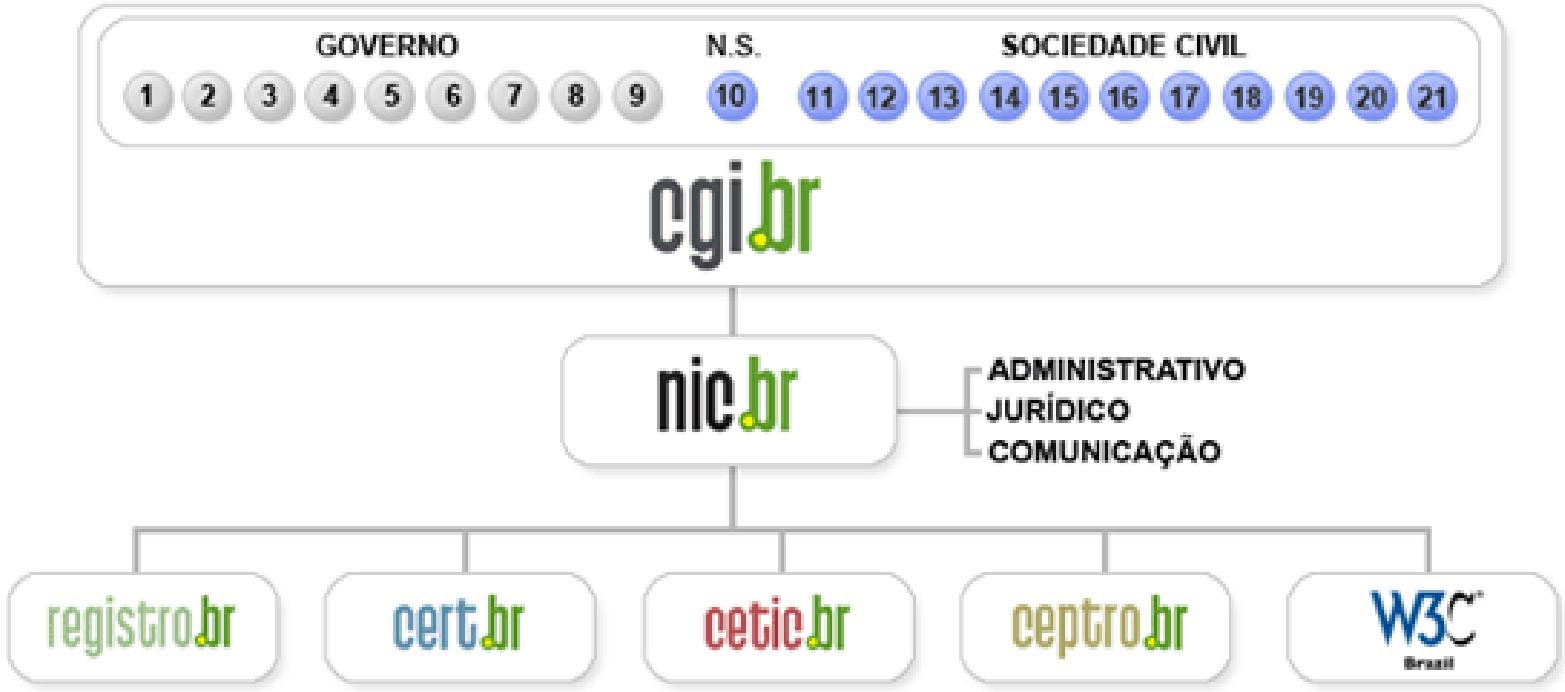
Panorama de Casos de *Phishing* Envolvendo o Brasil

Francisco J. C. Figueiredo
chicofig@cert.br
Marcelo H. P. C. Chaves
mhp@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

