Segurança da Internet 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

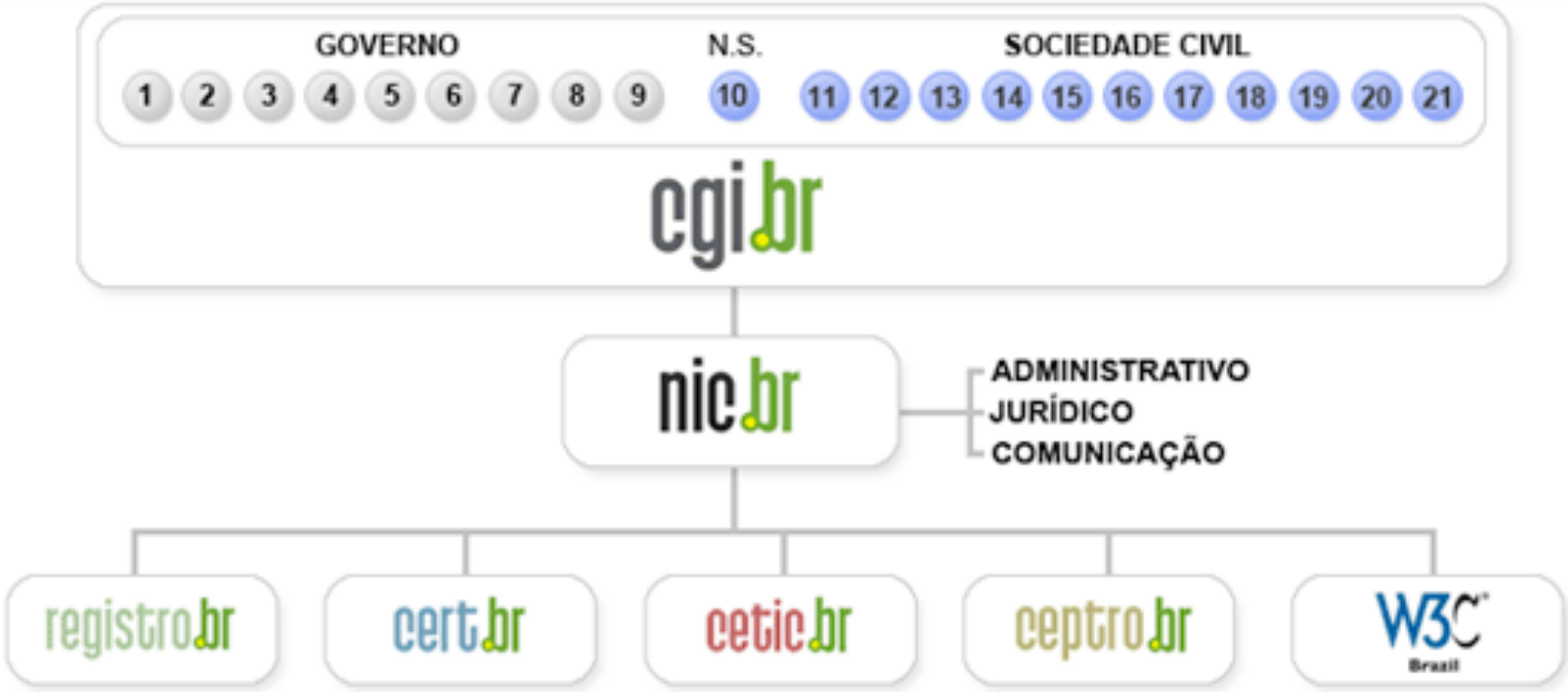
Comitê Gestor da Internet no Brasil – CGI.br

