Tratamento de Incidentes de Segurança e Tendências no Brasil

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

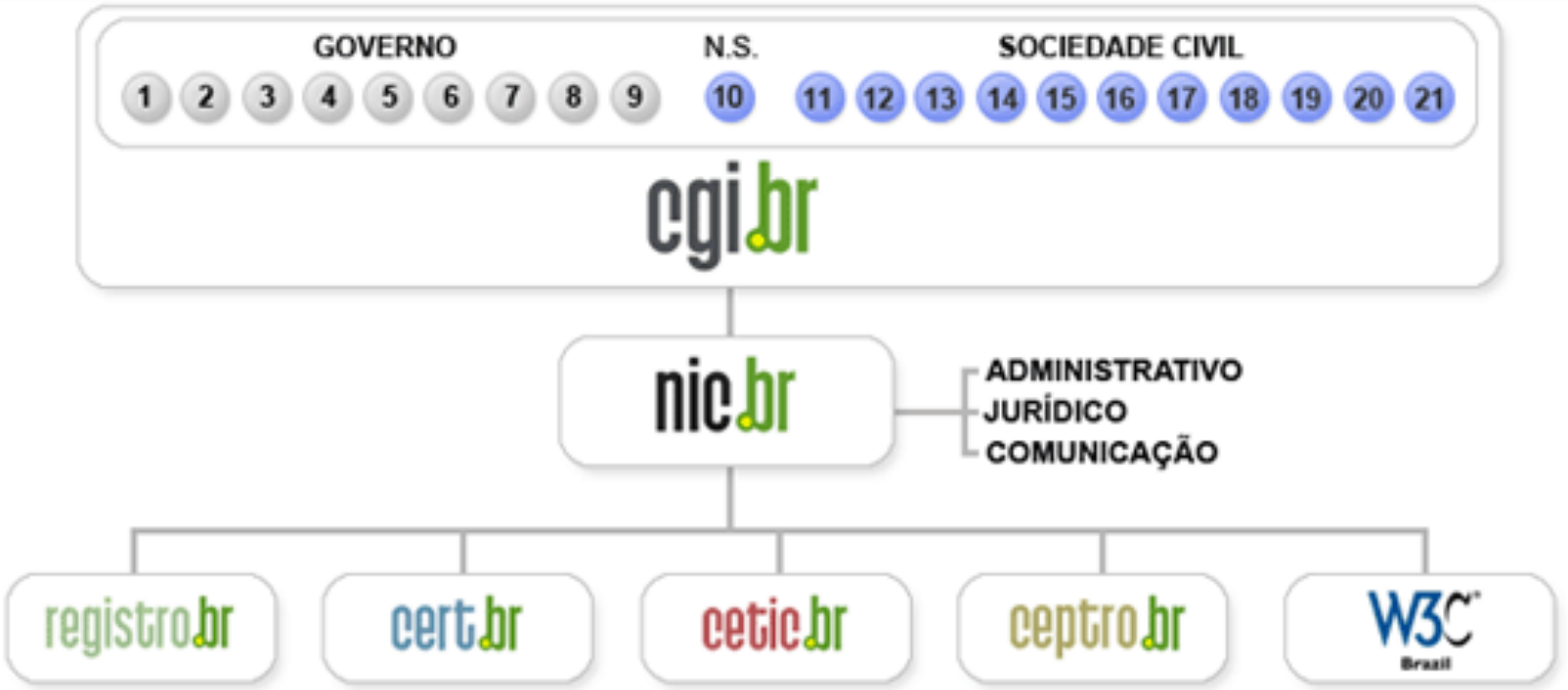
Comitê Gestor da Internet no Brasil – CGI.br

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

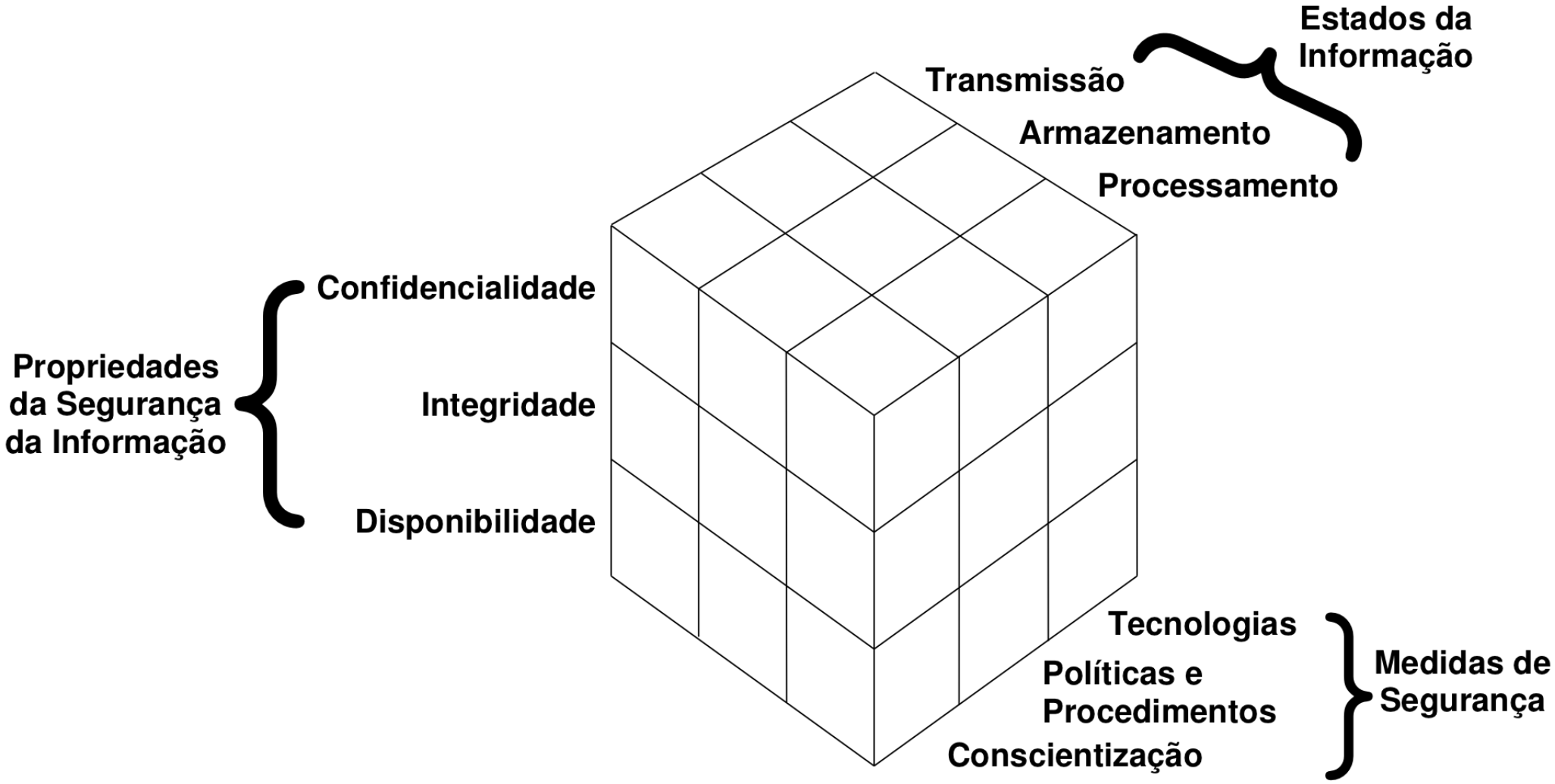
11 – provedores de acesso e conteúdo
12 – provedores de infra-estrutura de telecomunicações
13 – indústria de bens de informática, telecomunicações e software
14 – segmento das empresas usuárias de Internet
15-18 – representantes do terceiro setor
19-21 – representantes da comunidade científica e tecnológica

Agenda

- **Tratamento de Incidentes**
  - **Conceitos**
  - **Cenário Brasileiro**
- **Serviços do CERT.br para a Comunidade**
  - **Treinamento e Conscientização**
  - **Análise de Tendências**
  - **Tratamento de Incidentes**
- **Panorama de alguns tipos de incidentes no Brasil**

Alguns Conceitos

Relembrando o Modelo Clássico de Segurança da Informação



As Informações Estão em Diversos Locais e a Segurança Depende de Múltiplos Fatores

Incidente de Segurança

Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

-ou-

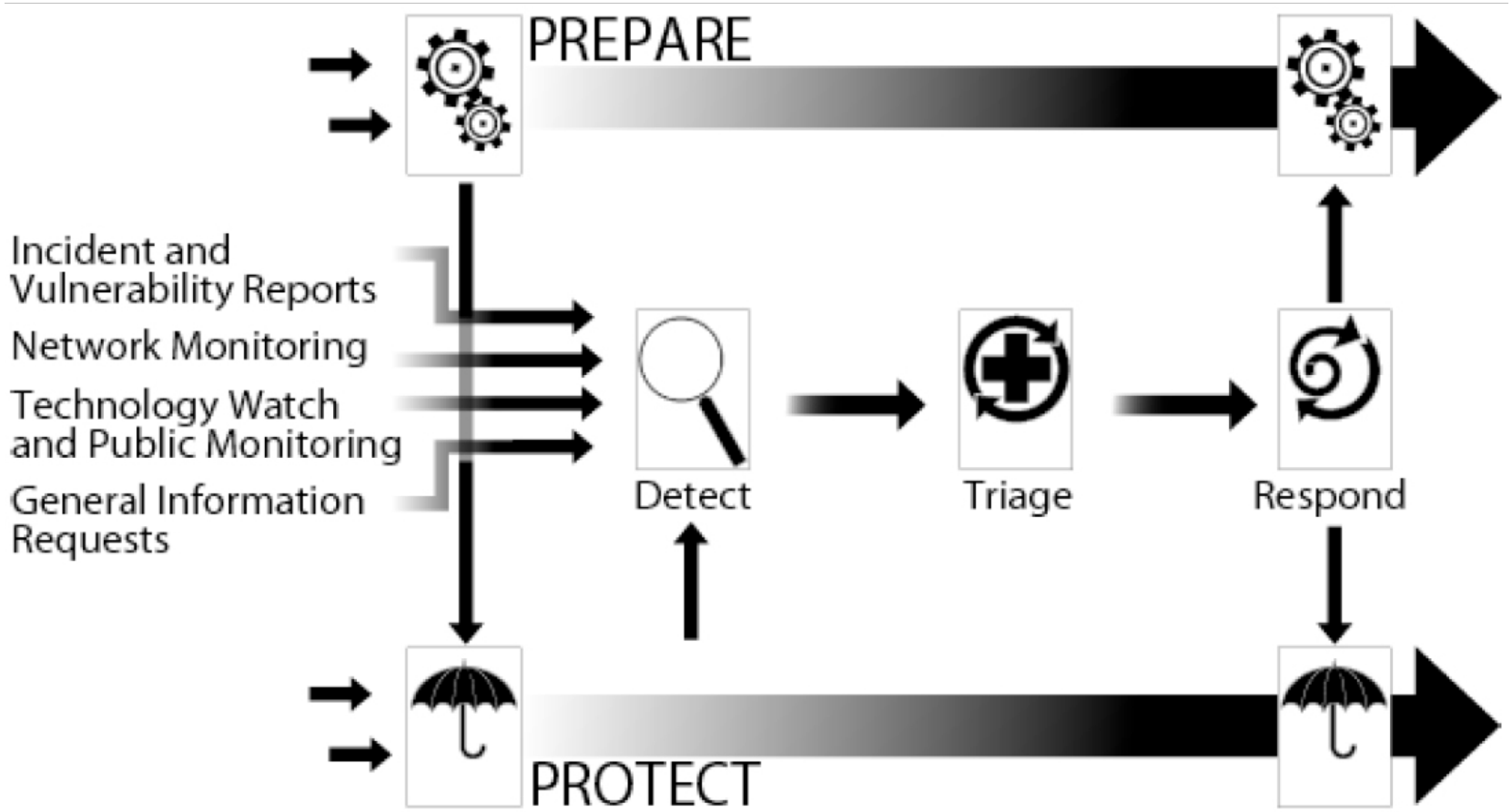
O ato de violar uma política de segurança, explícita ou implícita.

