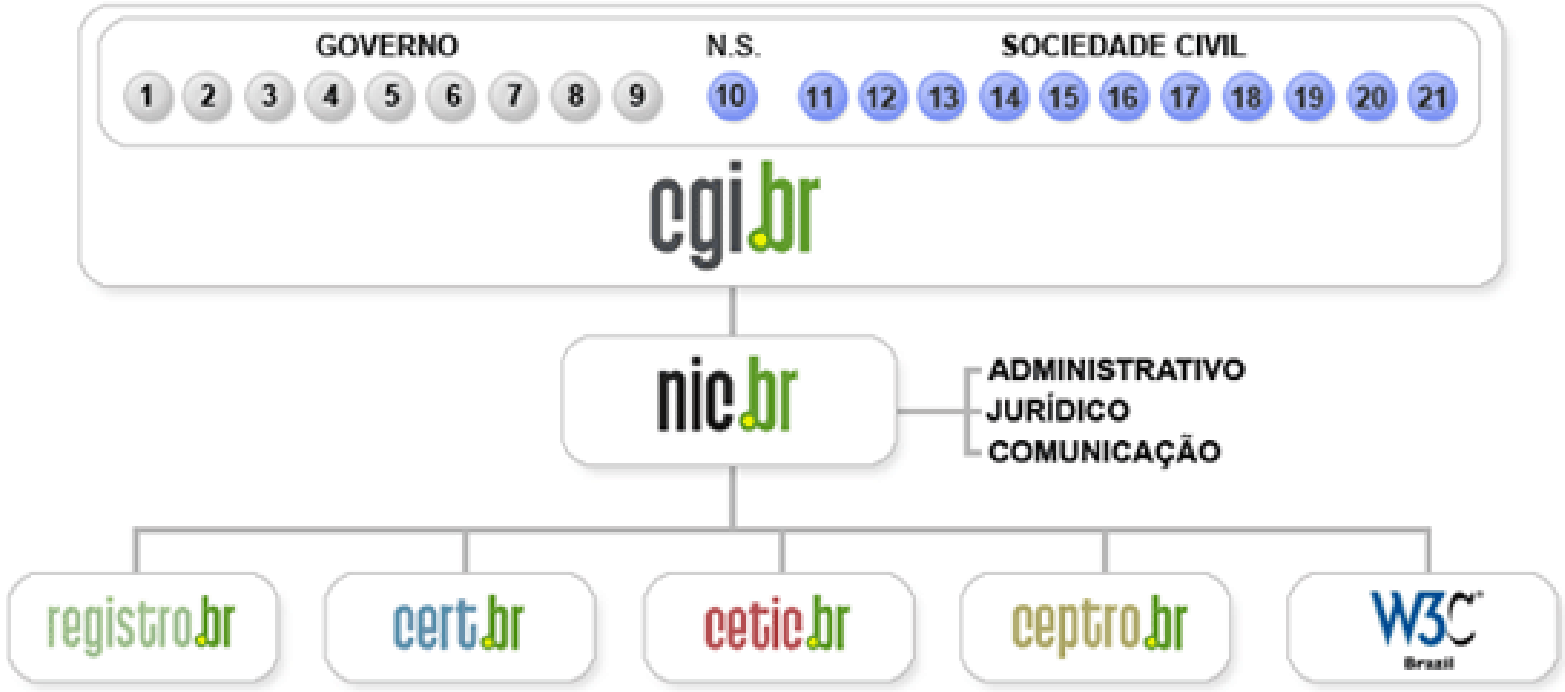
Cenário Brasileiro de Fraudes na Internet

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

Estrutura do CGI.br



01- Ministério da Ciência e Tecnologia
02- Ministério das Comunicações
03- Casa Civil da Presidência da República
04- Ministério do Planejamento, Orçamento e Gestão
05- Ministério do Desenvolvimento, Indústria e Comércio Exterior
06- Ministério da Defesa
07- Agência Nacional de Telecomunicações
08- Conselho Nacional de Desenvolvimento Científico e Tecnológico
09- Conselho Nacional de Secretários Estaduais para Assuntos de Ciência e Tecnologia

10- Notório Saber
11- Provedores de Acesso e Conteúdo
12- Provedores de Infra-estrutura de Telecomunicações
13- Indústria TICs (Tecnologia da Informação e Comunicação) e Software
14- Empresas Usuárias
15-18- Terceiro Setor
19-21- Academia