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;**

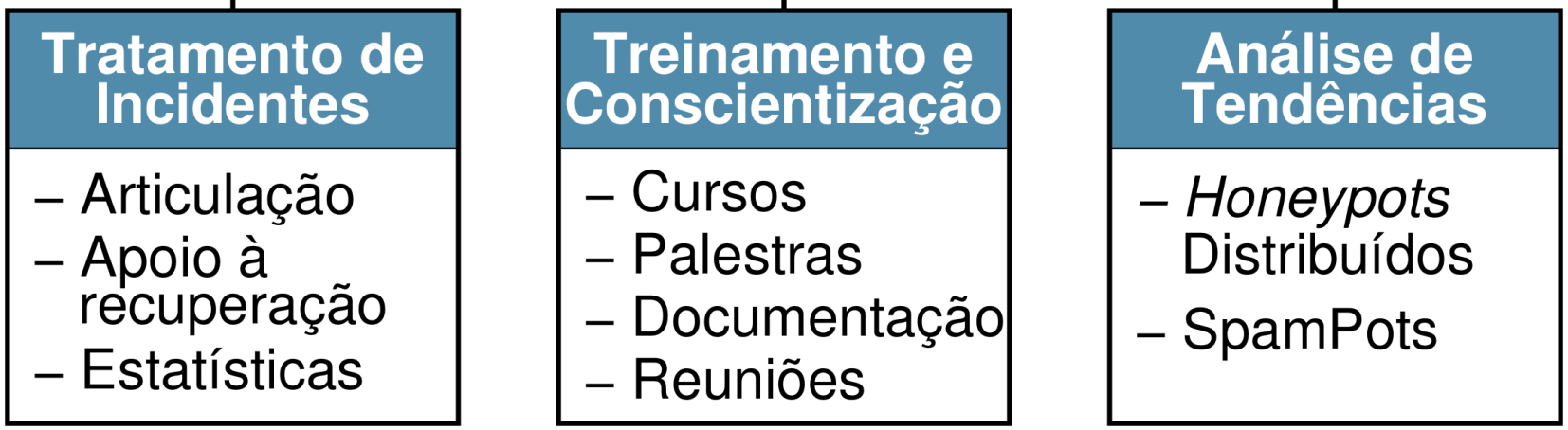
http://www.cgi.br/sobre-cg/

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

CERT.br



SEIPartner CERT Courses

FIRST Improving Security Together MEMBER

APWG RESEARCH PARTNER www.antiphishing.org

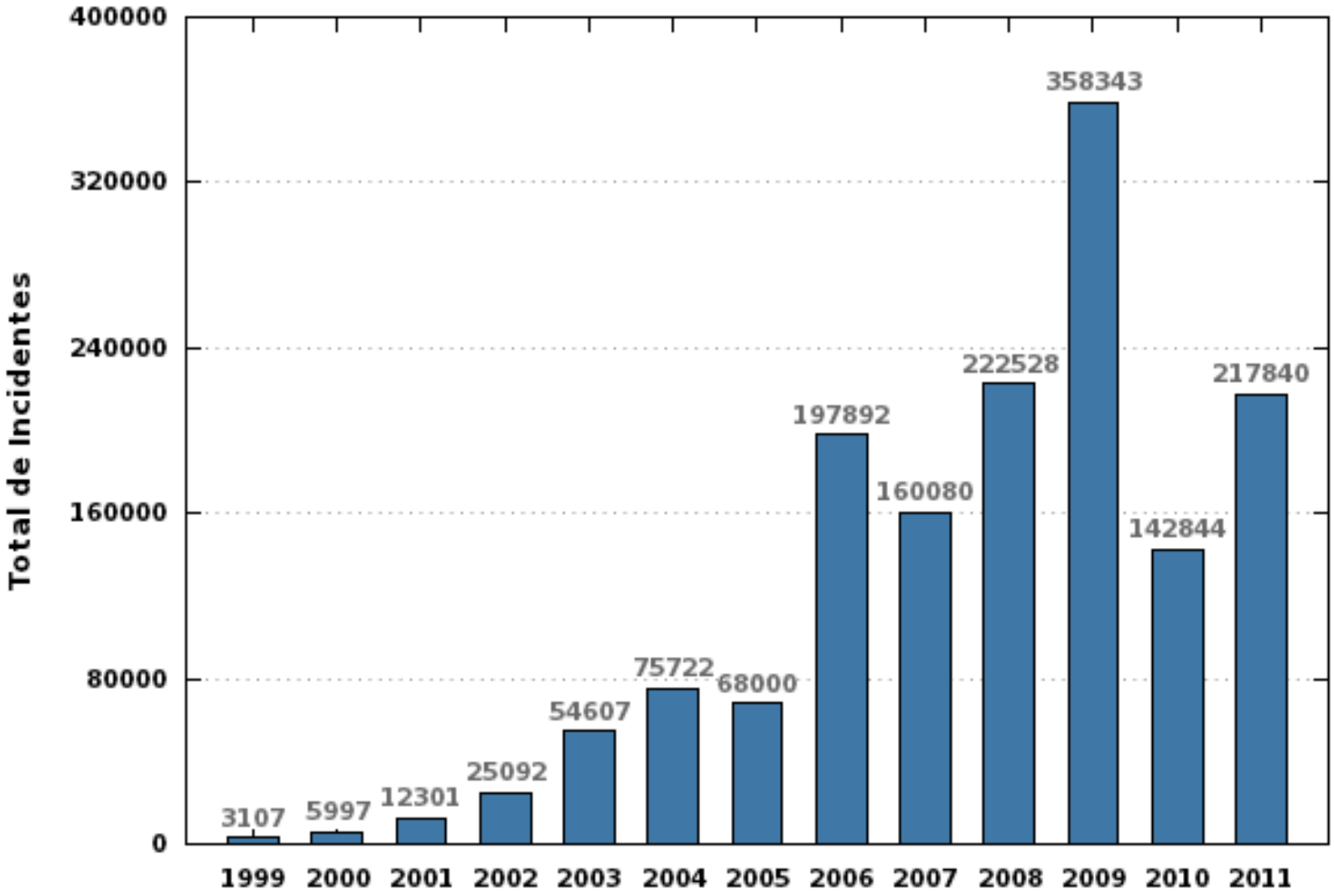
Criado em 1997 para:

- **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**

Agenda

- Incidentes de segurança mais frequentes
- Imagem do Brasil no exterior
- Causas fundamentais
- Mitos
- Desafios para melhora do cenário
- Considerações finais

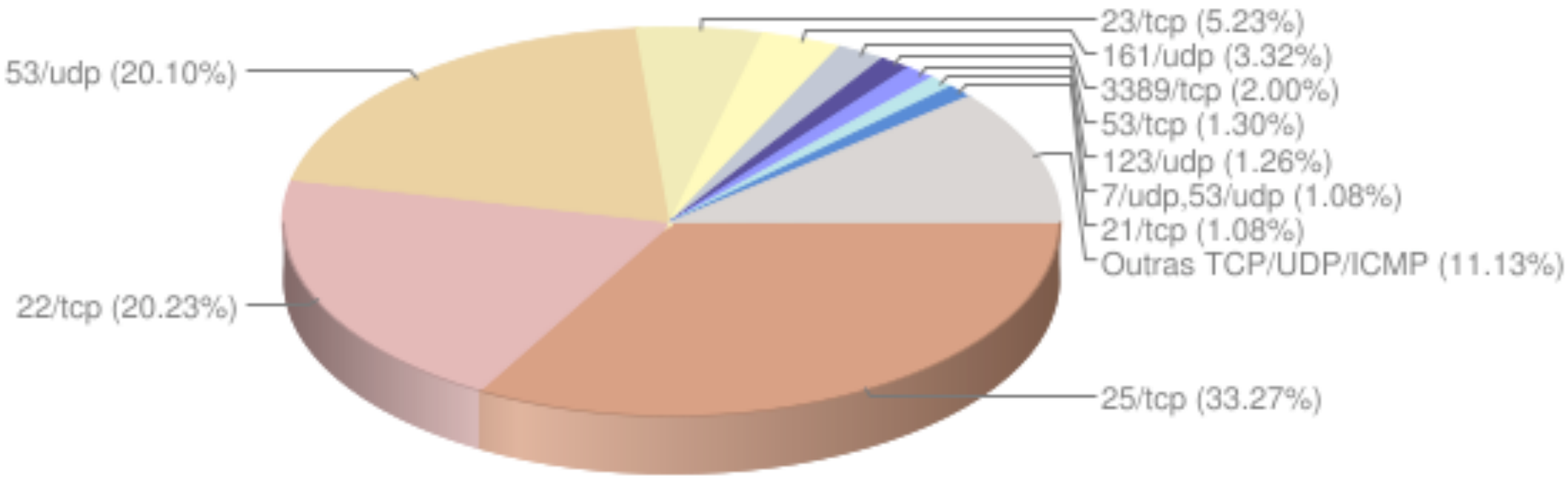
Incidentes reportados ao CERT.br – até junho/2011