http://www.cert.br/certcc/csirts/csirt_faq-br.html

Tratamento de Incidentes

"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

Evolução do Tratamento de Incidentes no Brasil

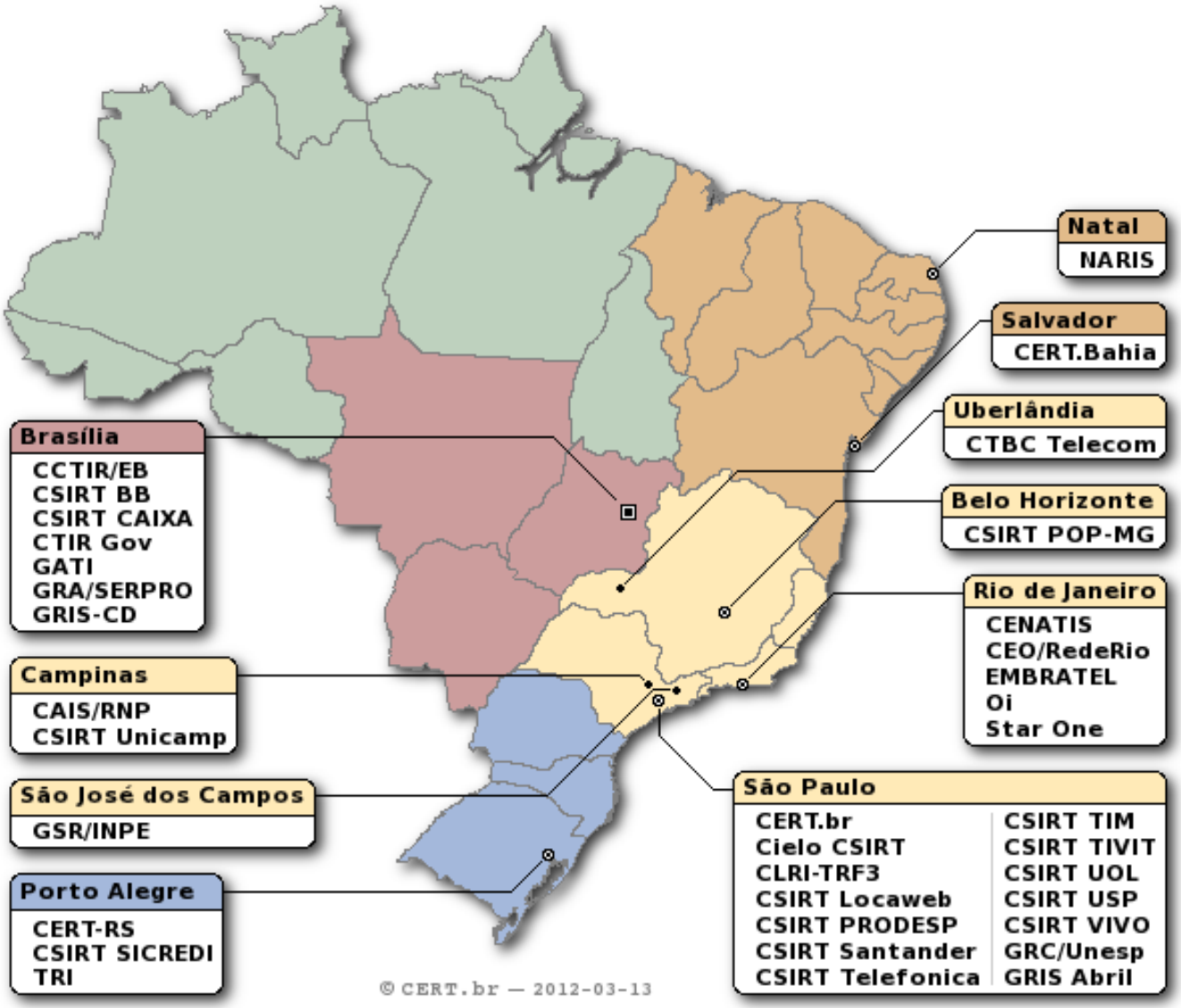
- Agosto/1996: o relatório "Rumo à Criação de uma Coordenadoria de Seguraça de Redes na Internet Brasil" é publicado pelo CGI.br[1]
- Junho/1997: o CGI.br cria o CERT.br (à época chamado NBSO – *NIC BR Security Office*), com base nas recomendações do relatório, como um grupo com responsabilidade nacional[2]
- 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 no MP 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

CSIRTs Brasileiros – Abril/2012

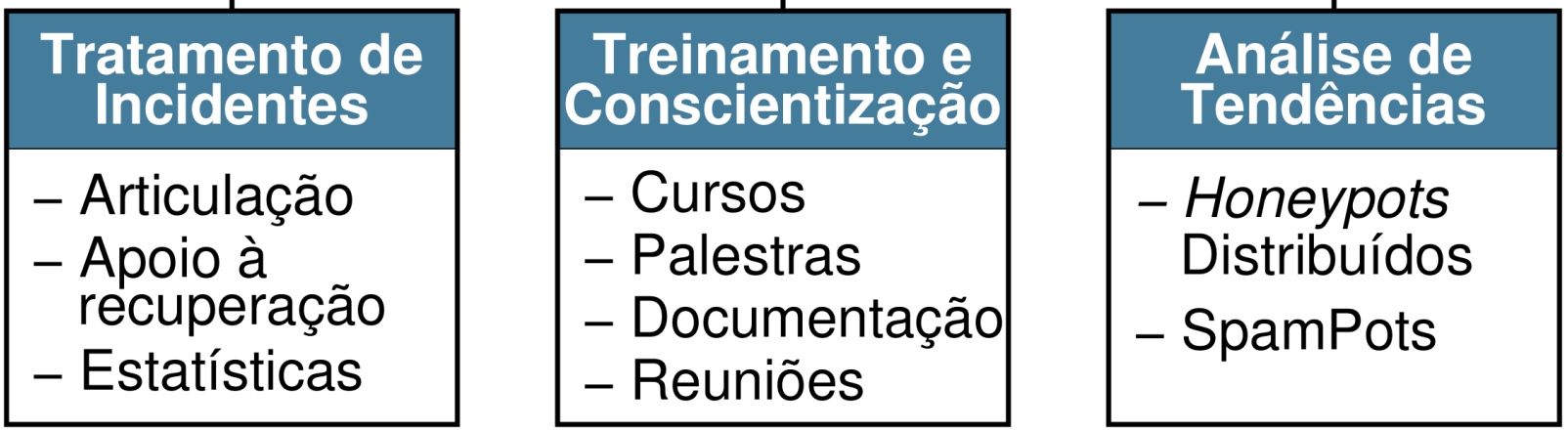
36 times com serviços anunciados ao público

Público Alvo	CSIRTs
Qualquer Rede no País	CERT.br
Governo	CCTIR/EB CLRI-TRF-3, CSIRT Prodesp, CTIR Gov, GATI, GRA/SERPRO, GRIS-CD
Setor Financeiro	Cielo CSIRT, CSIRT BB, CSIRT CAIXA, CSIRT Sicredi, CSIRT Santander
Telecom/ISP	CTBC Telecom, EMBRATEL, CSIRT Telefonica, CSIRT Locaweb, CSIRT TIM, CSIRT UOL, CSIRT VIVO, StarOne, Oi,
Academia	GSR/INPE, CAIS/RNP, CSIRT Unicamp, CERT-RS, NARIS, CSIRT POP-MG, CENATIS, CEO/RedeRio, CERT-Bahia, CSIRT USP, GRC/UNESP, TRI
Outros	CSIRT TIVIT, GRIS Abril



http://www.cert.br/csirts/brasil/

CERT.br



SEI Partner
Carnegie Mellon

FIRST
Improving Security Together
MEMBER

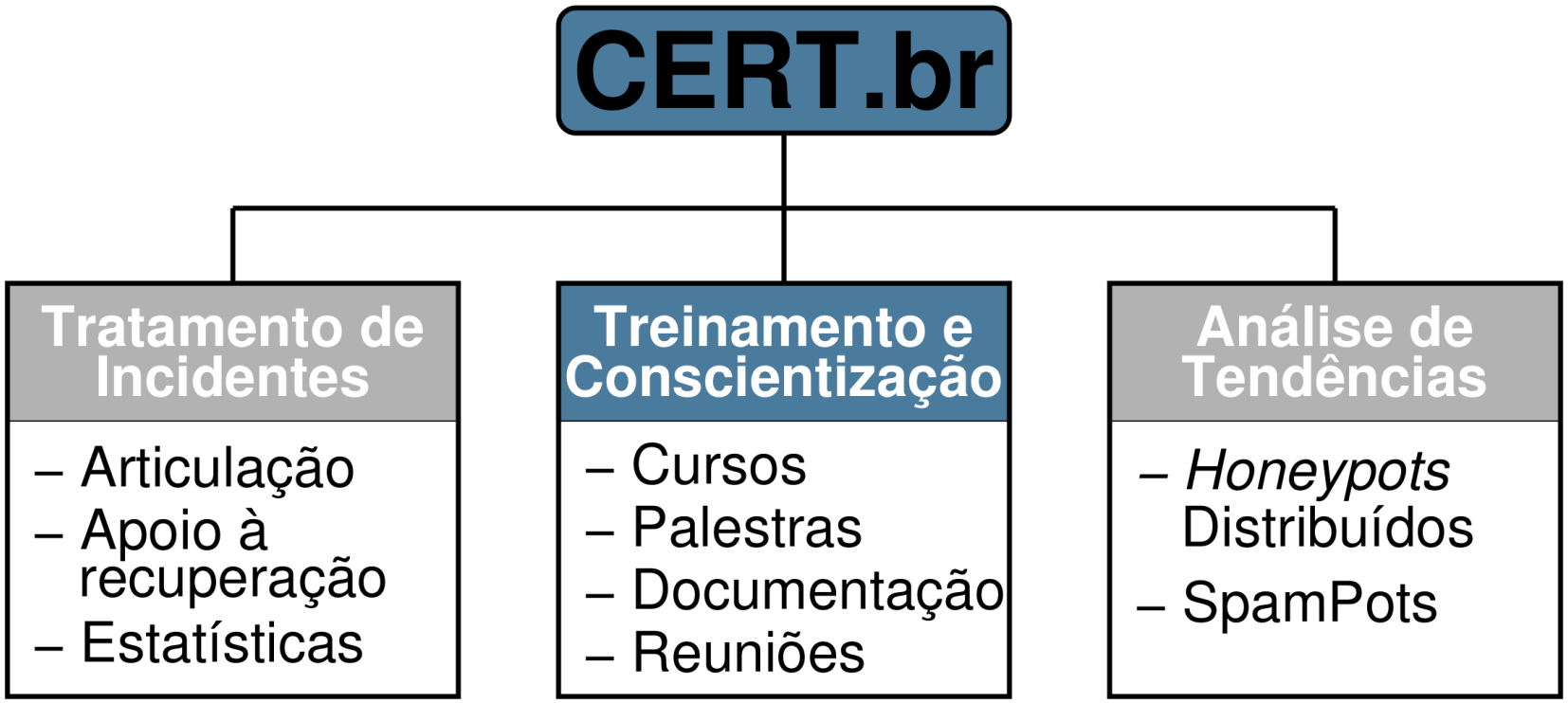
APWG
RESEARCH PARTNER
www.antiphishing.org

The Honeynet PROJECT

Criado em 1997 para:

- **Ser um ponto de contato nacional para notificação de incidentes**
- **Prover a facilitação e o apoio necessários no processo de resposta a incidentes**
- **Estabelecer um trabalho colaborativo com outras entidades**
- **Aumentar a conscientização sobre a necessidade de segurança na Internet**
- **Auxiliar novos CSIRTs (Grupos de Tratamento de Incidentes de Segurança) a estabelecerem suas atividades**

Rumo a Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil
http://www.nic.br/grupo/historico-gts.htm | http://www.cert.br/sobre/


CERT.br
Tratamento de Incidentes
– Articulação
– Apoio à recuperação
– Estatísticas
Treinamento e Conscientização
– Cursos
– Palestras
– Documentação
– Reuniões
Análise de Tendências
– *Honeypots* Distribuídos
– SpamPots

