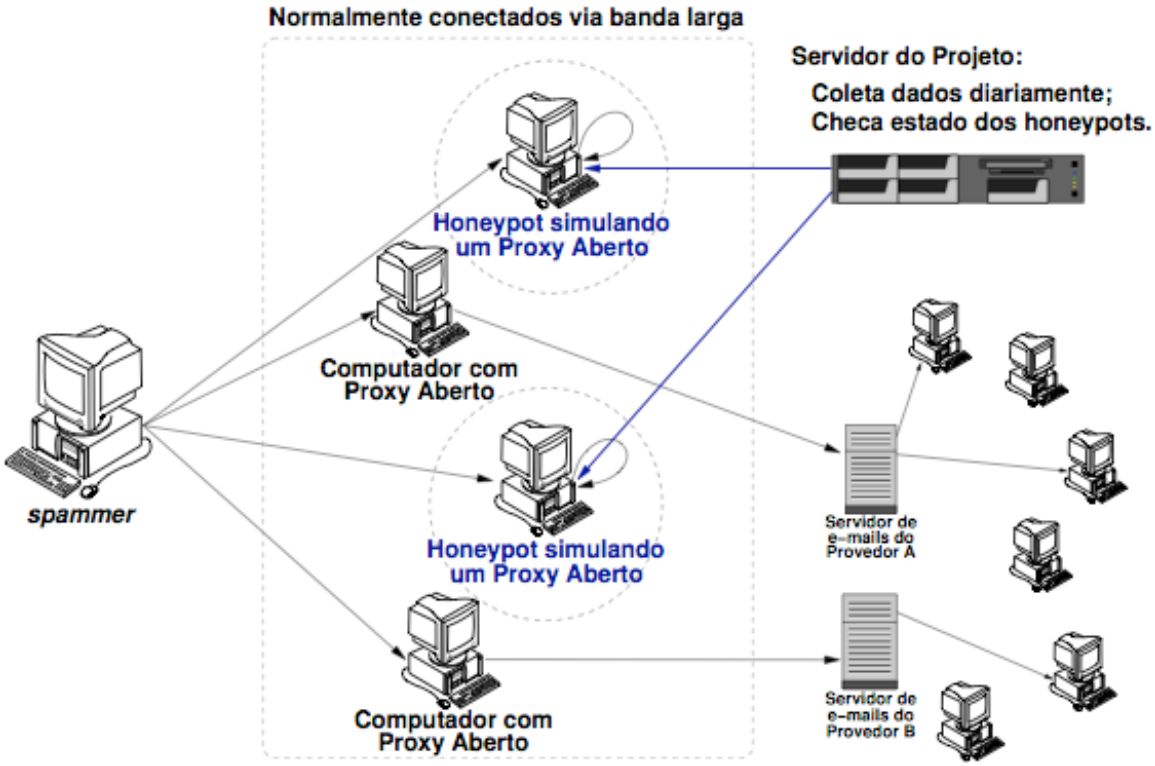
Dados do Projeto SpamPots

- **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***
  - **Incluiu financiamento da equipe de Data Mining do DCC/UFMG**
- **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/

Resultados – Abuso das Redes Brasileiras

Dias de coleta:	**466**
***E-mails* capturados:**	**524.585.779**
Destinatários:	**4.805.521.964**
Destinatários/*e-mail*:	**≈ 9.1**
***E-mails*/dia:**	**≈ 1.2 Milhões**
IPs únicos:	**216.888**
ASNs únicos:	**3.006**
***Country Codes*:**	**165**



Principais Resultados:

- **99.84% das conexões eram originadas do exterior**
- **os *spammers* consumiam toda a banda de *upload* disponível**
- **mais de 90% dos *spams* eram destinados a redes de outros países**

http://www.cert.br/docs/whitepapers/spampots/

Fase Internacional Iniciada em 2009

- **Coletando 8 milhões de spams por dia**
- **Continuidade do financiamento da equipe de *data mining* da UFMG**
- **Sensores em funcionamento:**
  - **AT:** CERT.at
  - **AU:** AusCERT
  - **BR:** CERT.br
  - **BR:** CSIRT-USP
  - **CL:** CLCERT
  - **NL:** SURFcert
  - **TW:** TWCERT/CC
  - **US:** Univ. of Washington
  - **UY:** CSIRT Antel
- **Próximos Sensores:**
  - **AE** (aeCERT)
  - **AR** (CSIRT Banelco and Univ. de La Plata)
  - **DE** (Telekom-CERT)
  - **EC** (Univ. de Loja)
  - **GR** (FORTH, ICS)
  - **MY** (MyCERT)
  - **PL** (CERT Polska)
  - **TH** (ThaiCERT)
  - **TN** (TunCERT)
  - **UK** (OX-CERT)
  - **US** (Univ. of Alabama at Birmingham e IBM)
  - **ZA** (via SURFcert)