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

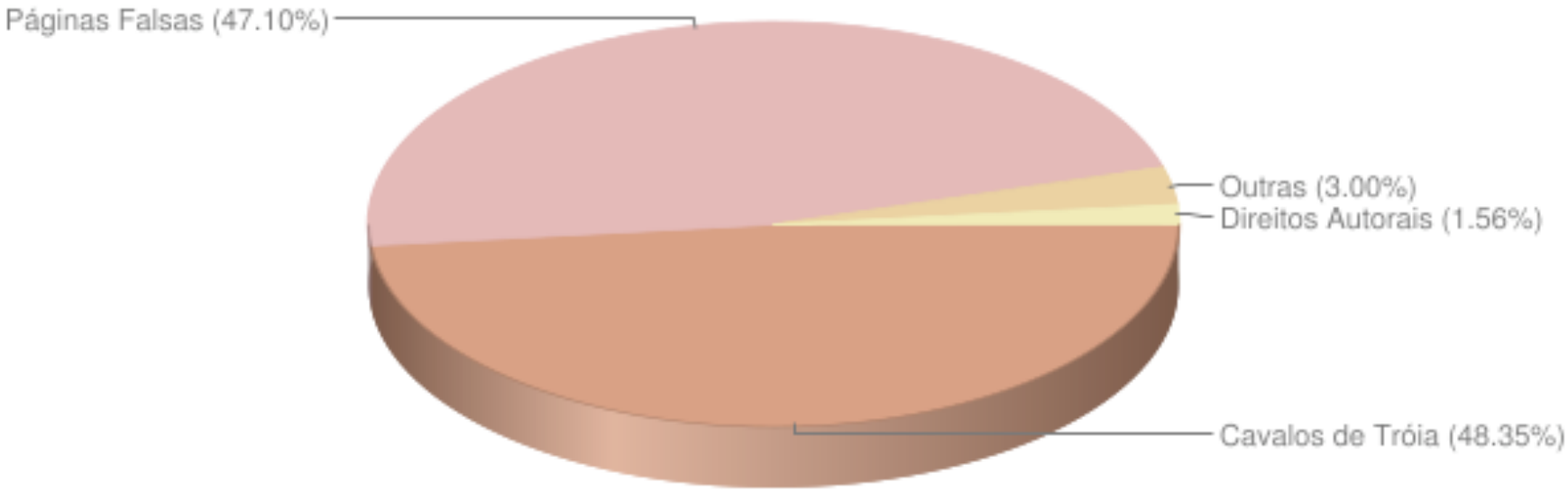
http://www.cert.br/stats/incidentes/

Varreduras Mais Frequentes – 2º Trim/2011



- **Força bruta:**
  - **SSH, TELNET, FTP, VNC, etc**
  - **Alvos:**
    - **senhas fracas, senhas padrão, contas temporárias**
  - **Pouca monitoração permite ao ataque perdurar por horas/dias**
- **Serviço DNS**