Treinamento

SEI Partner
Carnegie Mellon

Objetivos:

- Criar/aproximar CSIRTs (Grupos de Tratamento de Incidentes de Segurança) no Brasil
- Possuir profissionais preparados para resolver os problemas de segurança no país

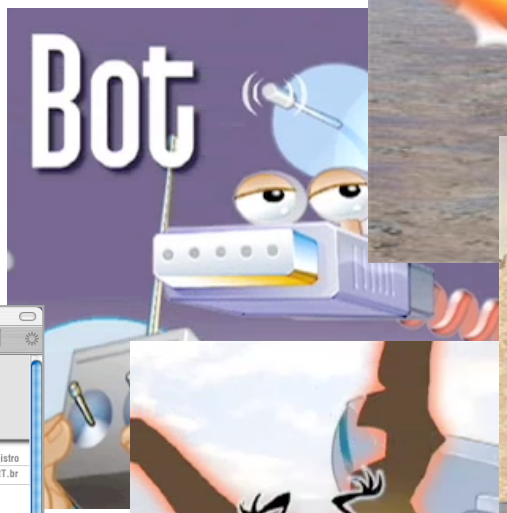
SEI/Carnegie Mellon Partner **desde 2004, licenciado para ministrar cursos do *CERT® Program* no Brasil:**

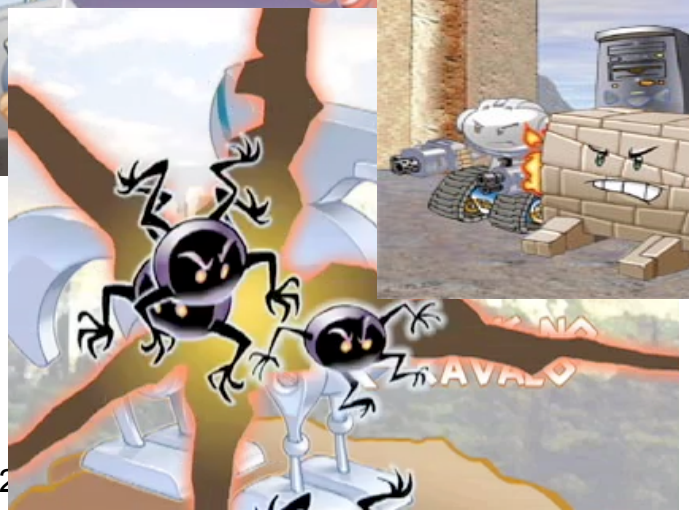
- http://www.cert.br/cursos/
  - ***Overview of Creating and Managing CSIRTs***
  - ***Fundamentals of Incident Handling***
  - ***Advanced Incident Handling for Technical Staff***
- **400+ profissionais treinados em tratamento de incidentes**
  - **máximo de 25 participantes por turma**

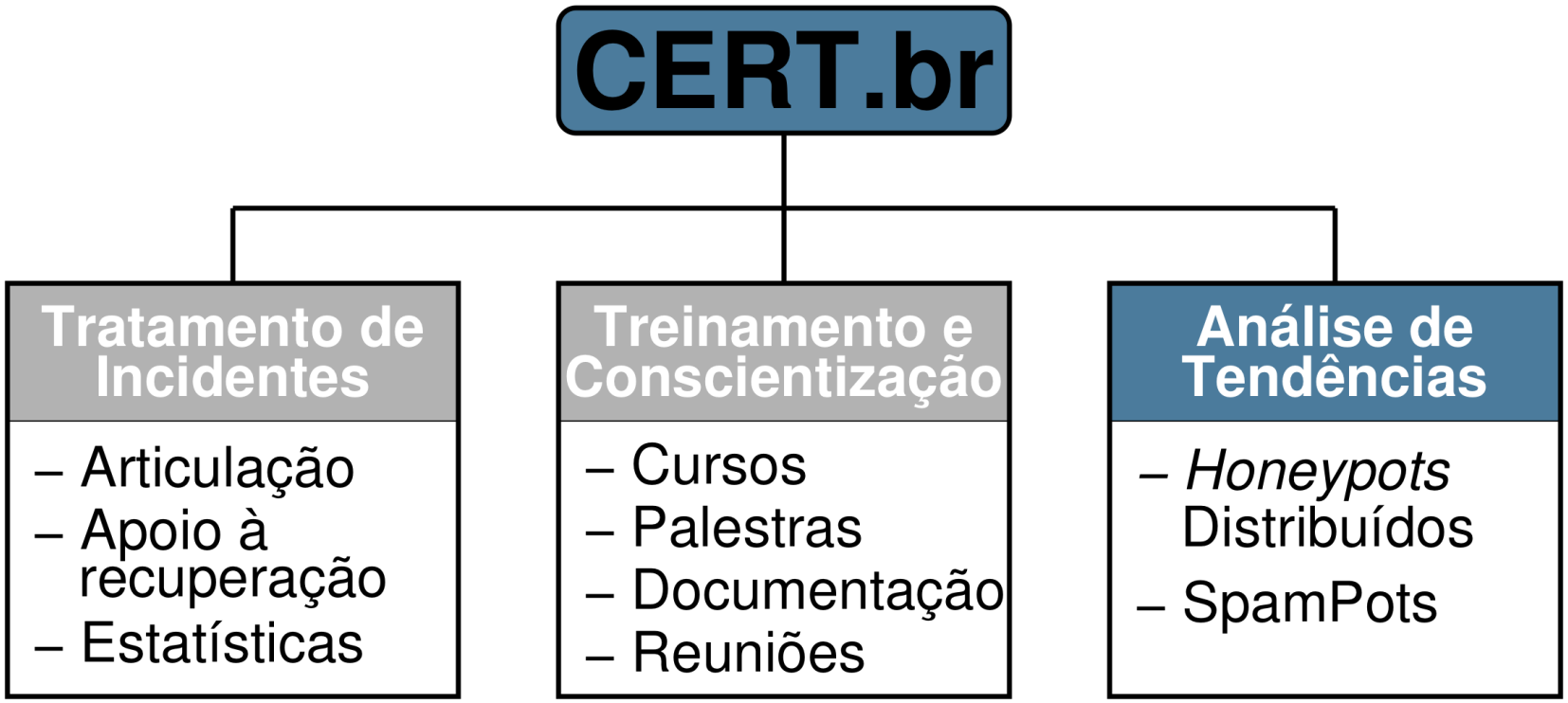
Produção de Material Gratuito para Educação sobre Riscos e Proteção na Internet

- Cartilha de Segurança para Internet
- Site Antispam.br
- Vídeos Educacionais
- InternetSegura.br

INTERNET SEGURA.BR





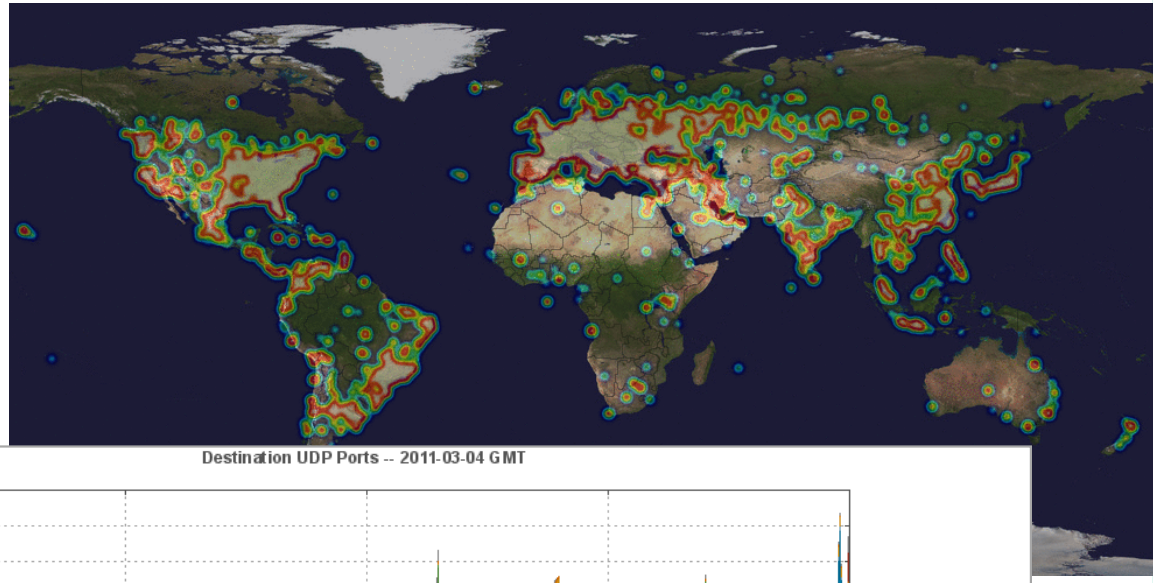

CERT.br
Tratamento de Incidentes
– Articulação
– Apoio à recuperação
– Estatísticas
Treinamento e Conscientização
– Cursos
– Palestras
– Documentação
– Reuniões
Análise de Tendências
– *Honeypots* Distribuídos
– SpamPots

Análise de Tendências

The Honeynet PROJECT

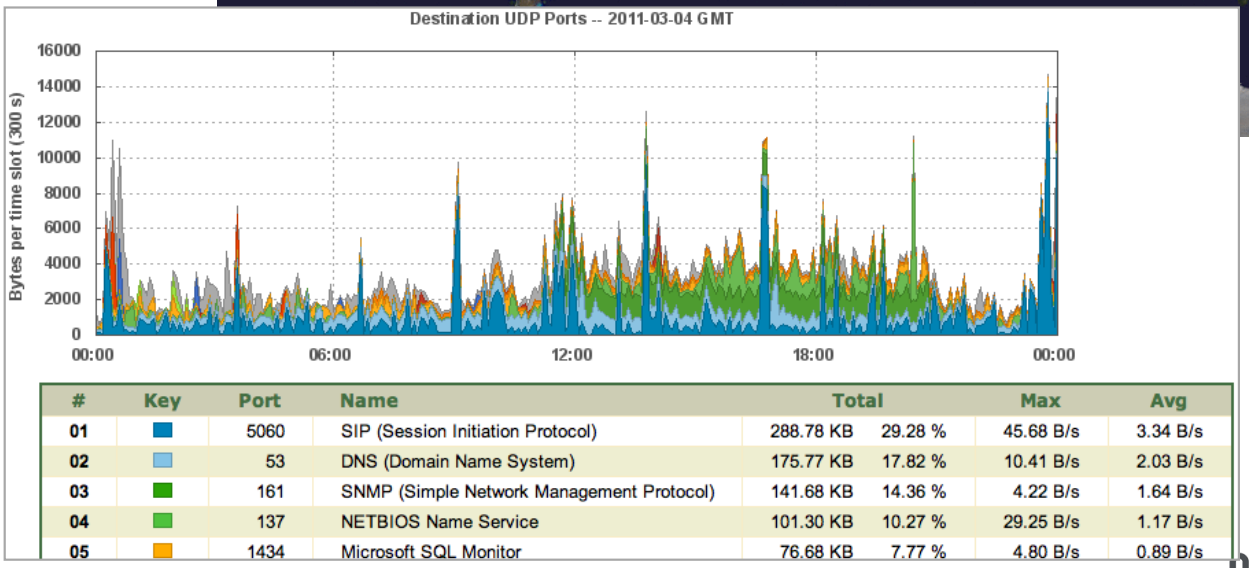
Objetivos

- Ter um "termômetro" das atividades maliciosas na Internet
- Entender o abuso da infra-estrutura da Internet por atacantes, *spammers* e fraudadores
- Propor técnicas para proteger os usuários e coibir o abuso



Projetos

- Honeypots Distribuídos
- SpamPots



#	Key	Port	Name	Total		Max	Avg
01		5060	SIP (Session Initiation Protocol)	288.78 KB	29.28 %	45.68 B/s	3.34 B/s
02		53	DNS (Domain Name System)	175.77 KB	17.82 %	10.41 B/s	2.03 B/s
03		161	SNMP (Simple Network Management Protocol)	141.68 KB	14.36 %	4.22 B/s	1.64 B/s
04		137	NETBIOS Name Service	101.30 KB	10.27 %	29.25 B/s	1.17 B/s
05		1434	Microsoft SQL Monitor	76.68 KB	7.77 %	4.80 B/s	0.89 B/s