Uso de *botnets* para DDoS

- **20 PCs domésticos abusando de Servidores DNS Recursivos Abertos podem gerar 1Gbps**
  - **No Brasil temos mais de 13.000 recursivos abertos no momento**
    (Dados do *Measurement Factory* passados ao CERT.br semanalmente)
- **Em março de 2009 foram atingidos picos de 48Gbps**
  - **em média ocorrem 3 ataques de 1Gbps por dia na Internet**
- **De 2% a 3% do tráfego de um grande *backbone* é ruído de DDoS**
- **Extorsão é o principal objetivo**
  - **mas *download* de outros *malwares*, *spam* e furto de informações também valem dinheiro e acabam sendo parte do *payload* dos *bots***

Fonte: ***Global Botnet Underground: DDoS and Botconomics*.**
***Jose Nazario, Ph.D., Head of Arbor* ASERT**
***Keynote* do Evento RioInfo 2009**

Reais Causas dos Problemas

- **Cenário atual é reflexo direto de**
  - **Aumento da complexidade dos sistemas**
  - **Falta de desenvolvedores capacitados para desenvolver com requisitos de segurança**
  - ***Softwares* com muitas vulnerabilidades**
  - **Pressão econômica para lançar, mesmo com problemas**
  - **É uma questão de "*Economics and Security*" http://www.cl.cam.ac.uk/~rja14/econsec.html**

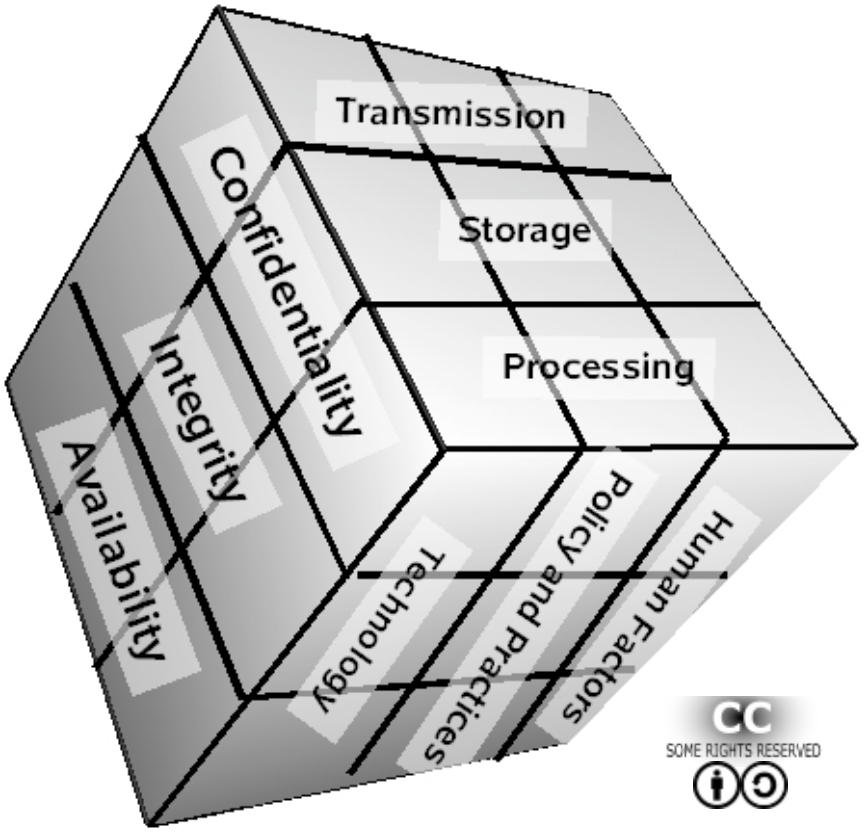
- **Os criminosos estão apenas migrando para onde os negócios estão**

Mitos

"Xxxxxx" é o componente mais importante!