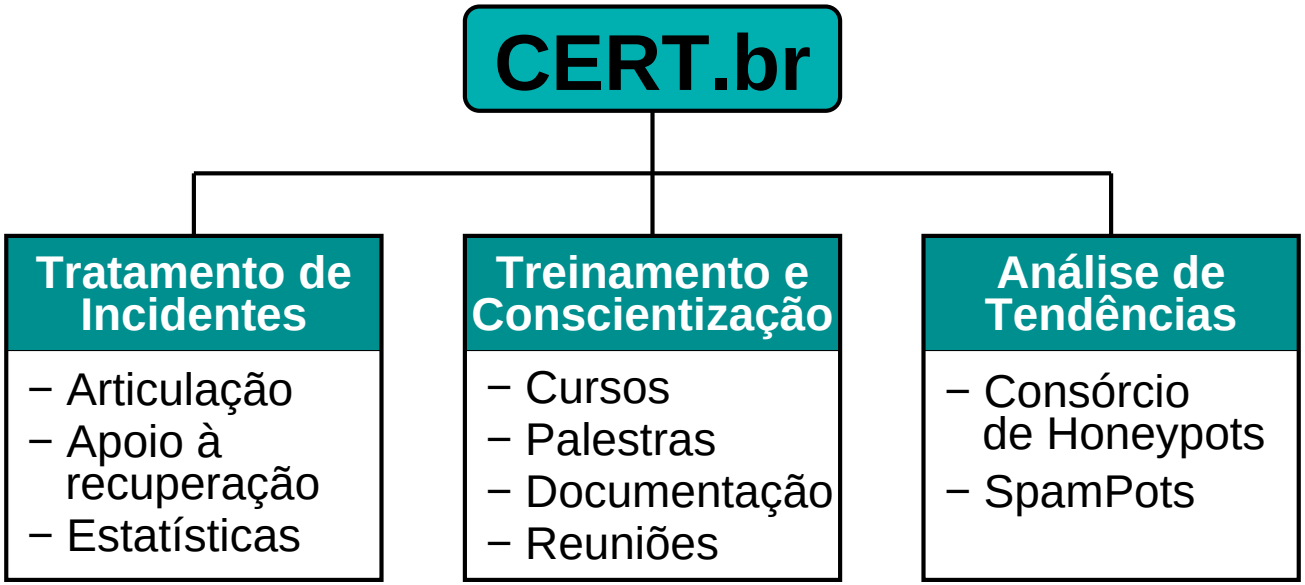
Atribuições do CGI.br

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®

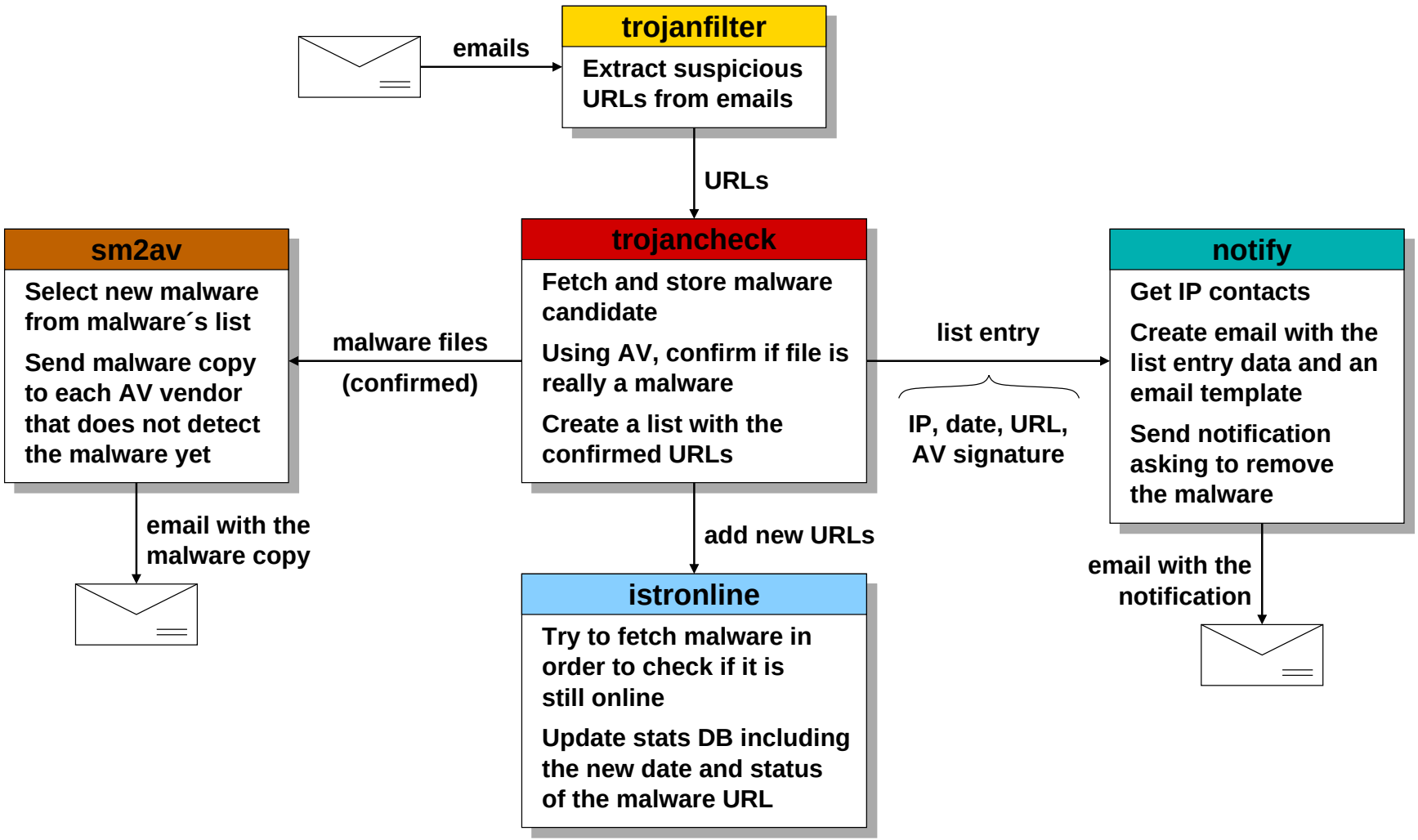
http://www.cert.br/missao.html

Agenda

- Fraude
  - Sistema de Notificação e Submissão de Malware
  - Estatísticas de Fraude
- Phishing
  - Sistema de Monitoramento de Páginas de Phishing
  - Estatísticas de Casos de Phishing
- Referências

Fraude

Sistema de Notificação e Submissão de *Malware*



Notificações de Fraude

Notificações tratadas:

2005	2006	2007	2008	2009	Q(1,2,3)/2010
27,292 (40%)	41,776 (21%)	45,298 (28%)	140,067 (62%)	250,362 (69%)	23,896 (23%)

Estatísticas de *Malware**: de 2007 a setembro de 2010

Categoria	2007	2008	2009	Q(1,2,3)/2010
URLs únicas	19,981	17,376	10,864	5,986
exemplares de *malware* únicos (*hashes* únicos)	16,946	14,256	8,151	4,382
Assinaturas de antivírus (únicas)	3,032	6,085	4,101	2,812
Assinatuas de antivírus (agrupadas por "família")	109	63	93	62
Extensões de arquivos	112	112	100	63
Domínios	7,795	5,916	4,447	2,690
Endereços IP	4,415	3,921	3,233	2,030
Países de Origem	83	78	76	66
Notificações enviadas pelo CERT.br	17,483	15,499	9,935	5,426

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

Comparativo das Estatísticas de Fraude (1/2)