The Honeynet Project

honeyTARG Chapter

http://honeytarg.cert.br/

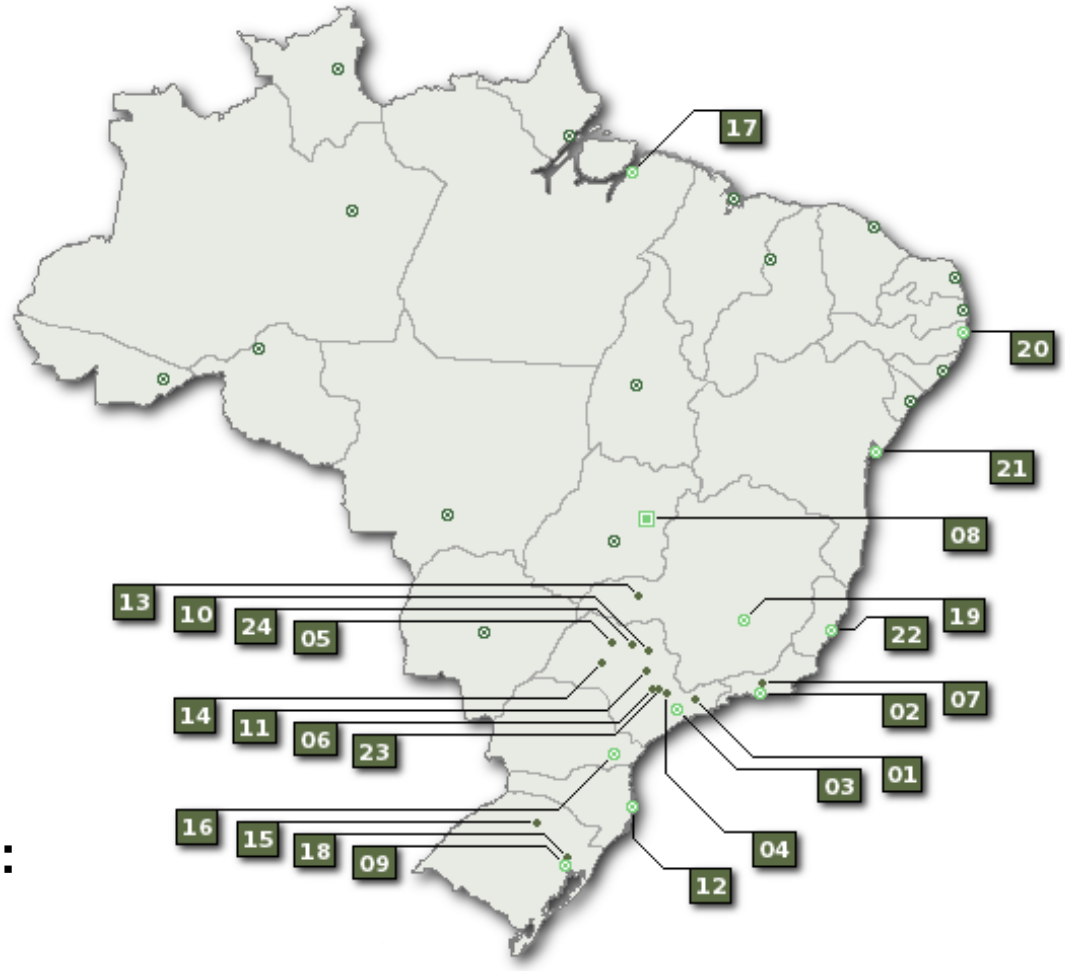
Honeypots Distribuídos

Mapeamento das atividades maliciosas na Internet no Brasil

- **51 sensores em 41 redes (universidades, governo, provedores, operadoras e empresas)**

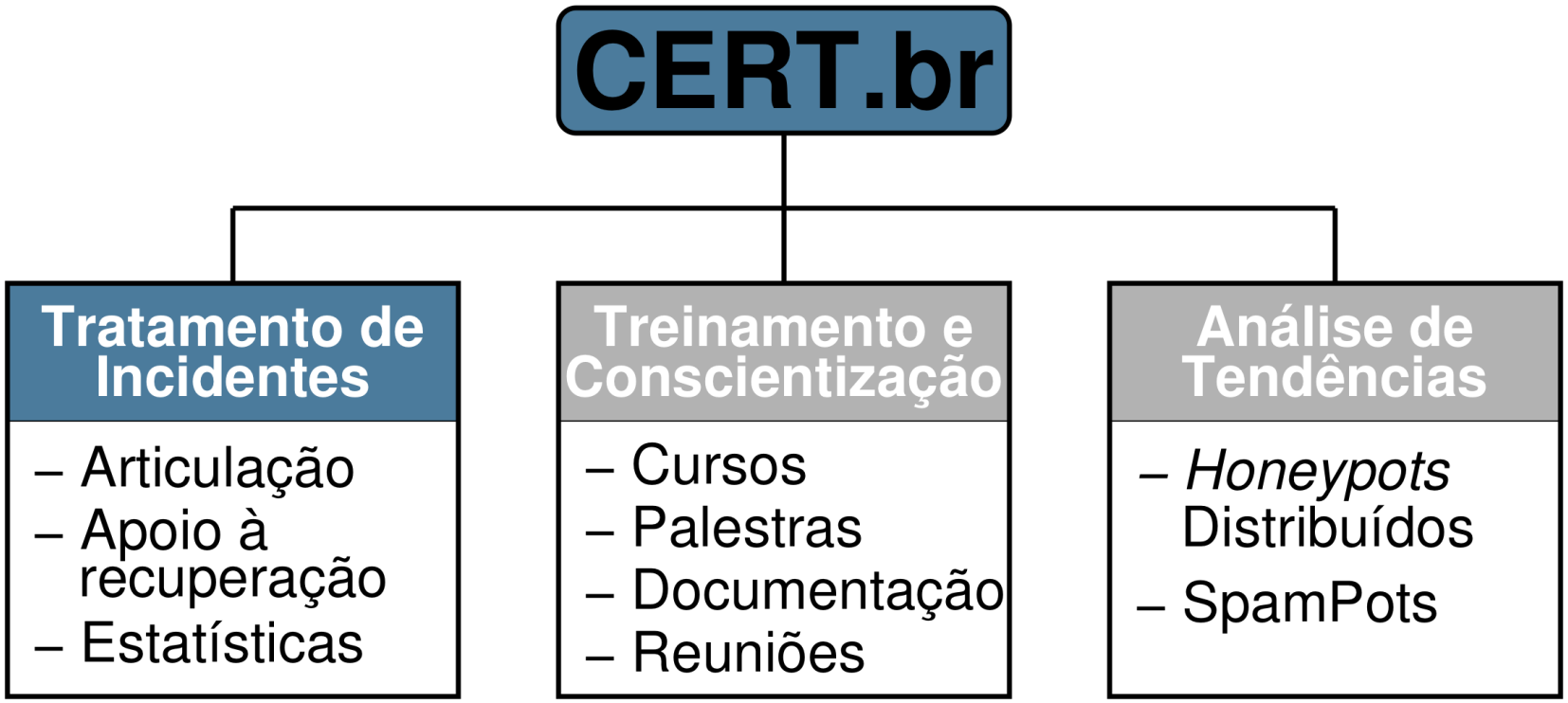
Uso dos dados:

- **Gerar estatísticas públicas sobre tendências**
- **Notificar *sites* brasileiros com problemas**
- **Enviar dados anonimizados**
  - **para CERTs Nacionais, para auxiliar esforços de combate a botnets: Austrália, Polônia, Uruguai, Argentina, Colômbia, Qatar**
  - **Entidades de combate a botnets: Arbor Atlas, Team Cymru, ShadowServer**



Projeto SpamPots

- Entender o abuso da infra-estrutura da Internet por *spammers* e fraudadores
- Propor técnicas para proteger os usuários e coibir o abuso
  - Exemplo: Acordo de Cooperação para Implementação de Gerência de Porta 25, assinado por Anatel, NIC.br, CGI.br, ABTA, SindiTelebrasil e Associações de Provedores de Acesso e Serviços.
- Parceria com o Laboratório eSpeed/DCC/UFMG para mineração de dados
  - Aprox. 11 milhões de spams coletados por dia
- Sensores em 8 países, em parceria com CERTs locais: AusCERT (Austrália), CERT.at (Áustria), CLCERT (Chile), CSIRT ANTEL (Uruguai). CSIRT USP (Brasil), CSIRT UTPL (Equador), SurfCERT (Holanda) e TWCERT/CC (Taiwan)
- Envio de dados para países originadores de abuso
  - Japão: JPCERT/CC, JADAC, IIJ e Min. das Comunicações
  - Taiwan: TWCERT/CC e NCC/TW

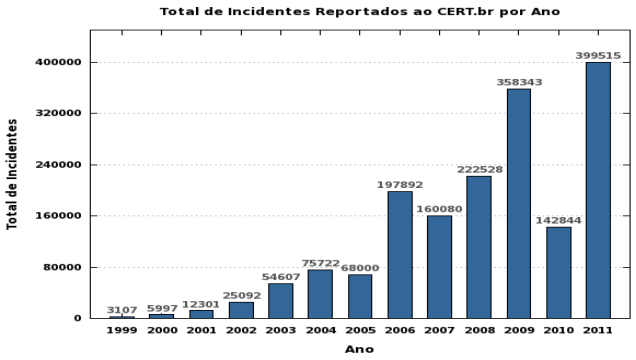

CERT.br
Tratamento de Incidentes
– Articulação
– Apoio à recuperação
– Estatísticas
Treinamento e Conscientização
– Cursos
– Palestras
– Documentação
– Reuniões
Análise de Tendências
– *Honeypots* Distribuídos
– SpamPots

Dados Usados para Tratamento de Incidentes

- **Notificações voluntárias de incidentes de segurança na Internet - são a fonte de dados das estatísticas trimestrais**

  Ponto de entrada: email cert@cert.br

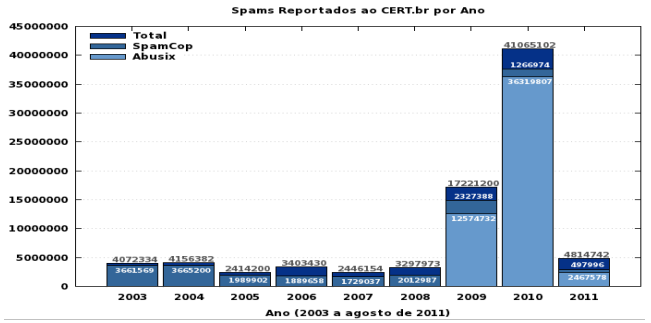
  - **2010: 885.731 *e-mails***
  - **2011 jan-set: 1.245.478 *e-mails***



- ***Feeds* de ataques partindo de redes brasileiras (Honeypots Distribuídos do CERT.br, Team Cymru, Arbor Atlas, ShadowServer, Operações Anti-*Botnets*)**

Agrupados e enviados aos donos das redes, com dicas para identificação e recuperação