- **Não há um componente mais importante que outro**
- **Componentes mais comumente citados como principais:**
  - **Criptografia**
  - **Firewalls**
  - **IDSs**
  - **Antivírus**
- **Componentes mais comumente negligenciados:**
  - **Políticas**
  - **Procedimentos**
  - **Treinamento**

Information Security Rubik's Cube



http://en.wikipedia.org/wiki/File:Mccumber.jpg

Só quem sabe invadir sabe proteger

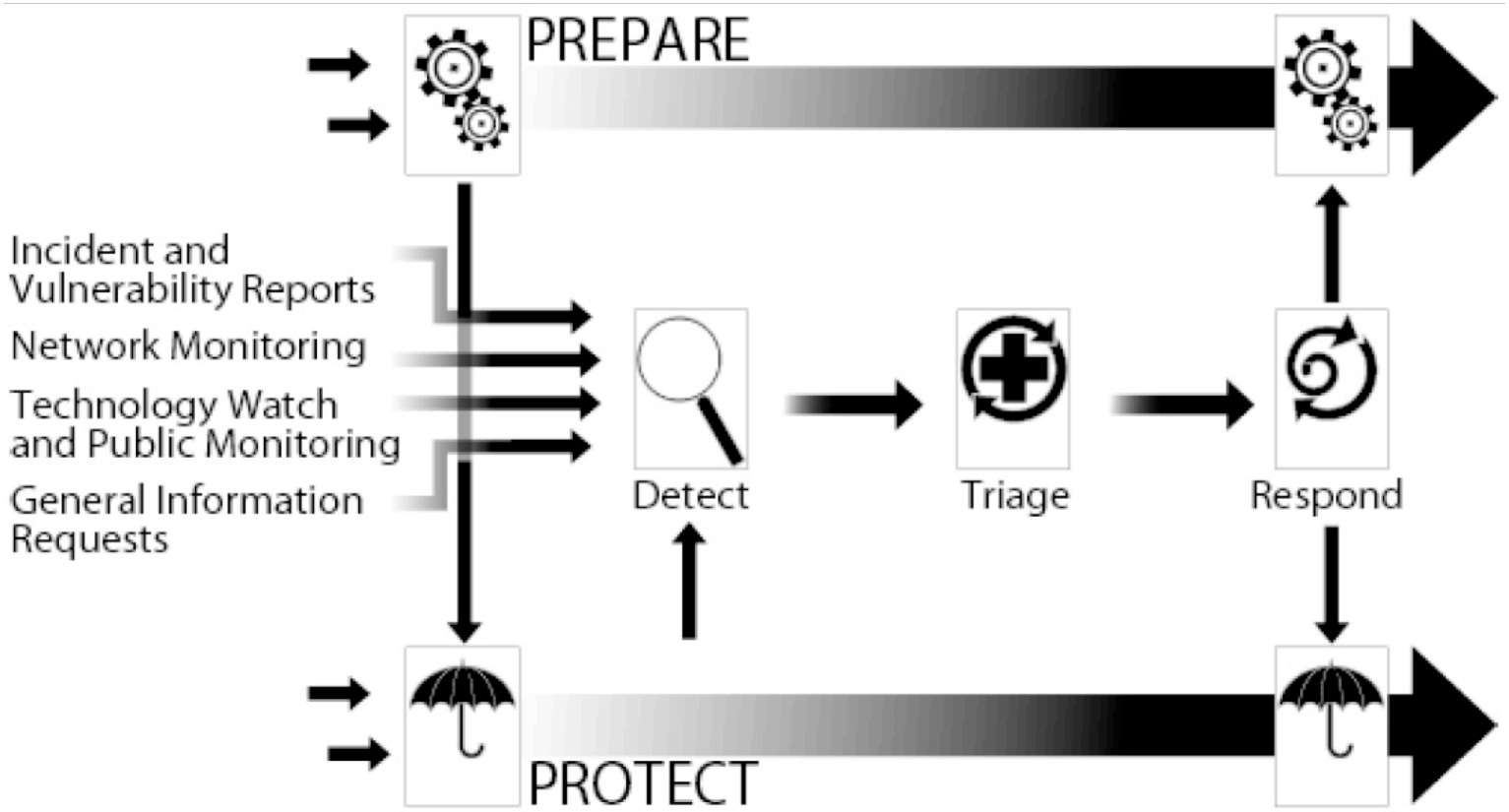
- **A realidade:**
  - **Raríssimos os atacantes que:**
    - **sabem como proteger uma rede ou corrigir um problema**
    - **sabem como funcionam as ferramentas que utilizam**
  - **Maioria absoluta utiliza ferramentas disponíveis na Internet**
    - **Difícil o ataque que não esteja hoje integrado ao *software* Metasploit**
  - **Um profissional com sólida formação tem mais sucesso em utilizar as ferramentas como auxiliares nos processos de análise de risco e proteção da infra-estrutura que um invasor**
- **Os riscos:**
  - **Colocar a segurança nas mãos de quem não está preparado**
  - **Ter informações confidenciais furtadas**
  - **Ter *backdoors* e cavalos de tróia instalados em sua infra-estrutura**