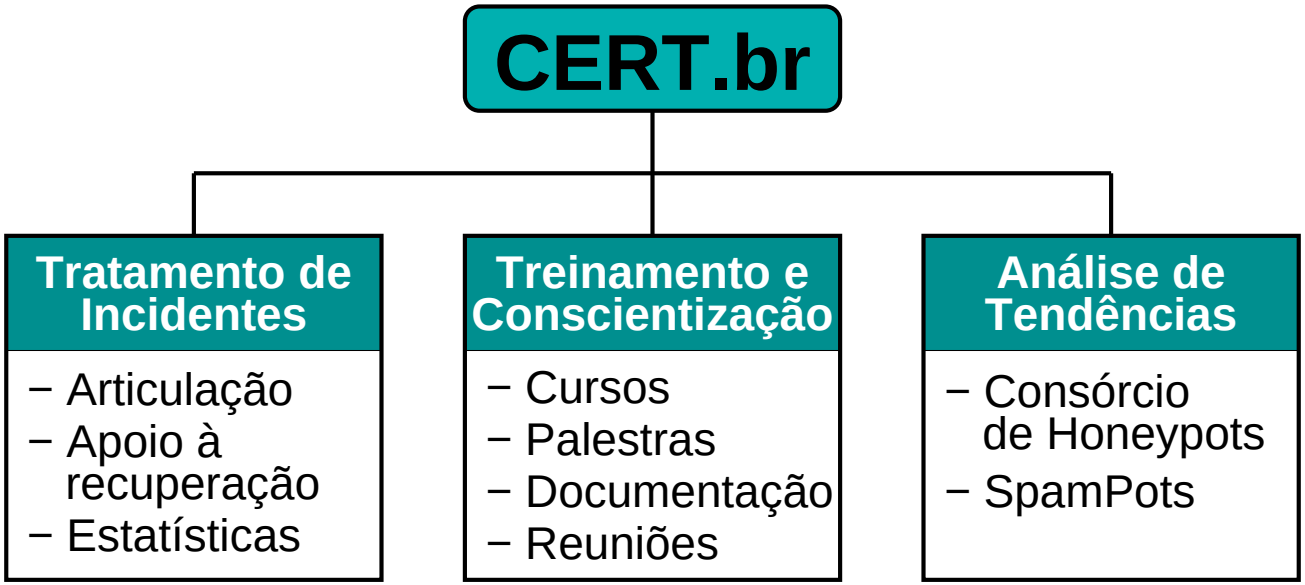
Atribuições do CGI.br

Entre as diversas atribuições e responsabilidades 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**

Sobre o CERT.br

Criado em 1997 como ponto focal para tratar incidentes de segurança relacionados com as redes conectadas à Internet no Brasil



FIRST Improving Security Together MEMBER

APWG RESEARCH PARTNER www.antiphishing.org

SEIPartner CERT Courses

The Honeynet PROJECT®

http://www.cert.br/missao.html

Agenda

Notificações Enviadas ao CERT.br

Malware
- Sistema de Notificação e Submissão de Malware
- Estatísticas de Malware

Phishing
- Sistema de Monitoramento de Páginas de Phishing
- Estatísticas de Casos de Phishing

Referências

Notificações Enviadas ao CERT.br

Categoria "Fraude" do CERT.br

Segundo Houaiss: "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro".

São classificadas como tentativa de fraude:

- Tentativas de fraude com objetivos financeiros envolvendo o uso de *malware* (Cavalos de Tróia);
- Tentativas de fraude com objetivos financeiros envolvendo o uso de *phishing* tradicional (Páginas Falsas);
- Notificações de eventuais violações de direitos autorais (Direitos Autorais).

Comparativo das Estatísticas de Fraude (1/2)

Notificações de Fraude:
(cavalos de tróia, *phishing*, quebra de direitos autorais, outros)