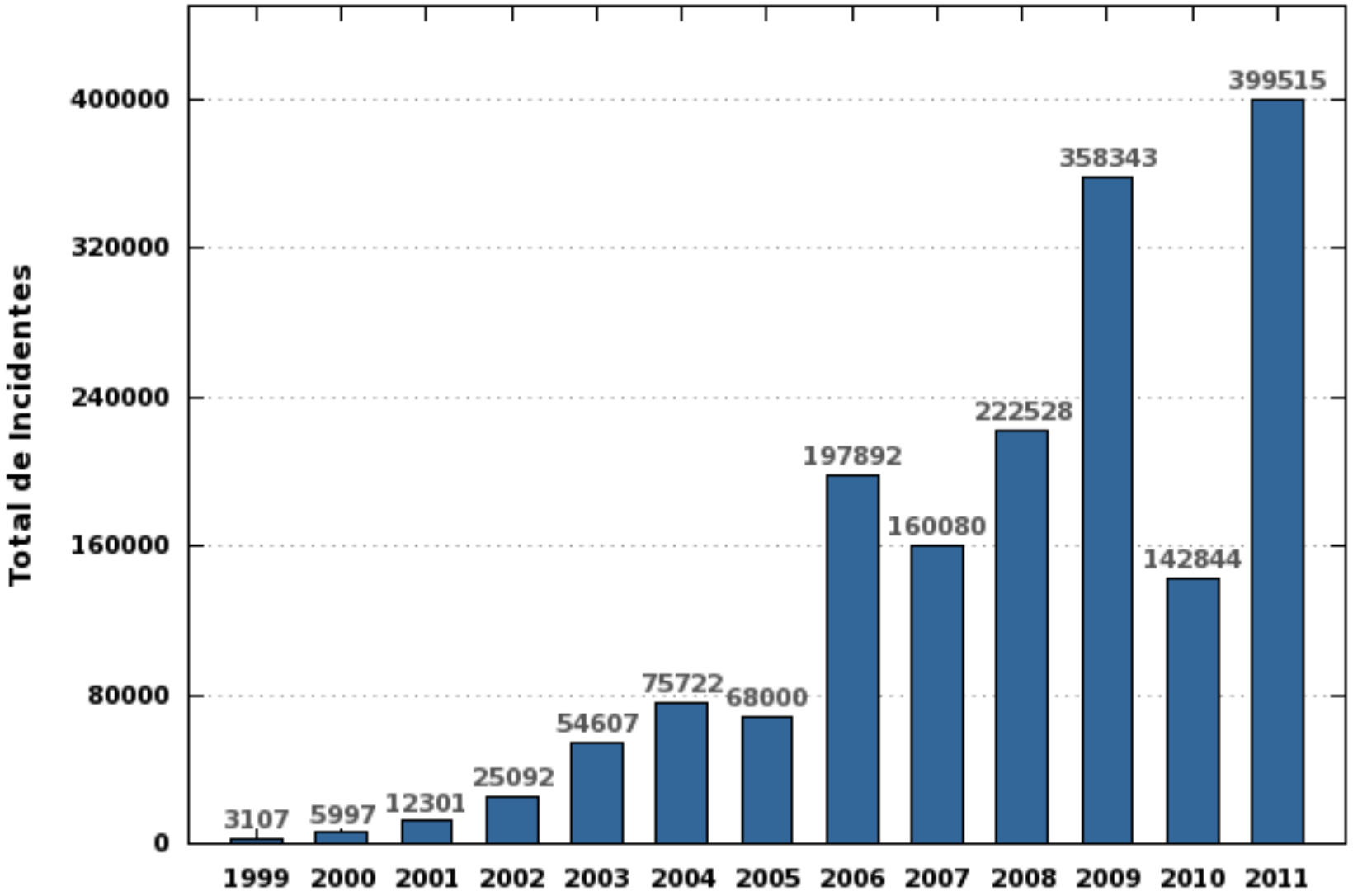
- **Reclamações de *Spams* que saem das redes Brasileiras - são a fonte das estatísticas de *spam* no Brasil**
  - **2011: 6.033.678 reclamações**



- **Monitoração de**
  - **Canais de IRC**
  - **Desfiguração de *sites***

Identificação de novas atividades e de ataques a redes de alto valor

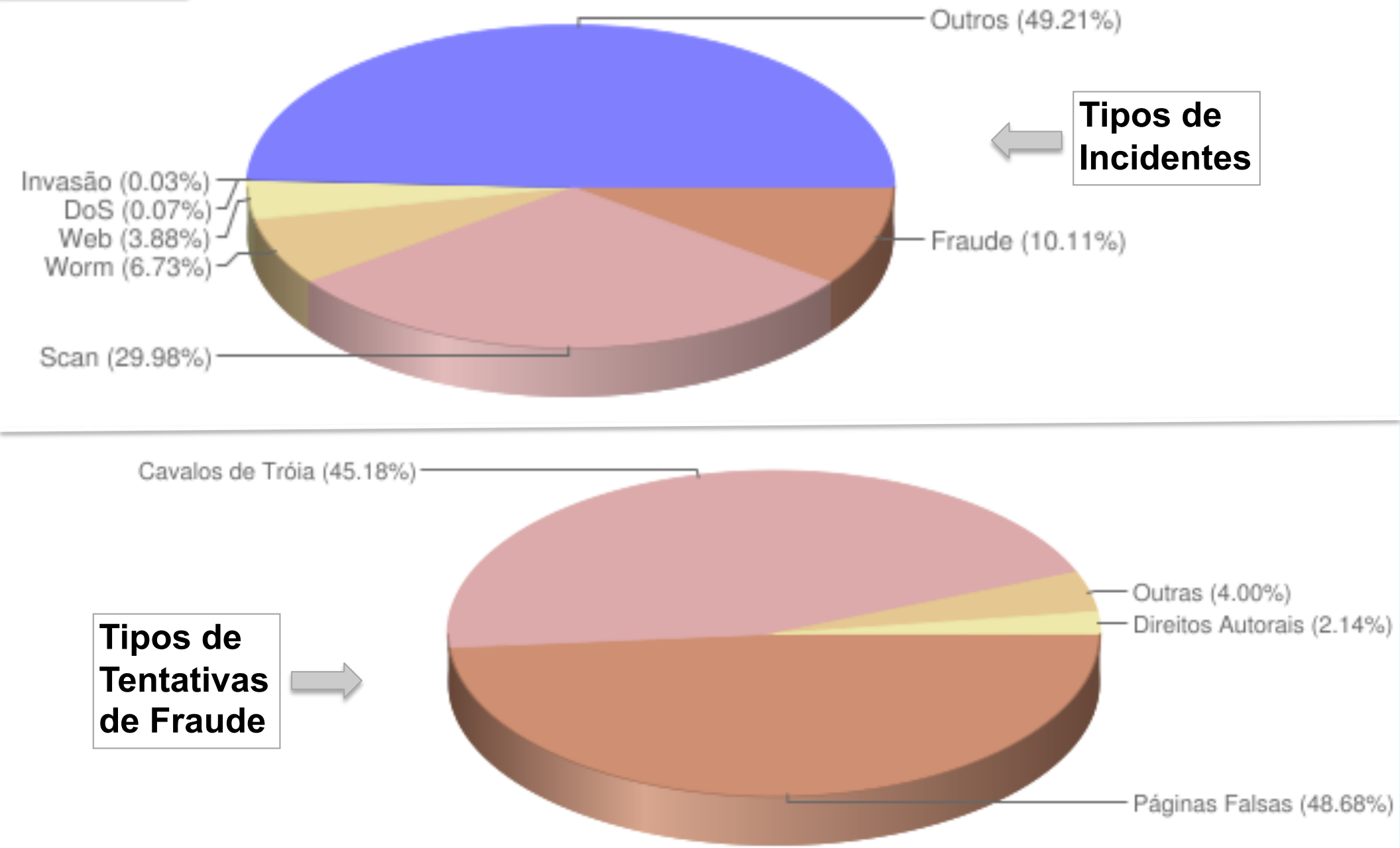
Incidentes reportados ao CERT.br – 1999-2011



Divididos em: *worms*/*bots*, ataques a servidores *web*, [D]DoS, invasões, varreduras, tentativas de fraude e outros ataques.