Tentativas de Fraude Reportadas – 2º Trim/2011



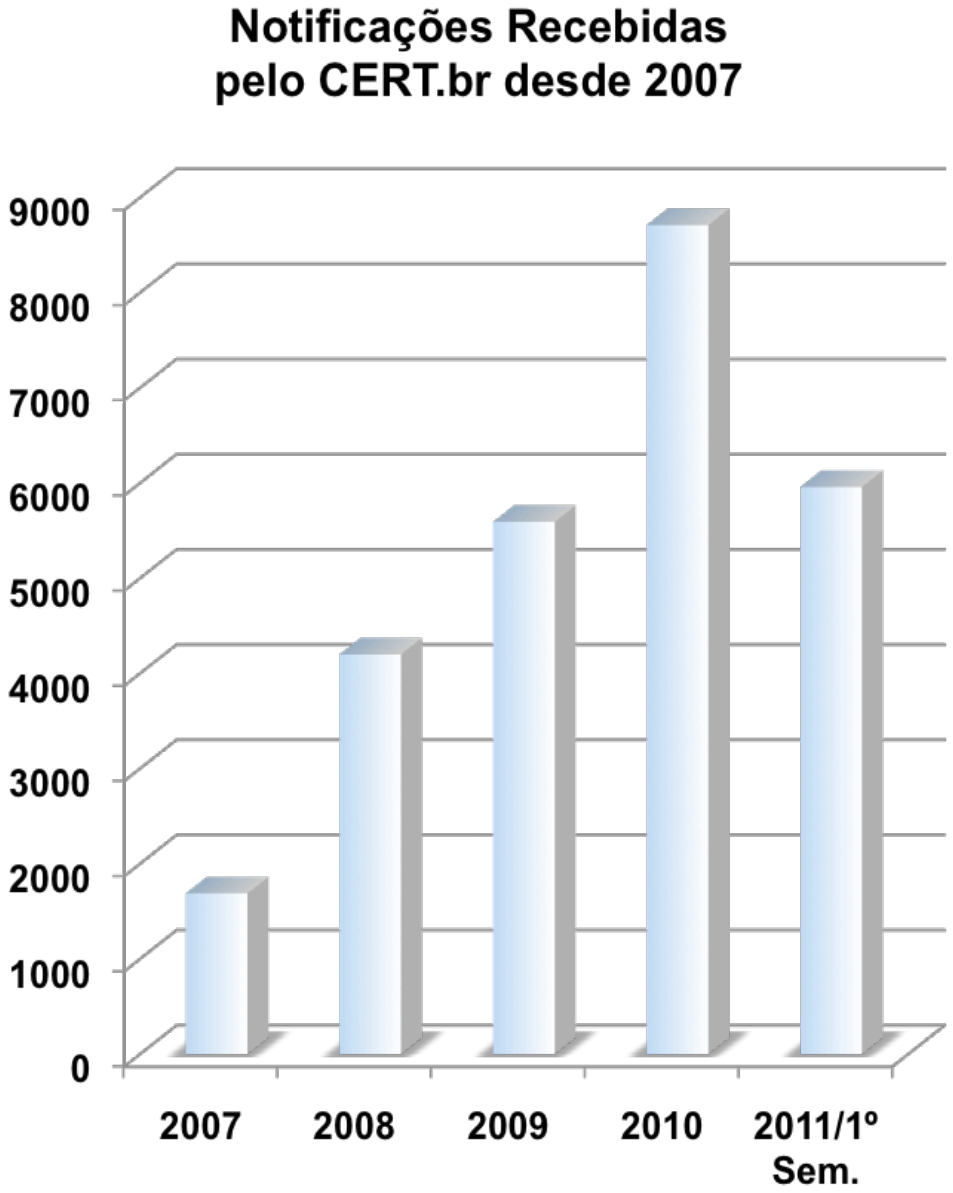
- ***Spams*** **em nome de diversas entidades/temas variados**
  - ***Links*** **para** ***trojans*** **hospedados em diversos** ***sites***
  - **Vítima raramente associa o** ***spam*** **com a fraude**
- **Retorno de páginas falsas**
  - **via** ***spams*** **em nome das instituições financeiras e/ou de comércio eletrônico**
  - **muitas envolvem alteração do arquivo hosts das máquinas**

Tentativas de fraudes reportadas (cont.)

- ***Drive-by downloads* intensamente utilizados**
  - **Via JavaScript, ActiveX, etc, inclusive em grandes *sites***
  - **Em conjunto com *malware* modificando:**
    - **arquivo *hosts***
    - **configuração de *proxy* em navegadores (arquivos PAC)**
- ***Links* patrocinados**
- ***Malware* para:**
  - ***Smartphones***
  - **Via redes sociais**
    - **explorando a confiança de seguidores**
    - **grande uso de *links* curtos**
- **Furtam diversos tipos de credenciais**
  - **E-mail, Redes Sociais Windows Live, *login* de consulta ao Serasa**
  - **Exploram confiança para propagação e vendem serviços**

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**



Obs.: **Não** são estatísticas de *defacements*, são ataques a serviços *web* em geral, incluindo SQL Injection, XSS, etc

Imagem do Brasil no Exterior

IPs do Brasil Enviando Spam - CBL

Países

CC	IPs	%	Pos.
IN	1.358.470	17,72	1
BR	643.188	8,39	2
VN	562.773	7,34	3
PK	420.120	5,48	4
RU	381.553	4,98	5
ID	367.462	4,79	6
CN	248.783	3,24	7
UA	193.933	2,53	8
RO	193.608	2,53	9
SA	191.890	2,50	10