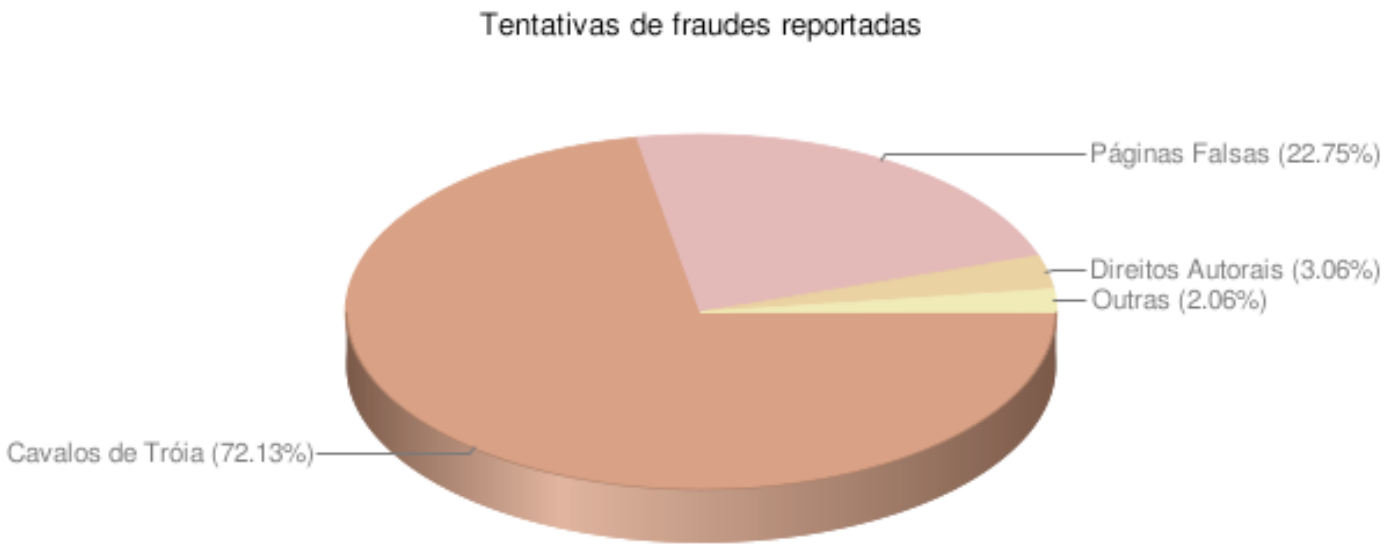
- 2009: 250.362 Q4/2009: 8.948
- 2010: 31.008 Q4/2010: 7.112

Destaques 2010:

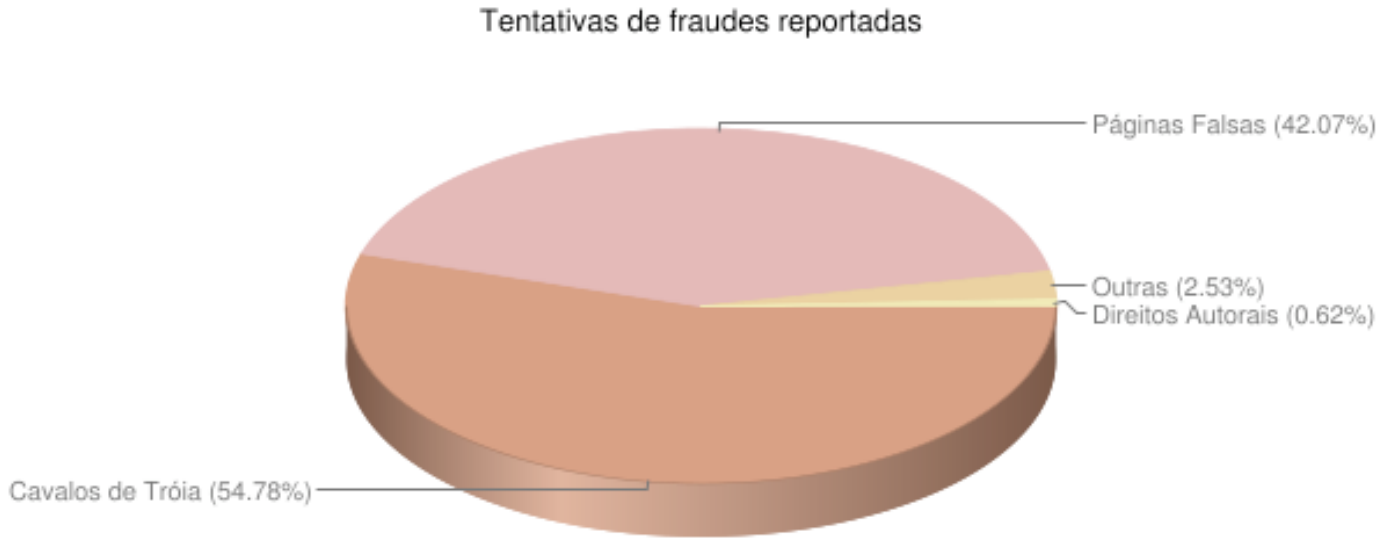
- cavalos de tróia: queda de 18% em relação a 2009
- *phishing* tradicional: aumento 94% em relação a 2009
- queda de notificações de possíveis quebras de direitos autorais levou à queda geral