O que Está Sendo Feito no Brasil

Desde 1999: Estímulo e Apoio para a Criação de Grupos de Tratamento de Incidentes (CSIRTs) no Brasil

"Um CSIRT provê serviços de suporte para prevenção, tratamento e resposta a incidentes de segurança em computadores."

– *CERT® Program CSIRT Development Team*



Fonte: ***Defining Incident Management Processes for CSIRTs: A Work in Progress*.** **Figura utilizada com permissão do CERT®/CC e do SEI/CMU.**
http://www.cert.org/archive/pdf/04tr015.pdf

Papel dos CSIRTs na Mitigação e Recuperação

- A redução do impacto é conseqüência da:
  - agilidade de resposta
  - redução no número de vítimas
- O sucesso depende da confiabilidade
  - nunca divulgar dados sensíveis nem expor vítimas, por exemplo
- O papel do CSIRT é:
  - auxiliar a proteção da infra-estrutura e das informações
  - prevenir incidentes e conscientizar sobre os problemas
- O CSIRT não é um investigador
  - A decisão de levar um caso à justiça deve ser da vítima
  - Em uma organização, leia-se: alta administração e setor jurídico
- A pessoa que responde um incidente é a primeira a entrar em contato com as evidências de um possível crime
  - seguir as políticas
  - preservar as evidências
  - responder incidentes – retornar o ambiente ao estado de produção

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 CSIRTs***
    - ***Fundamentals of Incident Handling***
    - ***Advanced Incident Handling for Technical Staff***
  - **400+ profissionais segurança treinados**
    - **máximo de 25 participantes por turma**

Treinamento de Profissionais e Fomento à Troca de Experiências

- **Cursos gratuitos do CEPTRO.br**
  - **Administração de Sistemas Autônomos**
  - **Administração de backbones IPv6**
- **Reuniões do GTER e GTS**
  - **Gratuitas e transmitidas pela Internet**
  - **Realizadas 2 vezes por ano**
  - **Com estudos de caso e mini-tutoriais**
- **Reuniões periódicas com diversos setores**
  - **Sistema Financeiro**
  - **Anatel, Associções, Provedores e Operadoras de Telecomunicações**
  - **Ministérios Públicos e Polícias**