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

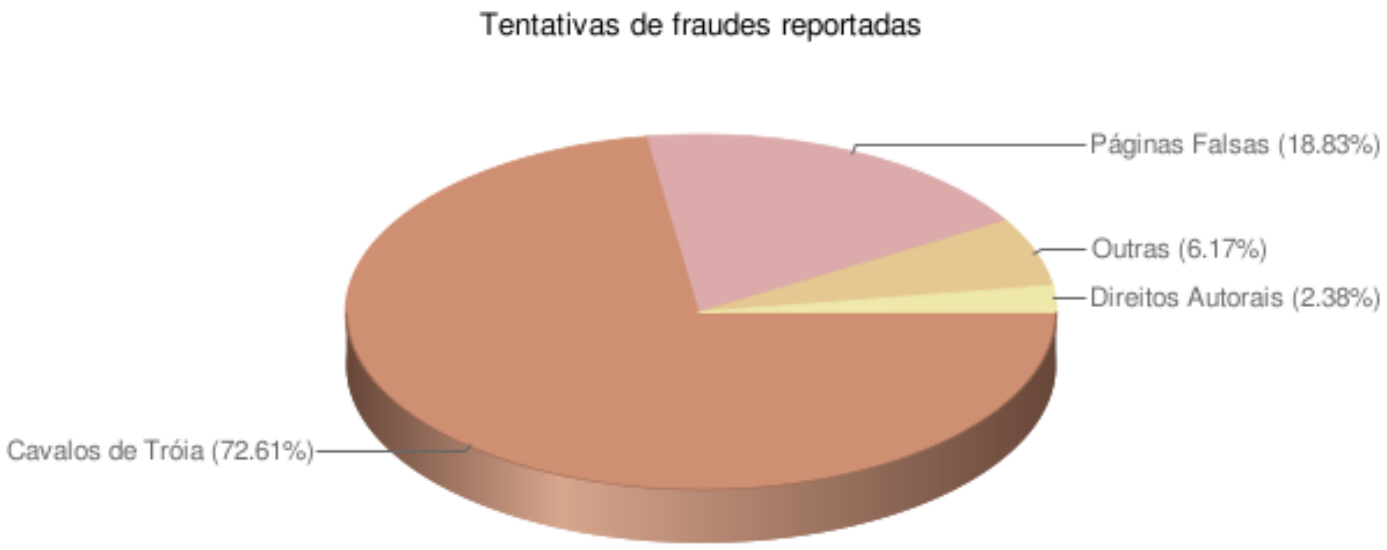
- Q3/2009: 7810
- Q3/2010: 7449

Q3/2010:

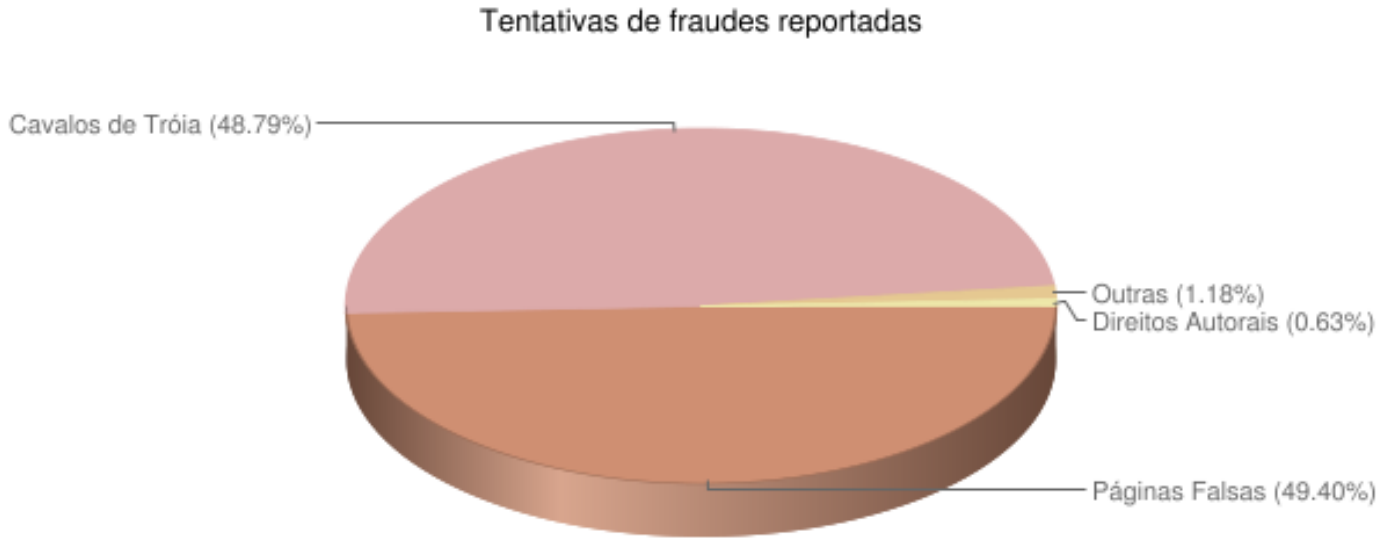
- queda de 5% em relação a Q3/2009
- queda de 7.5% em relação a Q2/2010
- aumento de 150% nos casos de *phishing* em relação a Q3/2009