Comparativo das Estatísticas de Fraude (2/2)

Q4/2009

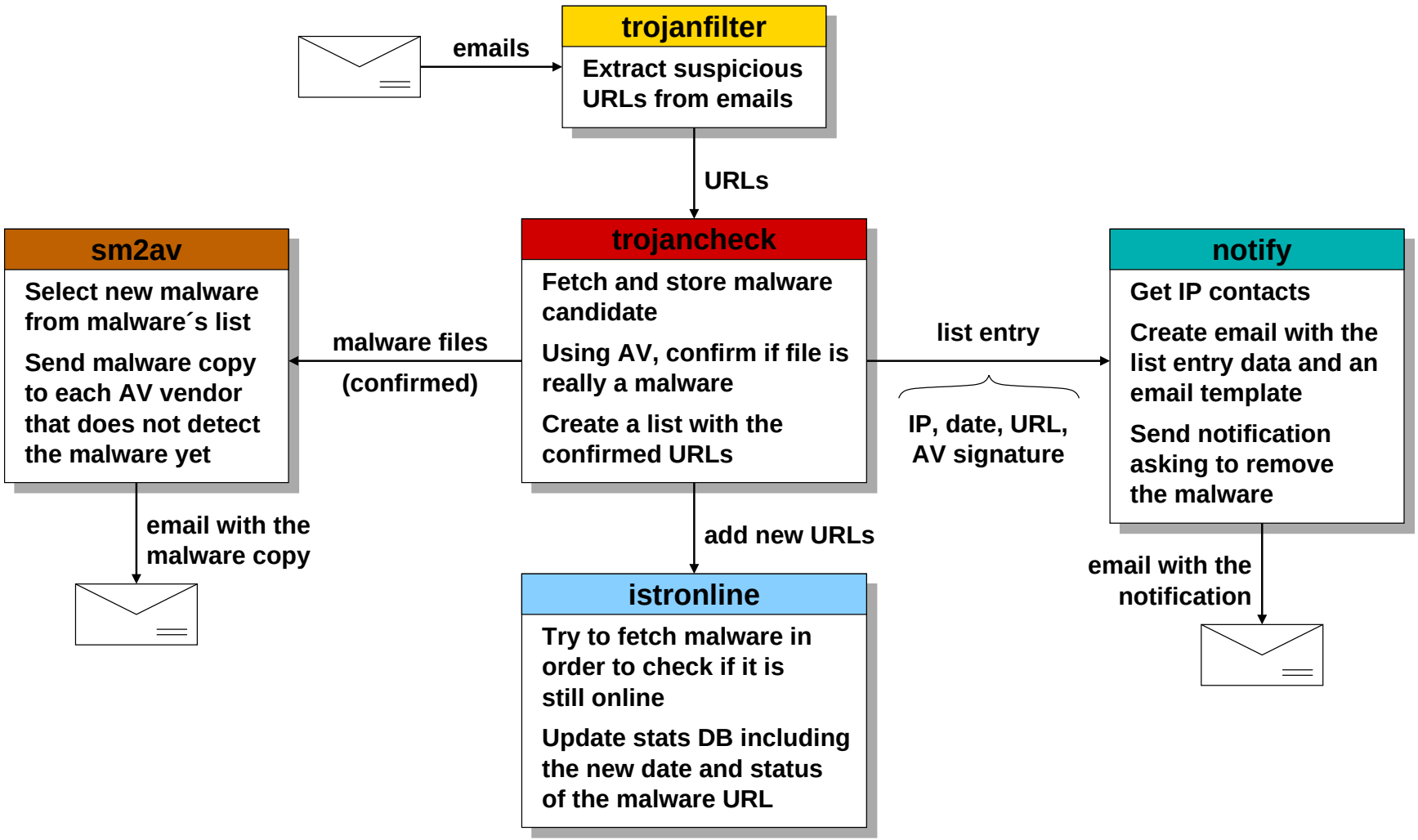


Q4/2010



Malware

Sistema de Notificação e Submissão de *Malware*

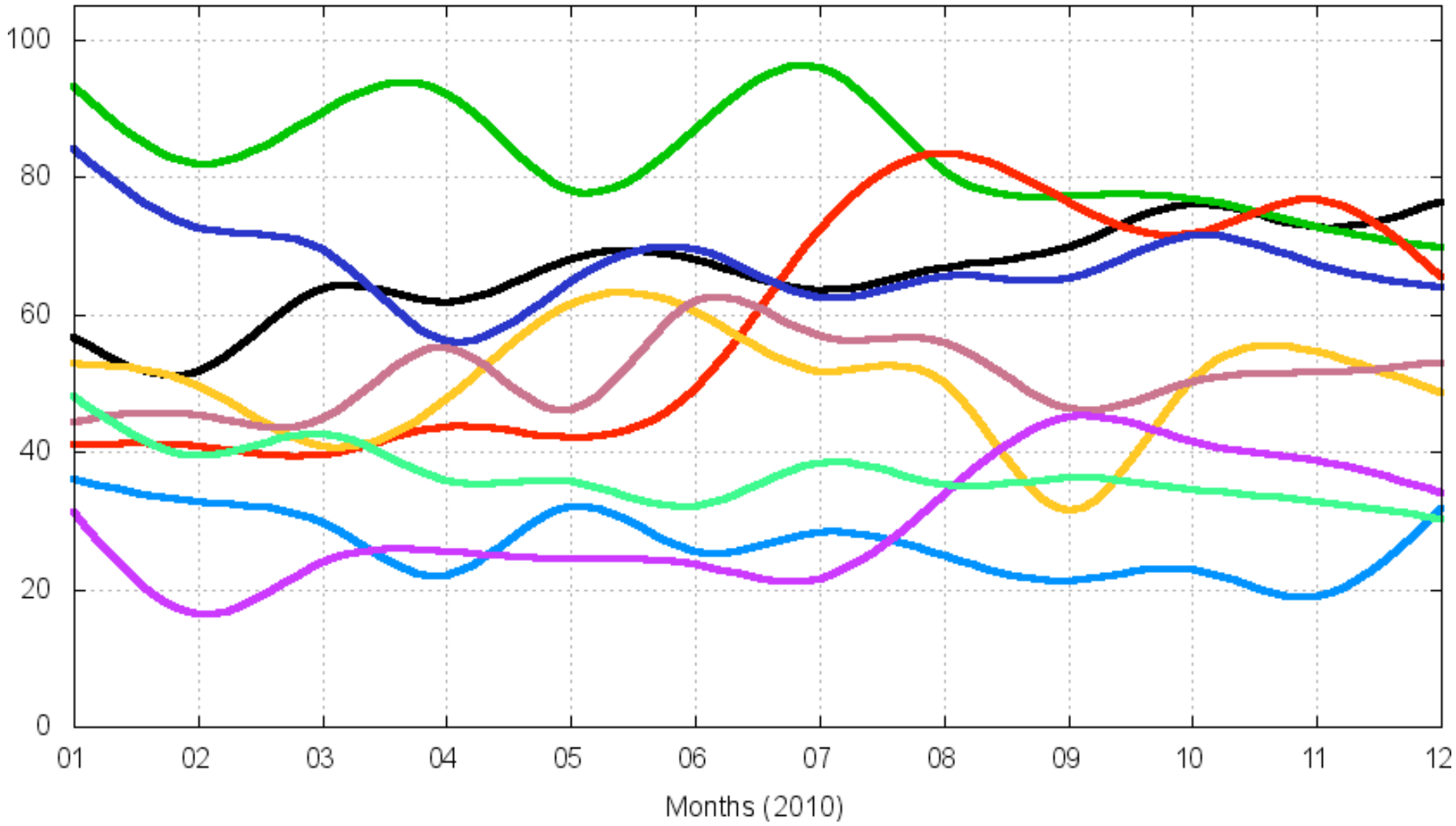


Estatísticas de *Malware*: 2007 a 2010

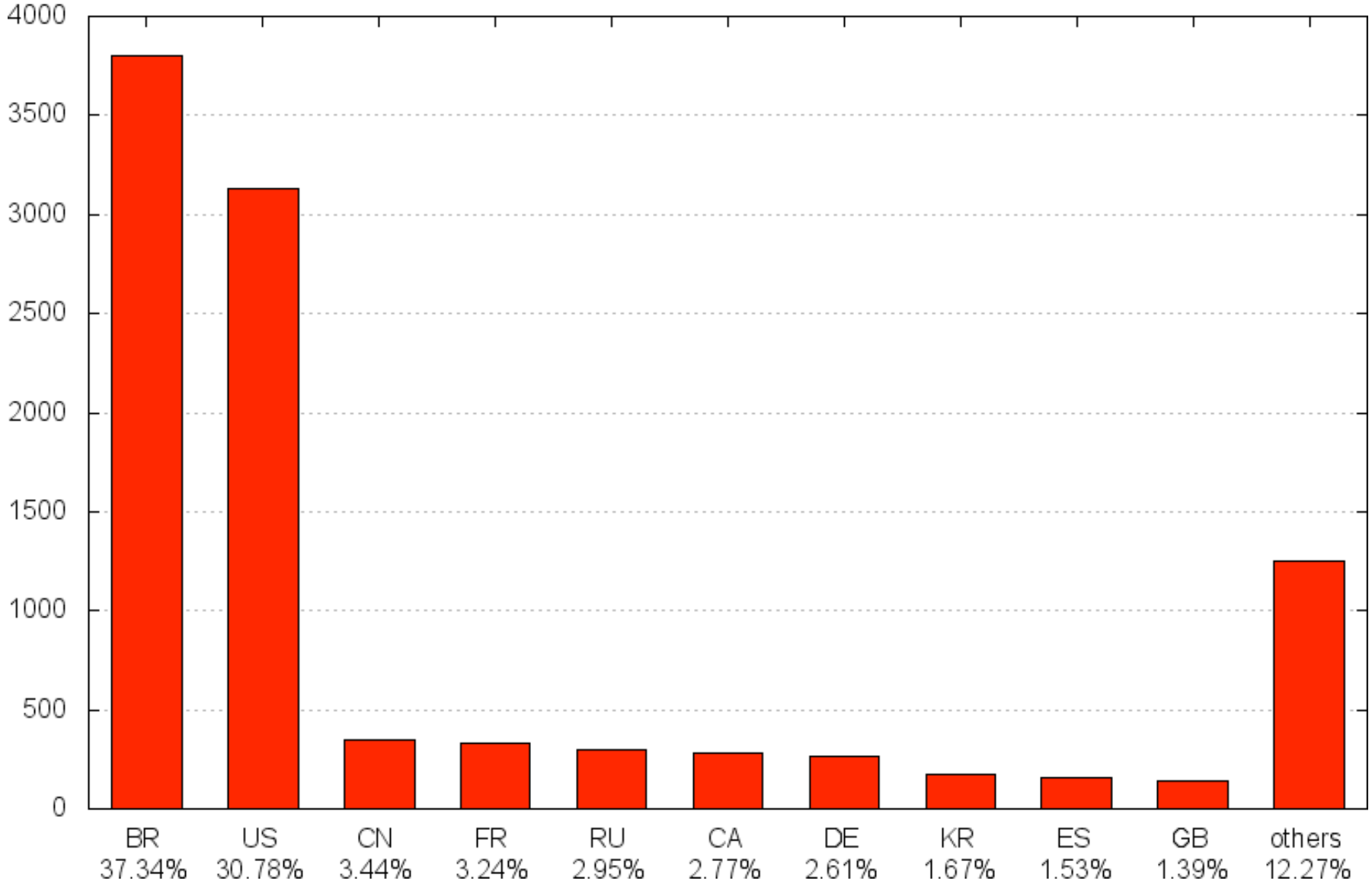
Categoria	2007	2008	2009	2010
URLs únicas	19.981	17.376	10.864	7.298
exemplares únicos (*hashes* únicos)	16.946	14.256	8.151	5.333
Assinaturas de antivírus (únicas)	3.032	6.085	4.101	3.355
Assinaturas de antivírus (“famílias”)	109	63	93	70
Extensões de arquivos	112	112	100	65
Domínios	7.795	5.916	4.447	3.317
Endereços IP	4.415	3.921	3.233	2.553
Países de Origem	83	78	76	72
Notificações enviadas pelo CERT.br	17.483	15.499	9.935	7.099

Incluem {*key*,*screen*}*loggers*, *trojan downloaders* – não incluem *bots*/*botnets* e *worms*