Domínios do Brasil nos "Top 200"

Predomínio de redes residenciais

Domínio	IPs	Pos.
telebahia.net.br (Oi)	251.277	6
brasiltelecom.net.br (Oi)	128.851	10
telesp.com.br	63.820	25
gvt.net.br	54.903	28
netservicos.com.br	35.846	35
ig.com.br	27.376	45
ctbctelecom.net.br	19.570	57
timbrasil.com.br	18.496	60
telet.com.br (Claro)	14.365	77
embratel.net.br	5.180	167

Fonte: CBL, lista de endereços IP de computadores que estavam infectados e comprovadamente enviaram *spams* nas últimas 24 horas

Dados gerados em Tue Jul 26 05:10:24 2011 UTC/GMT
Composite Blocking List - http://cbl.abuseat.org/

Quarterly Report PandaLabs (Jan-Mar 2011)

Most infected countries in Q1 2011

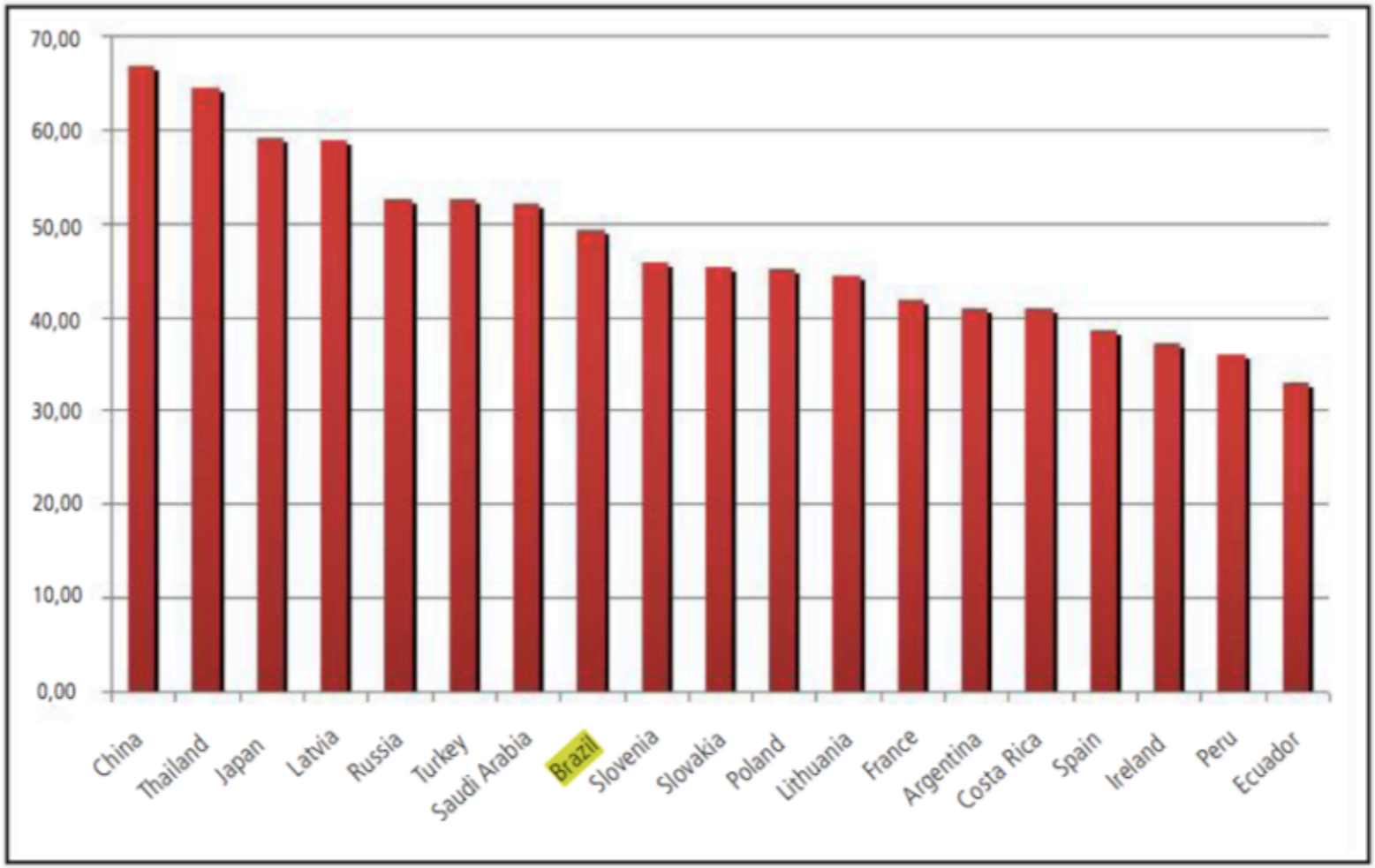


Gráfico dos países com maior taxa de infecção, dentre clientes Panda.

http://pandalabs.pandasecurity.com/pandalabs-quarterly-report-q1-2011/

Sophos Dirty Dozen - January–March 2011

Lista dos países que mais foram abusados para envio de spam (*relaying countries*)

1. USA	13.7%
2. India	7.1%
3. Russia	6.6%
4. Brazil	6.4%
5. S Korea	3.8%
6. United Kingdom	3.2%
7= Italy	3.1%
7= France	3.1%
9. Spain	2.8%
10. Germany	2.6%
11. Romania	2.5%
12. Poland	2.3%
Other	42.8%

http://nakedsecurity.sophos.com/2011/05/11/dirty-dozen-spam-relaying-countries/

Causas Fundamentais

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**
    - **Cultura do "*Deploy and patch later*"**
  - **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**

Motivações/Facilitadores para os Atacantes

Ataques a Serviços *Online*

- Grande demanda por *e-services*
- Dados sensíveis estão mais expostos
  - por necessidade, comodidade ou descuido