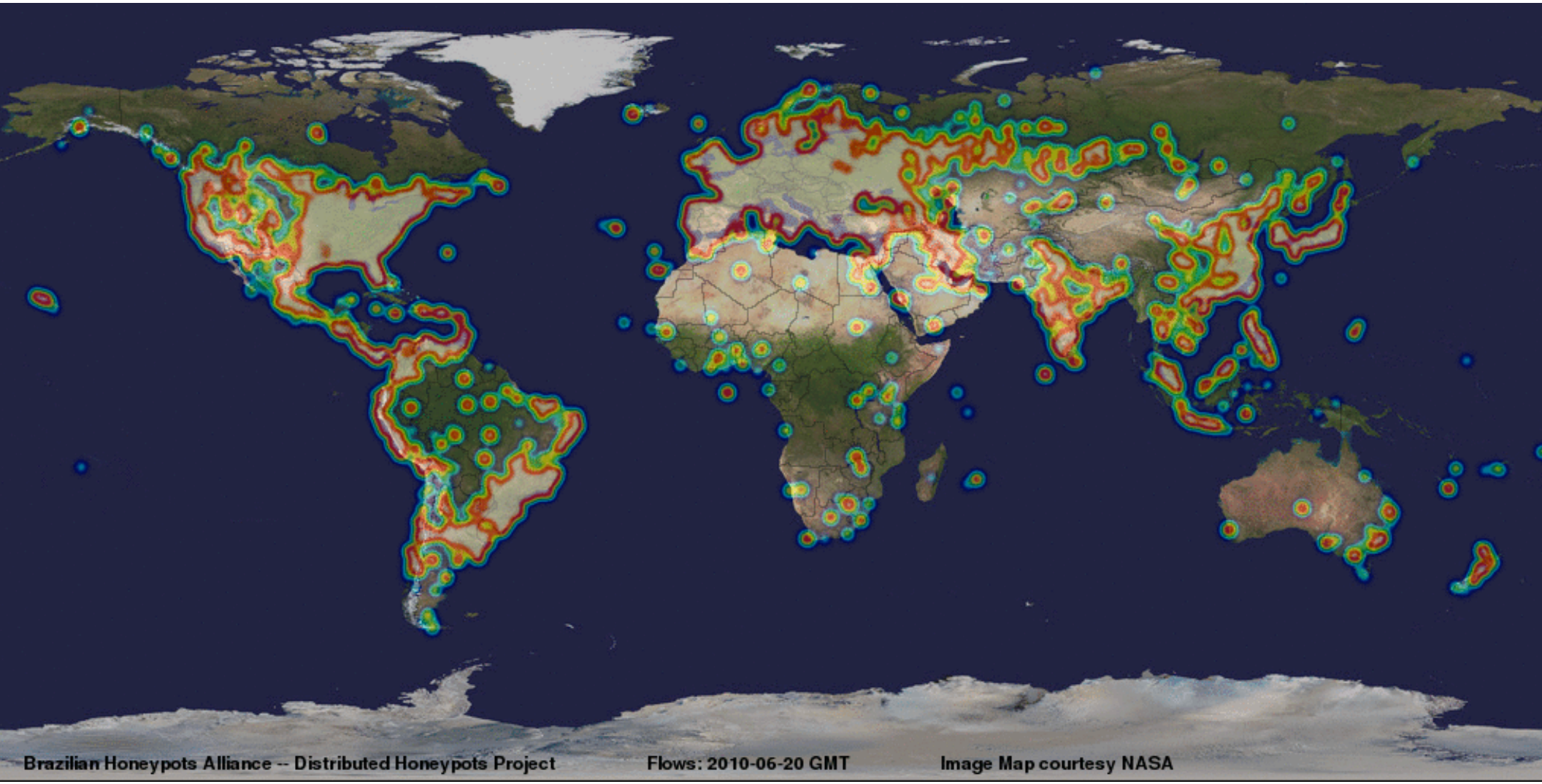
Proteção da Infra-Estrutura Crítica de Internet

- **Manutenção da Hora Oficial do Brasil para sincronia de computadores – NIC.br**
- **Manutenção dos Pontos de Troca de Tráfego nas áreas metropolitanas – PTT.br**
- **Manutenção de espelhos de 3 servidores raiz DNS no Brasil**
- **Adoção de DNSSEC pelo Registro.br**
  - **Brasil foi o segundo ccTLD a adotar DNSSEC**
  - **Hoje temos todo o `.br` com possibilidade de uso de DNSSEC**
  - **Treinamento gratuito online ou presencial**
  - **`.jus.br` e `.b.br` só permitem domínios com DNNSEC**
- **Uso de PKI na infra-estrutura de BGP**
  - **Tabelas de rotas passam a ser assinadas**
  - **LACNIC está fomento a mudança para um esquema com PKI**

Obs.: LACNIC é o Registro de Endereços da Internet para a América Latina e o Caribe.
Para as demais regiões há: AfriNIC (África), APNIC (Ásia Pacífico), ARIN (América do Norte) e RIPE NCC (Europa e Oriente Médio).