Eficiência dos Antivírus em 2010 - no primeiro dia

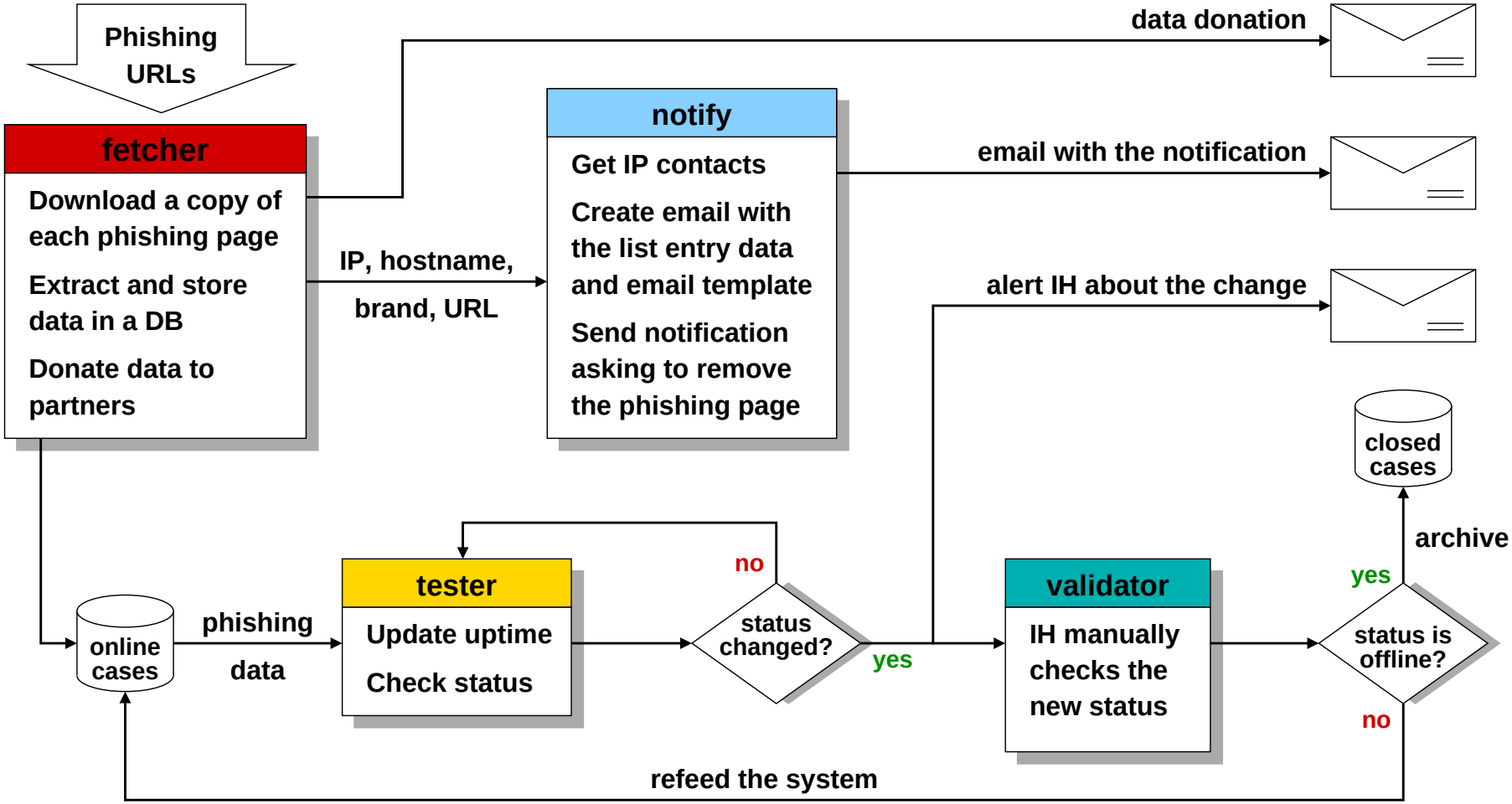


Países de Hospedagem em 2010 - de acordo com alocação do IP



Phishing

Sistema de Monitoramento de Páginas de *Phishing*



Estatísticas de Casos de *Phishing* (1/4)

Q(2,3,4)/2009

Número de casos	3266	100%
Bancos brasileiros	1868	57%
Outros alvos	1398	43%
URLs únicas	3153	
Hashes únicos	1635	
CCs	45	
ASs	356	
Domínios	1579	
Endereços IP	1313	

uptime	casos	(%)
$\leq$ 1 hora	341	10,4
$\leq$ 6 horas	752	23,0
$\leq$ 12 horas	254	7,8
$\leq$ 1 dia	354	10,8
$\leq$ 1 semana	1079	33,0
$>$ 1 semana	486	14,9

uptime (máx.)	218d 05h 26m
uptime (média)	4d 07h 16m

2010

Número de casos	7949	100%
Bancos brasileiros	5803	73%
Outros alvos	2146	27%
URLs únicas	7817	
Hashes únicos	3609	
CCs	70	
ASNs	743	
Domínios	4788	
Endereços IP	3493	

uptime	casos	(%)
$\leq$ 1 hora	939	11.8
$\leq$ 6 horas	1633	20.5
$\leq$ 12 horas	648	8.2
$\leq$ 1 dia	988	12.4
$\leq$ 1 semana	2194	27.6
$>$ 1 semana	1547	19.5

uptime (máx.)	357d 05h 30m
uptime (média)	8d 08h 41m

Estatísticas de Casos de *Phishing* (2/4)