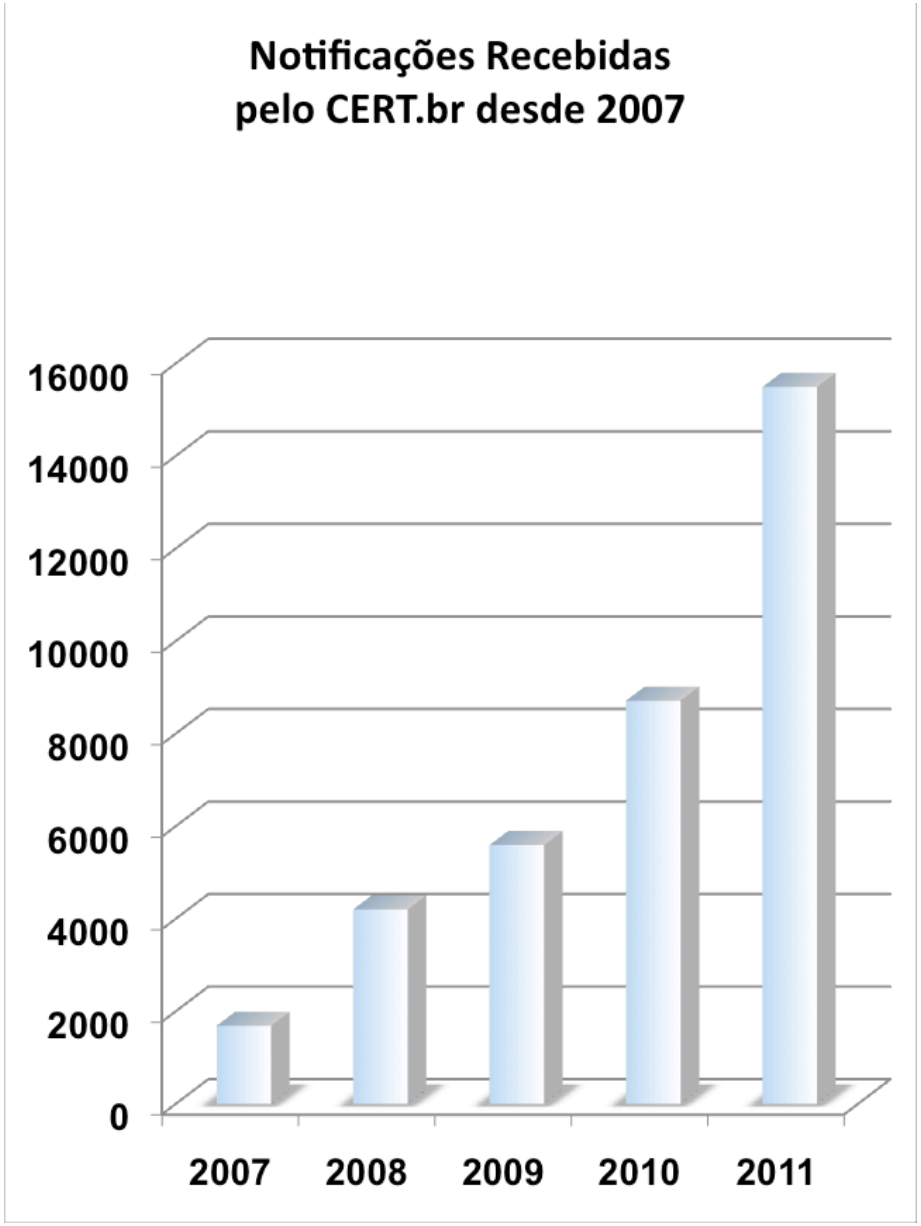
http://www.cert.br/stats/incidentes/

Incidentes por Categorias - 2011

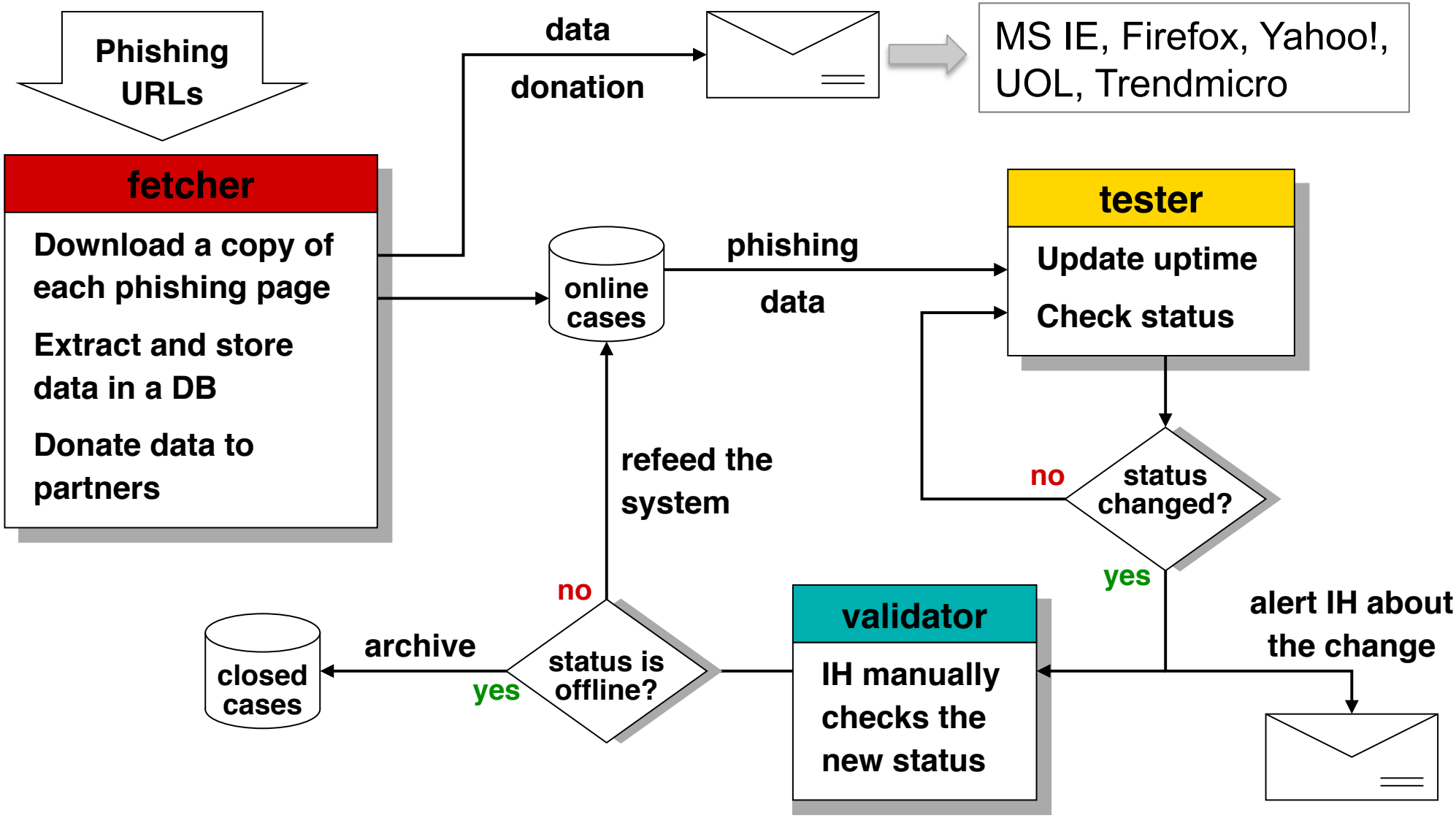


Ataques a servidores *Web*

- **A maioria das quebras de segurança nos serviços da "Web 2.0" são por falhas de programação**
  - **falta de validação de entrada**
  - **falta de checagem de erros**
- **Muitas vulnerabilidades de *Software***
  - **uso de pacotes prontos**
  - **falta de atualização dos sistemas e dos pacotes**



Sistema de Acompanhamento de *Phishings*



São tratados casos de *phishing* hospedados no Brasil e casos afetando instituições brasileiras e hospedados fora do Brasil

Estatísticas 2010 - 2011

2010

Total de casos: 7.959
URLs únicas: 7.826
SHA1s únicos: 3.609

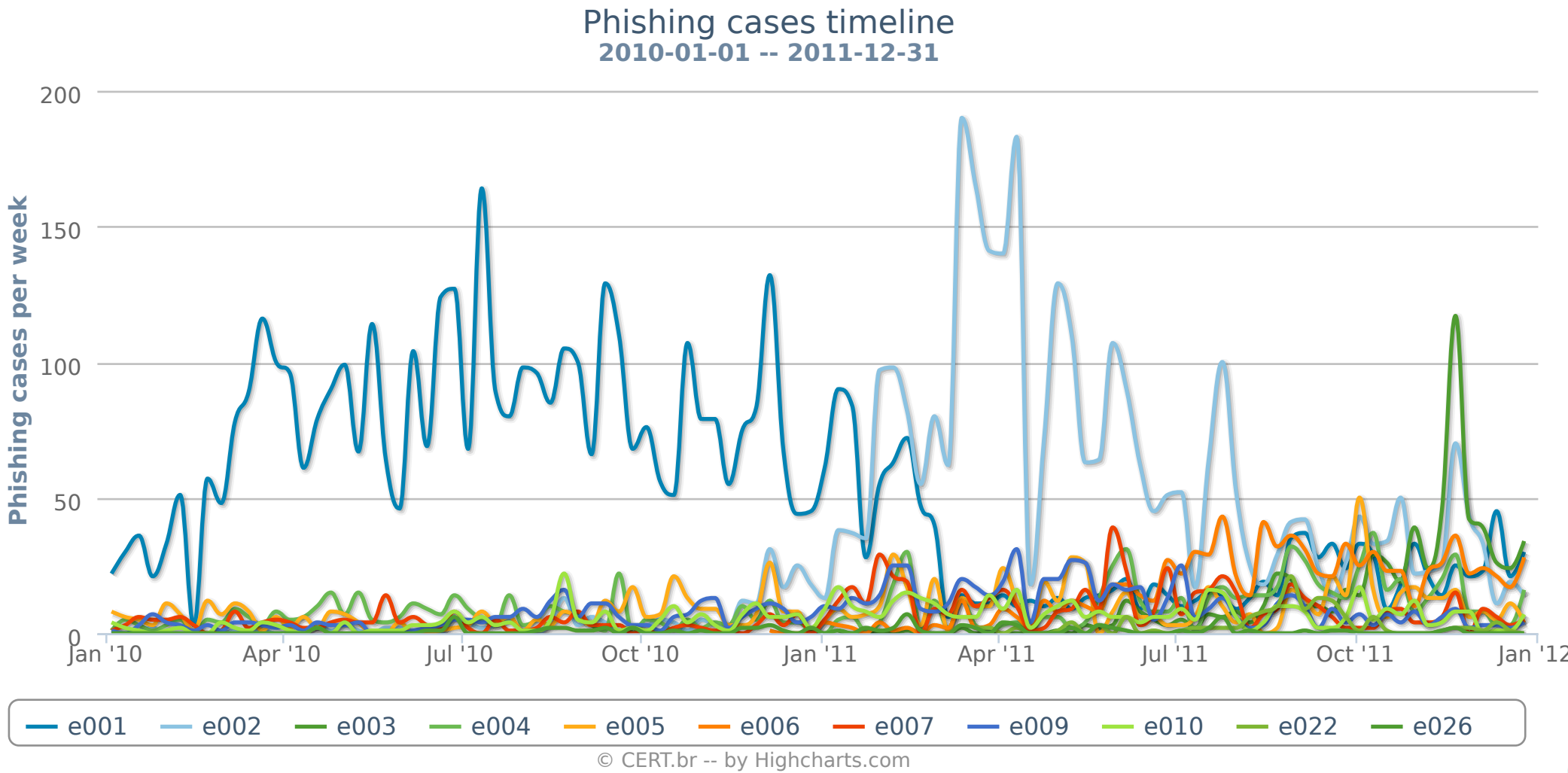
NET RESOURCES	
CCs	70
ASs	736
CIDRs	1099
IPs	3496
ccTLDs	96
gTLDs	10
notTLDs (IP)	578
Domains	4790

2011

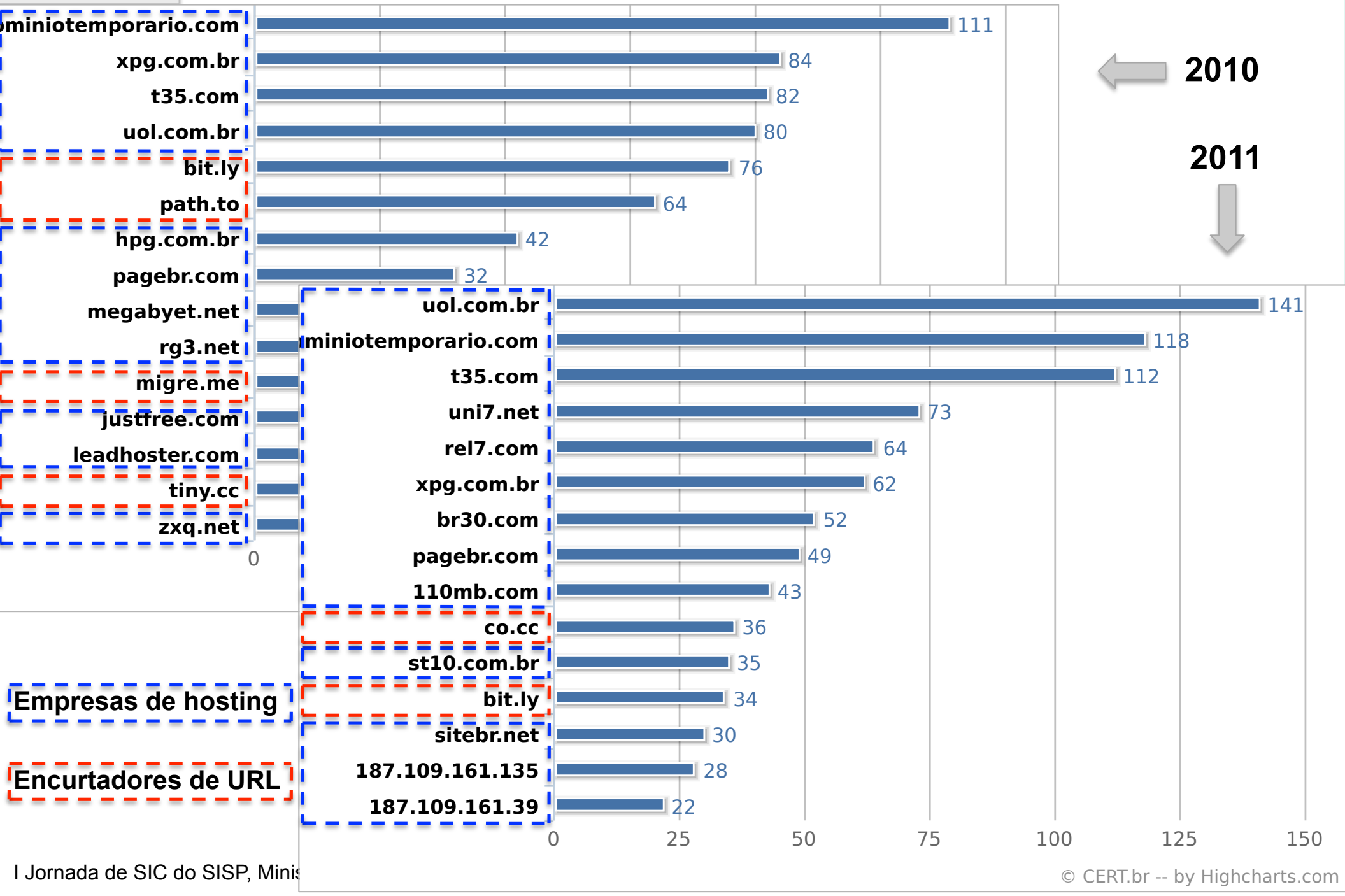
Total de casos: 12.466
URLs únicas: 12.298
SHA1s únicos: 6.330

NET RESOURCES	
CCs	85
ASs	954
CIDRs	1389
IPs	5092
ccTLDs	121
gTLDs	8
notTLDs (IP)	977
Domains	7308