Comparativo das Estatísticas de Fraude (2/2)

Q3/2009

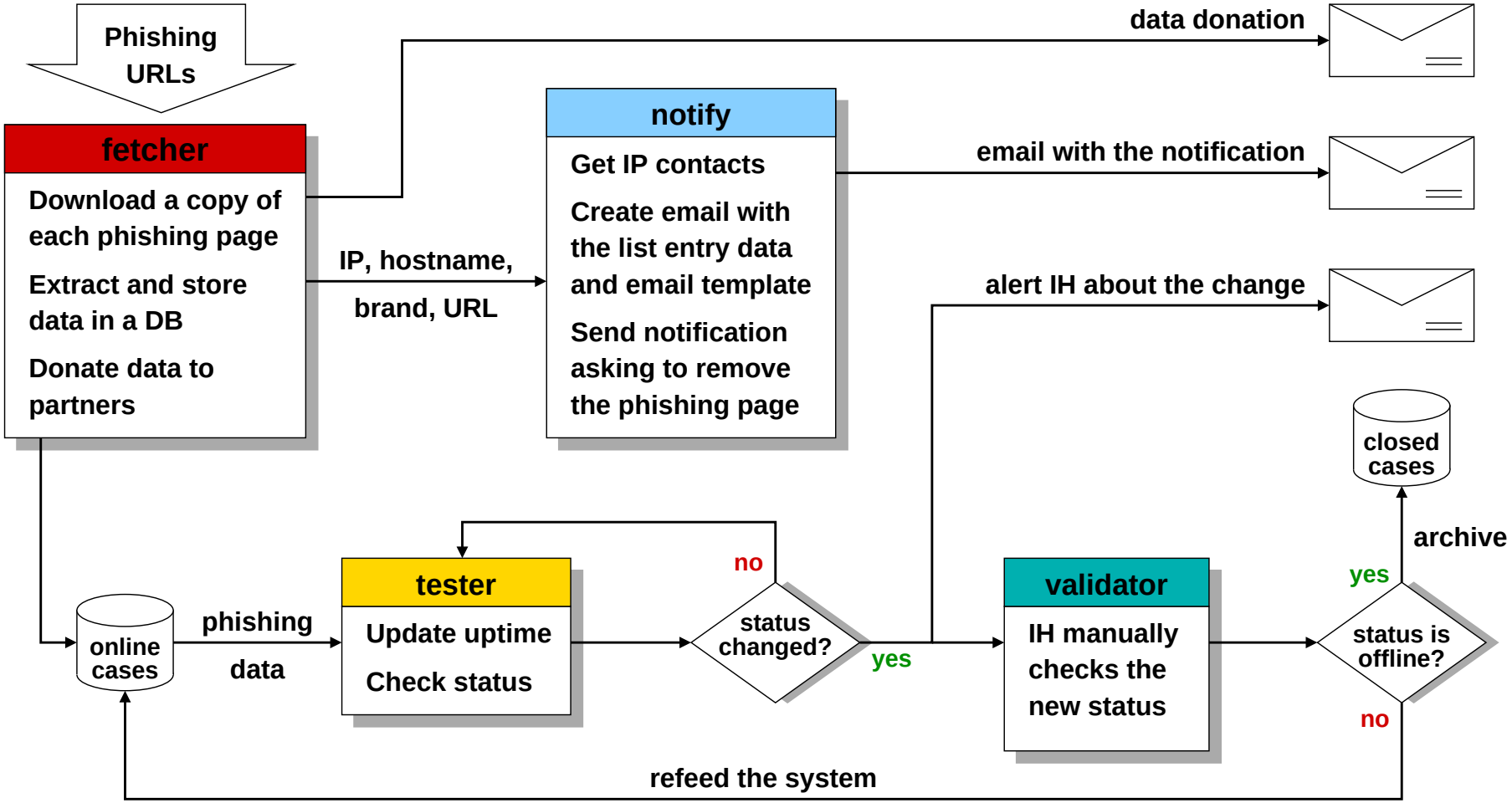


Q3/2010



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

Q(1,2,3)/2010

Número de casos	5859	100%
Bancos brasileiros	4194	72%
Outros alvos	1665	28%
URLs únicas	5764	
Hashes únicos	2681	
CCs	66	
ASs	635	
Domínios	3590	
Endereços IP	2704	

uptime	casos	(%)
$\leq$ 1 hora	710	12,1
$\leq$ 6 horas	1191	20,3
$\leq$ 12 horas	482	8,2
$\leq$ 1 dia	683	11,7
$\leq$ 1 semana	1607	27,4
$>$ 1 semana	1186	20,2

uptime (máx.)	265d 05h 30m
uptime (média)	7d 10h 40m

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

Q(1,2,3)/2010

#	Country Code	casos	(%)
1	BR	2107	35,96
2	US	2009	34,29
3	DE	242	4,13
4	FR	195	3,33
5	NL	131	2,24
6	RU	125	2,13
7	CN	105	1,79
8	IT	102	1,74
9	GB	92	1,57
10	CA	76	1,30

#	ASN		casos	(%)
1	28299	(Cyberweb)	476	8,06
2	15201	(Universo Online)	352	5,96
3	27715	(LocaWeb)	285	4,82
4	21844	(ThePlanet)	235	3,98
5	2914	(NTT America)	213	3,61
6	26496	(GoDaddy)	162	2,74
7	7738	(Oi)	146	2,47
8	46475	(Limestone)	139	2,35
9	16276	(OVH)	137	2,32
10	18479	(Plug-In)	129	2,18

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

Q(1,2,3)/2010

#	ccTLD	casos	(%)
1	br	1770	57,86
2	de	138	4,51
3	ru	116	3,79
4	cn	73	2,39
5	nl	70	2,29