Q(2,3,4)/2009

#	Country Code	casos	(%)
1	BR	1823	55,82
2	US	874	26,76
3	DE	81	2,48
4	PA	68	2,08
5	CA	43	1,32
6	FR	39	1,19
7	CN	38	1,16
	GB	38	1,16
9	KR	35	1,07
10	AU	25	0,77

#	ASN		casos	(%)
1	15201	(Universo Online)	564	17,22
2	27715	(LocaWeb)	395	12,06
3	8167	(Oi)	119	3,63
4	7738	(Oi)	110	3,36
5	21844	(ThePlanet)	98	2,99
6	2914	(NTT America)	86	2,63
7	7132	(AT&T)	84	2,56
8	16397	(Comdominio)	77	2,35
9	4230	(Embratel)	71	2,17
10	28299	(Cyberweb)	63	1,92

2010

#	Country Code	casos	(%)
1	BR	2838	35.70
2	US	2692	33.87
3	DE	326	4.10
4	FR	280	3.52
5	NL	183	2.30
6	RU	178	2.24
7	IT	127	1.60
8	GB	124	1.56
9	CA	121	1.52
10	CN	121	1.52

#	ASN		casos	(%)
1	15201	(Universo Online)	579	7.23
2	28299	(Cyberweb)	529	6.60
3	27715	(LocaWeb)	375	4.68
4	21844	(ThePlanet)	323	4.03
5	2914	(NTT America)	270	3.37
6	16276	(OVH)	211	2.63
7	7738	(Oi)	207	2.58
8	18479	(Plug-In)	184	2.30
9	46475	(Limestone)	184	2.30
10	26496	(GoDaddy.com)	182	2.27

Estatísticas de Casos de *Phishing* (3/4)

Q(2,3,4)/2009

#	ccTLD	casos	(%)
1	br	1142	81,28
2	de	38	2,70
3	au	25	1,78
4	fr	18	1,28
5	kr	16	1,14
6	cn	13	0,93
	ru	13	0,93
8	ws	11	0,78
9	nl	10	0,71
10	it	9	0,64
	uk	9	0,64

#	gTLD	casos	(%)
1	com	807	67,70
2	net	265	22,23
3	org	85	7,13
4	info	18	1,51
5	mobi	12	1,01
6	biz	5	0,42

2010

#	ccTLD	casos	(%)
1	br	2312	56.12
2	ru	163	3.96
3	de	161	3.91
4	tk	100	2.43
5	pl	93	2.26
6	fr	90	2.18
7	au	83	2.01
8	cn	83	2.01
9	it	82	1.99
10	nl	82	1.99

#	gTLD	casos	(%)
1	com	2147	73.55
2	net	416	14.25
3	org	251	8.60
4	info	53	1.82
5	biz	27	0.92
6	asia	9	0.31

Estatísticas de Casos de *Phishing* (4/4)

Uptime de acordo com o país onde está a instituição sendo afetada.

Período: 2010

uptime	todos		Brasil (1)		exterior (2)	
	casos	(%)	casos	(%)	casos	(%)
$\leq$ 1 hora	939	11.8	624	10.8	315	14.7
$\leq$ 6 horas	1633	20.5	1054	18.2	579	27.0
$\leq$ 12 horas	648	8.2	458	7.9	190	8.9
$\leq$ 1 dia	988	12.4	734	12.6	254	11.8
$\leq$ 1 semana	2194	27.6	1591	27.4	603	28.1
$>$ 1 semana	1547	19.5	1342	23.1	205	9.6

Obs.: Casos que afetam instituições no: (1) Brasil – (2) exterior

médias de uptime

todos	
máx.	357d 05h 30m
média	8d 08h 41m

Brasil (1)	
máx.	357d 05h 30m
média	10d 04h 12m

exterior (2)	
máx.	344d 05h 52m
média	3d 11h 00m

Todos os casos de empresas do exterior tratados pelo CERT.br são hospedados no Brasil – a média de uptime é menos da metade do tempo de todos os casos somados.

Referências

- Esta apresentação pode ser encontrada em:
  http://www.cert.br/docs/palestras/
- Comitê Gestor da Internet no Brasil – CGI.br
  http://www.cgi.br/
- Núcleo de Informação e Coordenação do Ponto br – NIC.br
  http://www.nic.br/
- Centro de Estudo, Resposta e Tratamento de Incidentes no Brasil – CERT.br
  http://www.cert.br/