Timeline 2010-2011 - Organizações Brasileiras

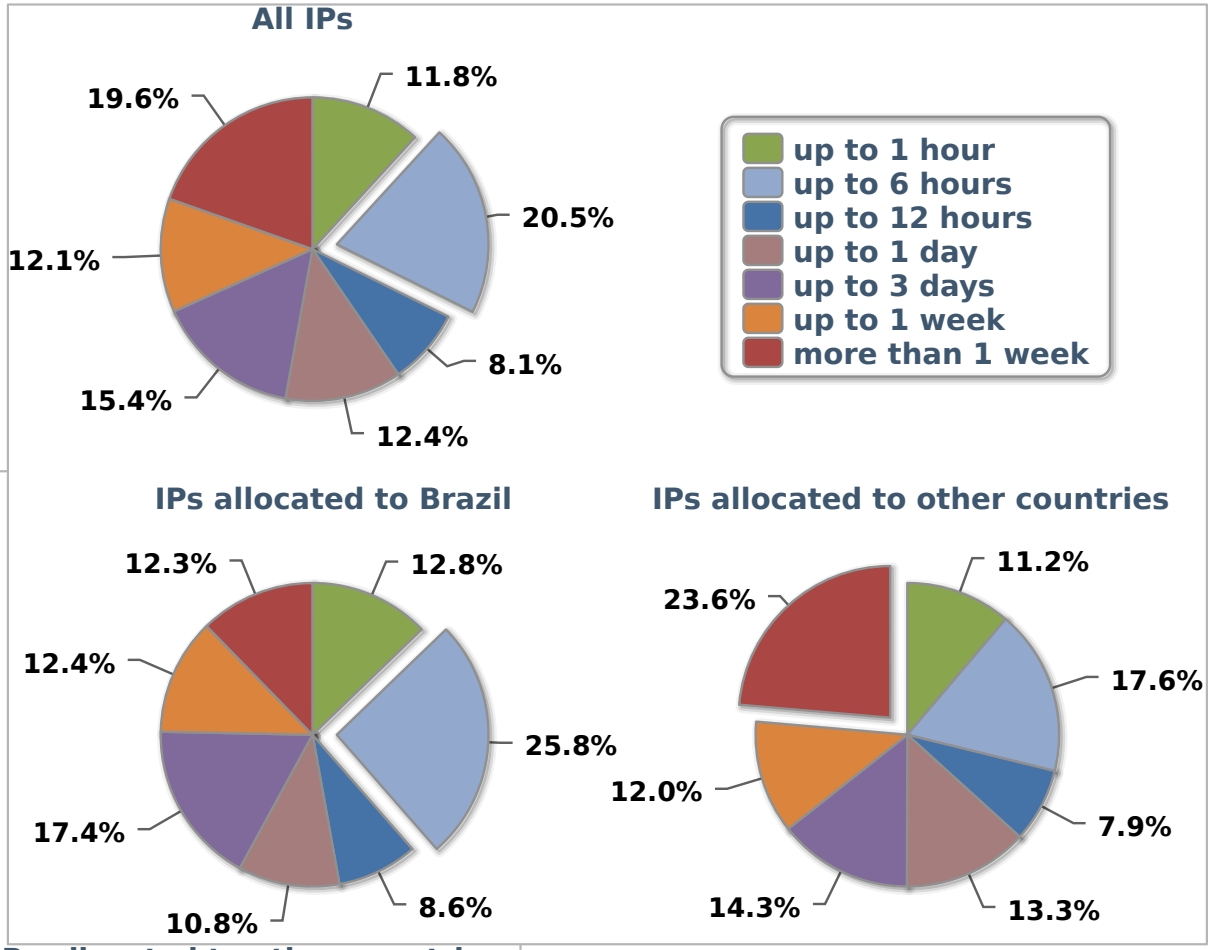


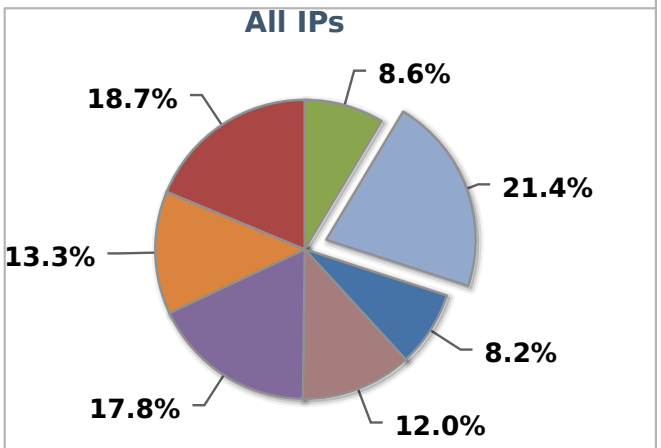
Domínios Onde as Páginas Estavam Hospedadas

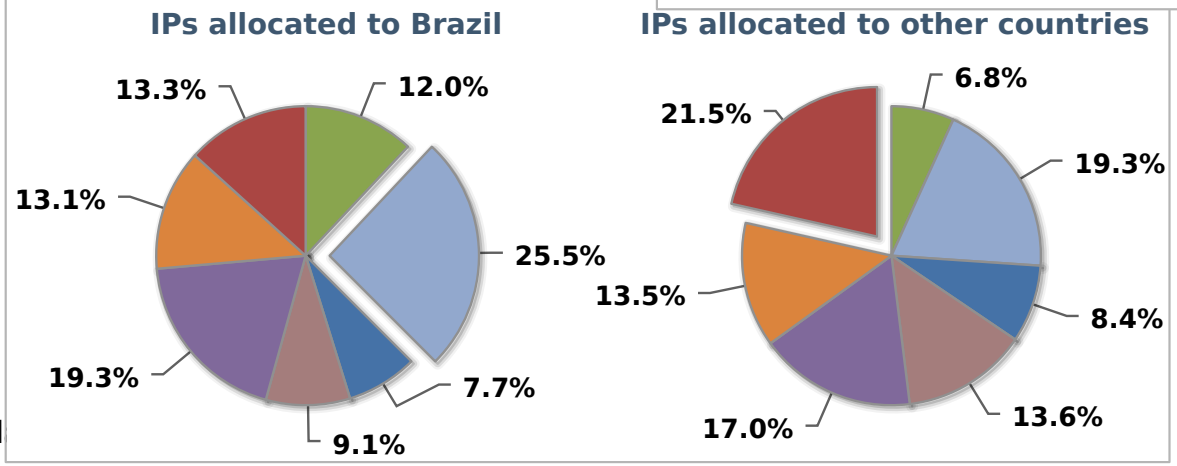


Uptime Médio no Ar das Páginas de *Phishing*

2010

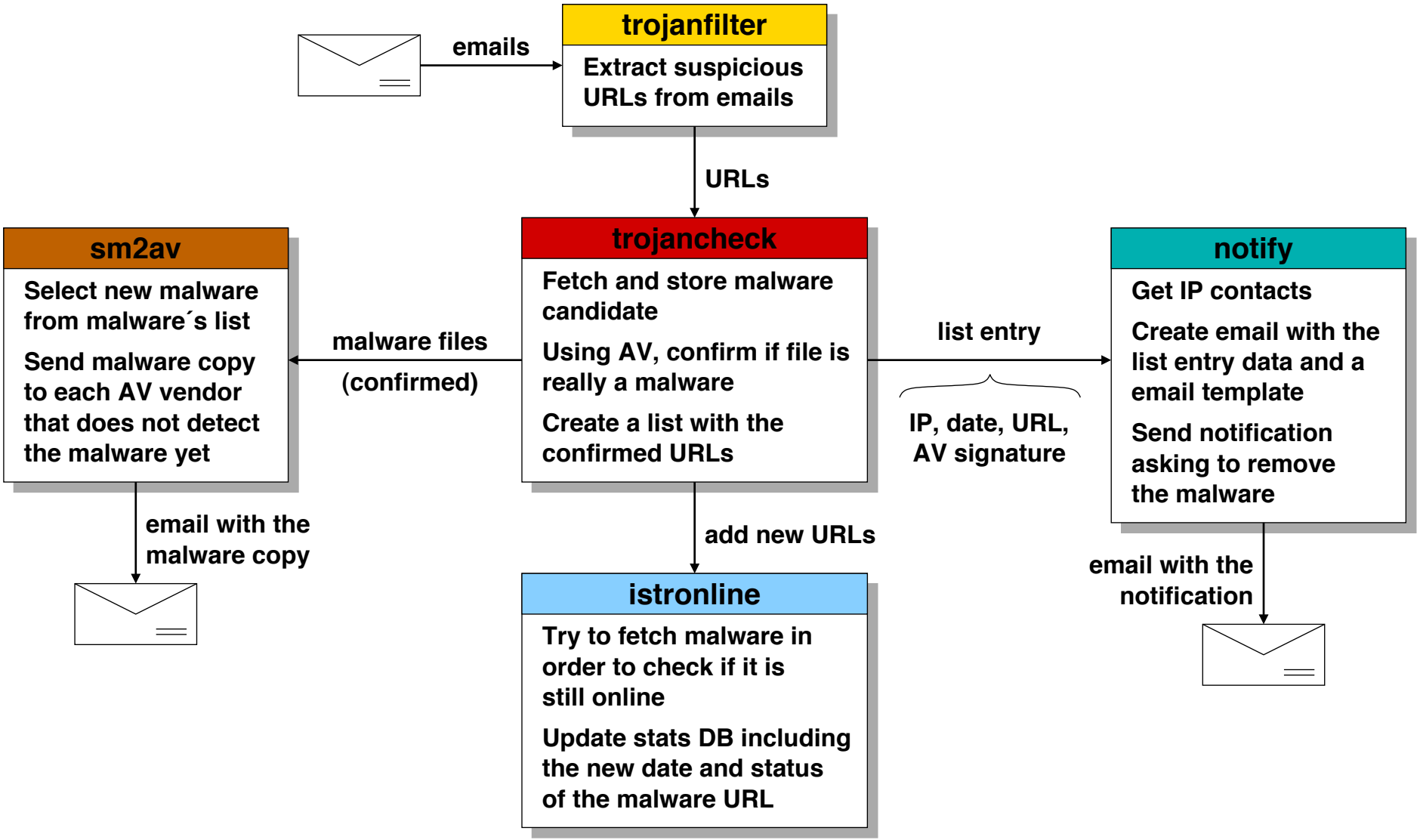






2011

Sistema de Acompanhamento de *Malware*

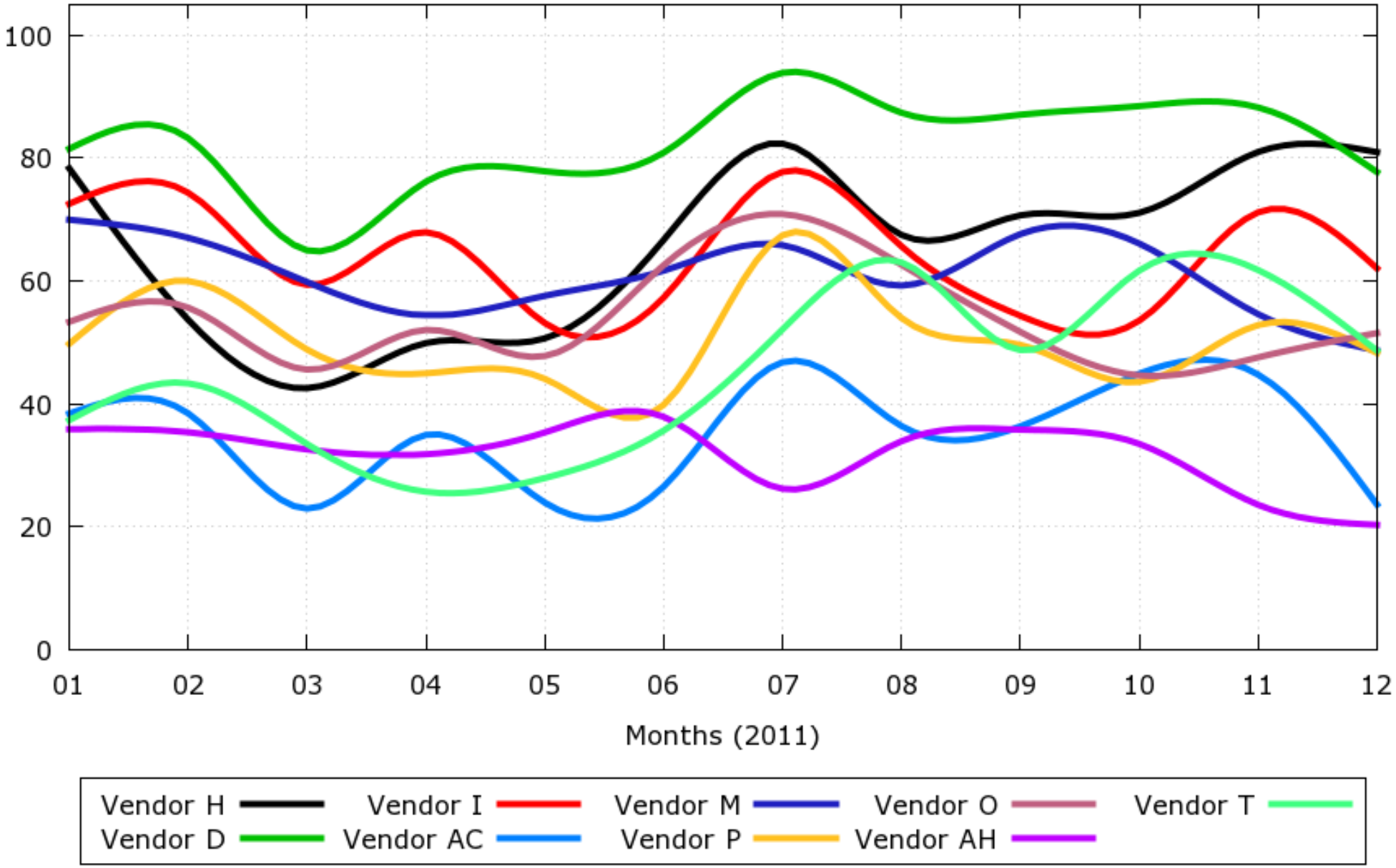


Trata apenas códigos maliciosos que afetam instituições Brasileiras
Não inclui *bots*, *worms* e vírus