- Segurança não é prioridade
- Impactos não são compreendidos
- Sistemas críticos são colocados na Internet
  - controle de infra-estrutura crítica
  - caixas bancários
  - sistemas de imigração e identificação

Ataques a Clientes/Usuários

- Internet passou a fazer parte do dia-a-dia
- Usuários não são especialistas
- Grande base
  - de máquinas vulneráveis
  - com banda disponível
- Mais fáceis de atacar
- Possuem dados de valor
  - endereços de e-mail válidos
  - credenciais de acesso
  - dados financeiros
- Computadores podem ser usados para outros ataques
  - ***botnets***

Uso de Botnets

- **Uma base muito grande de computadores com *software* desatualizado/vulnerável sendo ativamente abusada por criminosos**
  - **Especialmente em países em desenvolvimento**
- **Uso de *botnets:***
  - **DDoS**
  - **Extorsão**
  - ***Download* de outros tipos de *malware***
  - **Furto de informações**
  - ***Proxies* abertos**
    - **envio de *spam***
    - ***navegação anônima***

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**

Alguns Exemplos Recentes de Descuido / Ingenuidade

- **Localização de sistemas SCADA via Google**

  http://news.cnet.com/8301-27080_3-20087201-245/researchers-warn-of-scada-equipment-discoverable-via-google/

  AUGUST 2, 2011 4:02 PM PDT

  "*Among the results was one referencing a "RTU pump status" for a Remote Terminal Unit, like those used in water treatment plants and pipelines, that appeared to be connected to the Internet. The result also included a password – '1234.' "*

- **Operation Shady RAT – 72 empresas/agências de governo com segredos furtados**