Monitoração do Espaço Internet Brasileiro

Criação e Manutenção da Infra-Estrutura, Desenvolvimento de Software e de Estatísticas do Consórcio de *Honeypots*



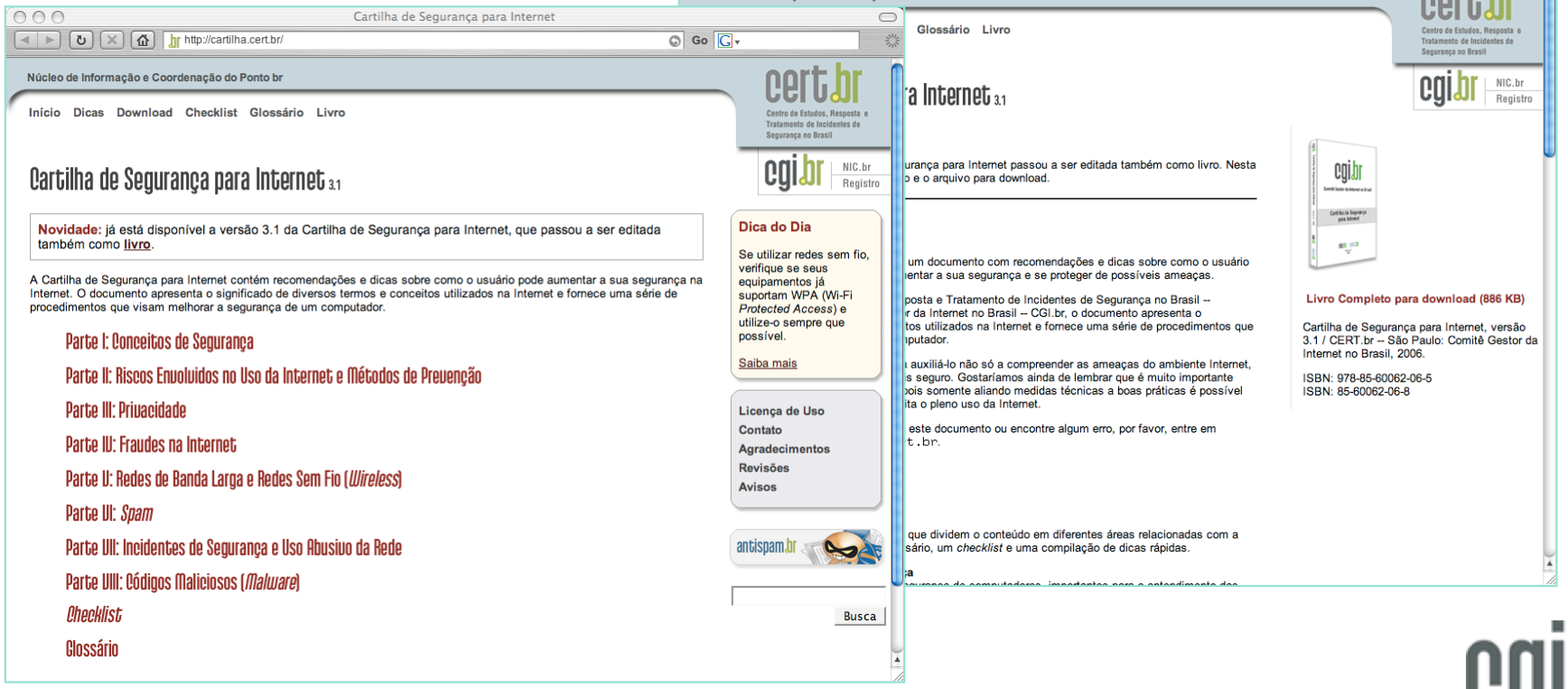
Manutenção da Rede Mundial de Sensores para Coleta de *Spam*, *Phishing* e outras ameaças por *e-mail*