Estatísticas

	2006	2007	2008	2009	2010	2011
AntiVirus signatures (grouped by "family")	140	109	63	93	70	454
AntiVirus signatures (unique)	1988	3032	6085	4101	3355	2535
CIDRs	1498	1687	1569	1335	1022	1019
Contacts for the domains/networks	2143	2205	1937	1642	1317	1316
Domains	5594	7857	5915	4447	3317	2818
Email notifications sent by CERT.br	18839	17483	15499	9935	7099	7308
File Extensions	72	112	111	100	65	54
Hosts	9671	10870	9715	6246	4509	3852
IP Addresses	3859	4415	3921	3233	2553	2512
IP Allocation's Country Codes	74	84	79	76	72	73
Protocols	3	3	2	3	3	2
Trojans' file names	10155	9812	8297	5772	3828	3033
URLs notified by CERT.br	33191	24732	21468	12877	10181	11856
Unique URLs	25087	19981	17376	10864	7298	6186
Unique trojan samples (unique hashes)	19148	16946	14256	8151	5333	4162

Eficiência dos Antivírus – 2011 (momento da descoberta)

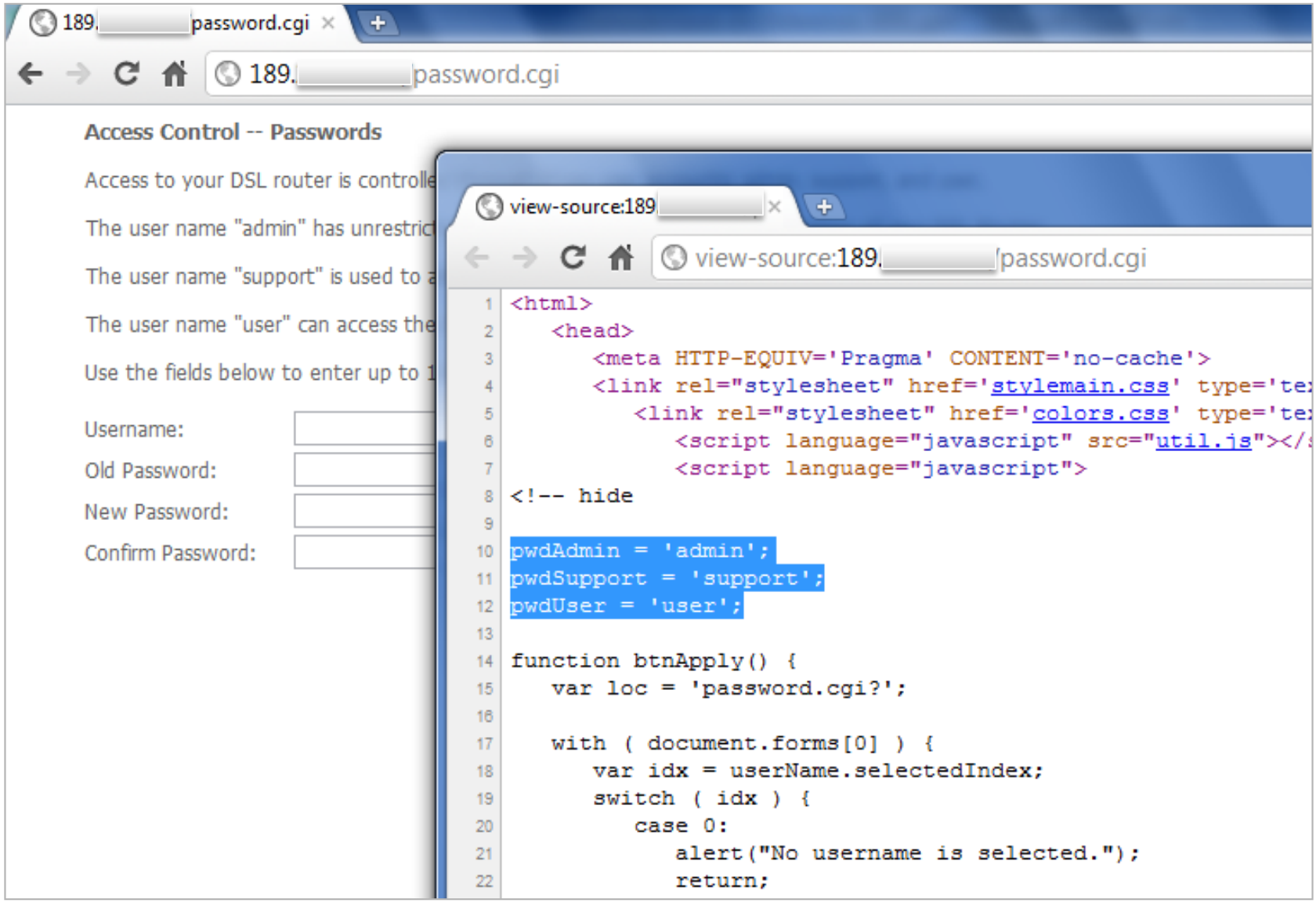


Fraude Financeira via Uso de *Malware*, Comprometimento de Modems ADSL e Uso de Páginas Falsas em Conjunto

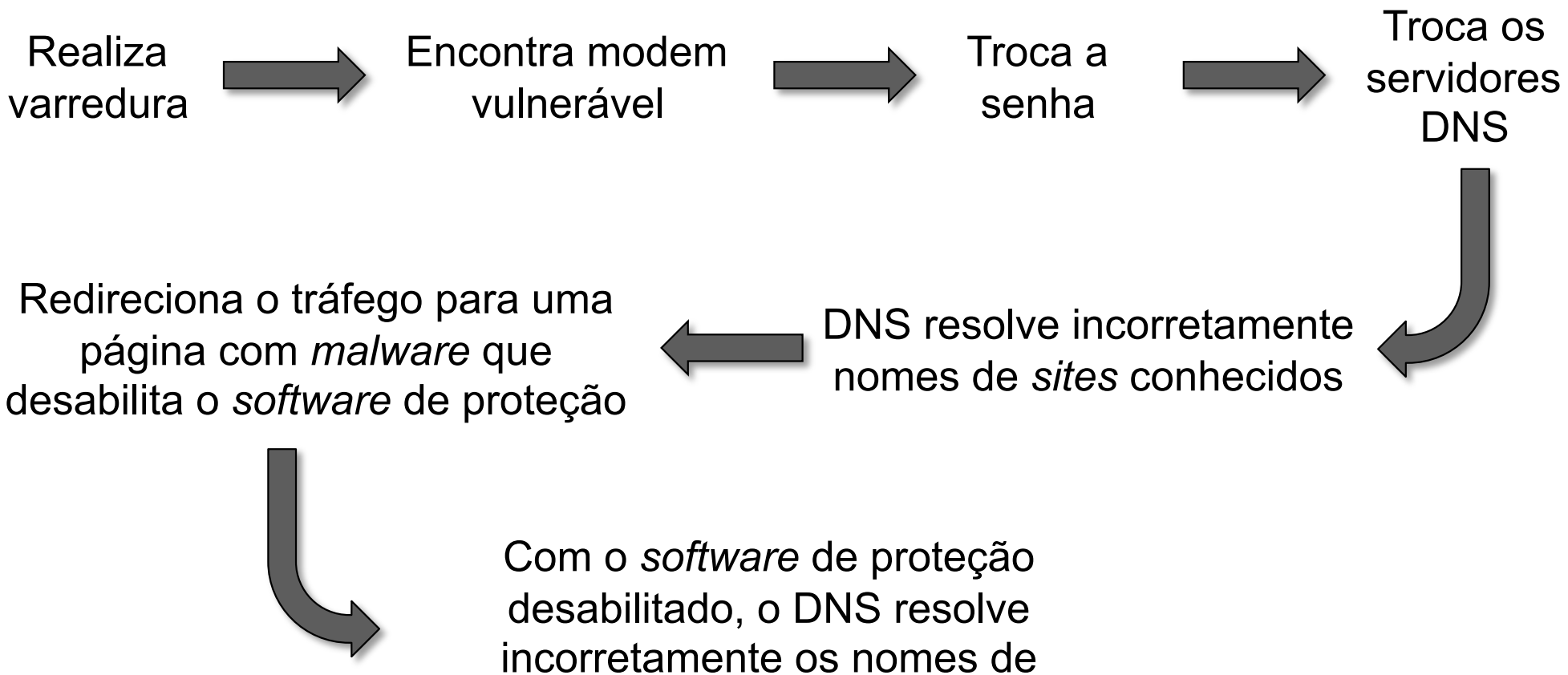
- **Afeta modems ADSL**
  - **senha de administração exposta via a interface web de gerência**
  - **modem permite administração via WAN**
  - **os modems afetados usam o mesmo *chipset***
  - **a falha era corrigida e reintroduzida em novas versões de *firmware***

- **A falha em si é antiga**

Senha Visível via Interface Web



Como Funciona o Ataque



Estatísticas do Segundo Semestre de 2011


US
96%


China
2%


Ukrain
2%

40 servidores DNS maliciosos detectados

Janeiro de 2012: mais de 300 mil modems ainda infectados

Ataques Ainda Ocorrem (*logs de honeypots*)

```
# fornece a senha antiga "pwdOld", a nova senha "pwNew"
# e uma confirmação "pwCfm"

T 2012/03/20 05:34:21.727864 208.115.204.2:36710 -> x.x.x.226:80
POST /password.cgi?usrPassword=dnschange HTTP/1.1..
Content-Type: application/x-www-form-urlencoded....
userName=3&pwdOld=user&pwNew=dnschange&pwCfm=dnschange


# POST /dnscfg.cgi
# define dois servidores DNS x.x.x.86 e x.x.x.191

T 2012/03/21 16:46:52.767176 69.65.43.74:34763 -> x.x.x.69:80
POST /dnscfg.cgi HTTP/1.1..Authorization: Basic YWRtaW46YWRtaW4=..
Content-Type: application/x-www-form-urlencoded....
dnsPrimary=x.x.x.86&dnsSecondary=x.x.x.191
&dnsDynamic=0&dnsRefresh=0
```

Outras Iniciativas do NIC.br

Proteção da Infra-Estrutura Crítica de Internet

- **Manutenção da Hora Oficial do Brasil para sincronia de tempo em computadores – NTP.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`, `leg.br` e `.b.br` só permitem domínios com DNSSEC**
- **Uso de PKI na infra-estrutura de BGP**
  - **Informações de rotas passam a ser assinadas**
  - **LACNIC está fomentando 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).

"It is a well-known fact that no other section of the population avail themselves more readily and speedily of the latest triumphs of science than the criminal class."

Inspector John Bonfield
Chicago Herald, 1888

Fonte: "*The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century's On-Line Pioneers*"
ISBN-13: 978-0802716040

Perguntas?

Cristine Hoepers

cristine@cert.br

- **CGI.br - Comitê Gestor da Internet no Brasil**
  http://www.cgi.br/
- **NIC.br - Núcleo de Informação e Coordenação do .br**
  http://www.nic.br/
- **CERT.br -Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**
  http://www.cert.br/