  http://blogs.mcafee.com/mcafee-labs/revealed-operation-shady-rat

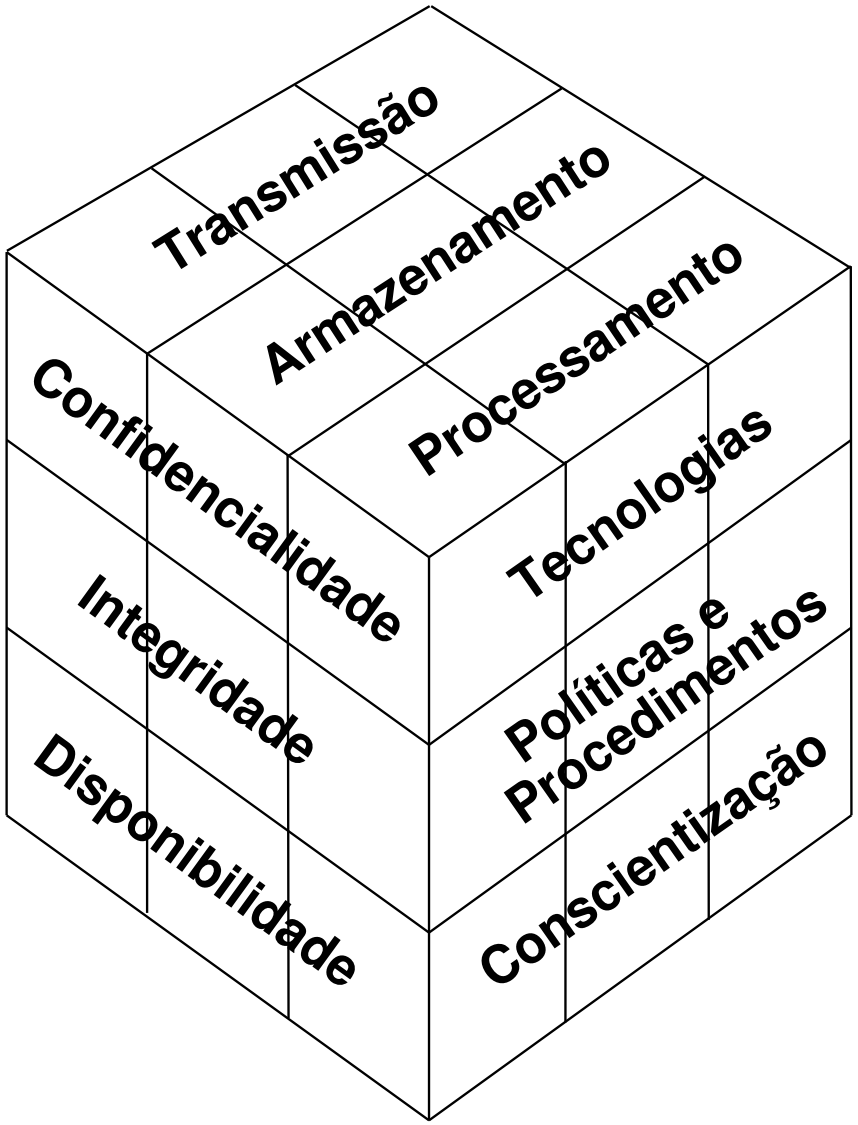
  Tuesday, August 2, 2011 at 9:14pm

  "*a spear-phishing email containing an exploit is sent to an individual with the right level of access at the company, and the exploit when opened on an unpatched system will trigger a download of the implant malware"*

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



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**

Desafios para Melhora do Cenário

Desafios – Desenvolvimento de *Software*

- **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**
  - **Os sistemas para usuários finais forem menos complexos**
    - **Mudança total de paradigma de uso da tecnologia**

Desafios – Empresas e Provedores de Banda Larga

- 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 riscos?
- Ir além do "*compliance*"
- Provedores de acesso e serviço, operadoras e administradores de redes em geral serem mais pró-ativos
  - Identificação e correção de clientes infectados com *bots*
    - já sendo feito no Japão, Holanda, Alemanha e Austrália
  - Gerência de saída de tráfego com destino à porta 25/TCP para redução de *spam*

    http://www.antispam.br/admin/porta25/

Considerações Finais

- **Mas é necessário cuidado:**
  - **Nem todas as medidas sendo defendidas ou implantadas são efetivas**
    - **Algumas só reduzem a privacidade, sem aumentar a segurança**
  - **Ao mesmo tempo:**
    - **Medidas efetivas acabam sendo "boicotadas" em nome da privacidade, mesmo quando não interferem em nada na privacidade**
- **Não será possível erradicar todos os problemas, precisamos torná-los gerenciáveis**
  - **cada setor precisa fazer a sua parte – isso é cooperação para a solução dos problemas**
  - **a solução não virá de uma ação única**

Informações de Contato

- **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/
- **Esta palestra**
  http://www.cert.br/docs/palestras/

Cristine Hoepers
cristine@cert.br