SpamPots Project – Statistics

#	CC	description	emails (%)		recipients (%)		connections	proto	spampots
1	US	United States	3,315,279	51.35	154,874,994	76.90	836,977	HTTP, SMTP, S4, S4a, S5	8
2	TW	Taiwan, Province of China	1,361,503	21.09	31,760,766	15.77	683,307	HTTP, SMTP, S4, S4a, S5	8
3	CN	China	1,114,050	17.25	4,925,335	2.45	101,717	HTTP, SMTP, S4, S5	7
4	HK	Hong Kong	275,327	4.26	4,333,383	2.15	139,566	HTTP, SMTP, S4, S4a, S5	8
5	JP	Japan	218,358	3.38	236,508	0.12	106,476	HTTP, SMTP, S4, S5	6
6	BR	Brazil	55,346	0.86	1,739,851	0.86	21,504	SMTP	8
7	IN	India	23,608	0.37	755,316	0.38	9,415	SMTP	6
8	RU	Russian Federation	12,602	0.20	391,564	0.19	4,936	SMTP	7
9	ID	Indonesia	11,097	0.17	328,018	0.16	4,393	SMTP	7
10	TH	Thailand	8,183	0.13	264,049	0.13	3,278	SMTP	6
11	AR	Argentina	8,133	0.13	260,159	0.13	3,213	SMTP, S4, S5	7
12	CO	Colombia	6,400	0.10	214,540	0.11	2,580	SMTP	7
13	MY	Malaysia	5,356	0.08	80,295	0.04	4,814	SMTP	7
14	KR	Korea, Republic of	2,949	0.05	86,476	0.04	1,124	SMTP	7
15	PL	Poland	2,699	0.04	85,836	0.04	1,017	SMTP	6
16	TR	Turkey	2,539	0.04	86,441	0.04	1,002	SMTP	6
17	FR	France	2,449	0.04	80,192	0.04	943	SMTP, S4	6
18	IL	Israel	2,372	0.04	82,411	0.04	911	SMTP	5
19	PK	Pakistan	2,339	0.04	80,231	0.04	932	SMTP	5
20	ZA	South Africa	2,180	0.03	69,573	0.03	868	SMTP	6
21	UA	Ukraine	2,084	0.03	61,584	0.03	813	SMTP	6
22	VN	Vietnam	1,650	0.03	47,129	0.02	626	SMTP	6
23	CZ	Czech Republic	1,609	0.02	44,291	0.02	569	SMTP	6
24	GR	Greece	1,275	0.02	42,509	0.02	513	SMTP	7
25	GT	Guatemala	1,178	0.02	38,354	0.02	481	SMTP	6
26	CL	Chile	1,177	0.02	30,406	0.02	428	SMTP	6
27	HU	Hungary	1,116	0.02	38,568	0.02	452	SMTP	5
28	GB	United Kingdom	985	0.02	19,559	0.01	326	SMTP	7
29	NP	Nepal	919	0.01	31,028	0.02	383	SMTP	5
30	NG	Nigeria	753	0.01	22,659	0.01	494	SMTP, S4, S5	4
31	others (48)		11,143	0.17	288,835	0.14	4,533	HTTP, SMTP, S5	——
Total			**6,456,658**	**100.00**	**201,400,860**	**100.00**	**1,938,591**		

Produção de Material que Reflete os Incidentes Mais Comuns e as Tendências Observadas (2/2)

- **Práticas de Segurança para Administradores de Redes Internet**
  http://www.cert.br/seg-adm-redes/
  - **boas práticas em configuração, administração e operação segura de redes conectadas à Internet**
- **Cartilha de Segurança para Internet**
  http://cartilha.cert.br/



Produção de Material que Reflete os Incidentes Mais Comuns e as Tendências Observadas (2/2)

- **Site Antispam.br – Vídeos Educacionais no escopo das atividades da CT Anti-Spam do CGI.br**
  http://www.antispam.br/

Desafios

Desafios (1/2)

- **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)
  - ***Desenvolvimento seguro de software* se tornar parte da formação de projetistas e programadores**
    - **Desde a primeira disciplina de programação e permeado em todas as disciplinas**
  - **Provedores de acesso e serviço, operadoras e administradores de redes em geral forem mais pró-ativos**
  - **Os sistemas para usuários finais forem menos complexos**
    - **Mudança total de paradigma de uso da tecnologia**

Desafios (2/2)

- **Há falta de pessoal treinado no Brasil para lidar com Redes e com segurança em IPv4**
  - **A falta de pessoal com essas habilidades em IPv6 é ainda mais gritante**
- **Vencer a cultura de que é melhor investir em tecnologia do que treinamento e implantação de boas políticas**
  - **Quantas instituições realmente implementam tecnologias com base em uma análise de risco?**
- **Ir além do "*compliance*"**

Referências

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/
- **CETIC.br - Centro de Estudos sobre as Tecnologias da Informação e da Comunicação**
  http://www.cetic.br/