6	fr	65	2,12
7	au	64	2,09
8	ly	62	2,03
9	it	60	1,96
10	to	58	1,90

#	gTLD	casos	(%)
1	com	1503	70,70
2	net	328	15,43
3	org	206	9,69
4	info	47	2,21
5	biz	22	1,03
6	asia	9	0,42
7	mobi	6	0,28

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

Período: 01/01/2010 a 20/11/2010

Categoria	todos	Brasil (1)	exterior (2)
Número de casos	6847	2451	4396
Bancos brasileiros	4955	826	4129
Outros alvos	1892	1625	267
URLs únicas	6738	2409	4332
Hashes únicos	3141	1391	1916
CCs	68	1	67
ASs	700	79	622
Domínios	4175	1296	2897
Endereços IP	3113	760	2353

uptime

todos	
máx.	316d 05h 30m
média	8d 07h 14m

Brasil (1)	
máx.	190d 05h 03m
média	4d 03h 35m

exterior (2)	
máx.	316d 05h 30m
média	10d 14h 47m

uptime	todos		Brasil (1)		exterior (2)	
	casos	(%)	casos	(%)	casos	(%)
$\leq$ 1 hora	811	11,8	316	12,9	495	11,3
$\leq$ 6 horas	1391	20,3	622	25,4	769	17,5
$\leq$ 12 horas	557	8,1	208	8,5	349	7,9
$\leq$ 1 dia	808	11,8	248	10,1	560	12,7
$\leq$ 1 semana	1886	27,5	736	30,0	1150	26,2
$>$ 1 semana	1394	20,4	321	13,1	1073	24,4

47% dos casos hospedados em IPs alocados para o Brasil saem do ar em até 12 horas, contra 37% dos casos no exterior.

Obs.: hospedados em IPs alocados para: (1) Brasil – (2) exterior

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/