

Panorama de Incidentes de Segurança no Brasil

Miriam von Zuben

miriam@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

- **Governança da Internet no Brasil**
 - CGI.br, NIC.br e CERT.br
- **Cenário brasileiro**
 - incidentes de segurança
 - *spam*
- **Desafios**
 - mercado negro
 - tratamento dos incidentes
 - como melhorar o cenário
- **Considerações finais**

Governança da Internet no Brasil

Evolução da Internet no Brasil

1989	Criação e delegação do código de país (ccTLD) “.br” à FAPESP
1991	Primeira conexão TCP/IP brasileira, realizada entre a FAPESP e o Energy Sciences Network (ESNet) por meio do Fermilab (<i>Fermi National Accelerator Laboratory</i>)
1995	Criação do CGI.br (Portaria Interministerial MC/MCT nº 147, de 31 de maio) com a missão de 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

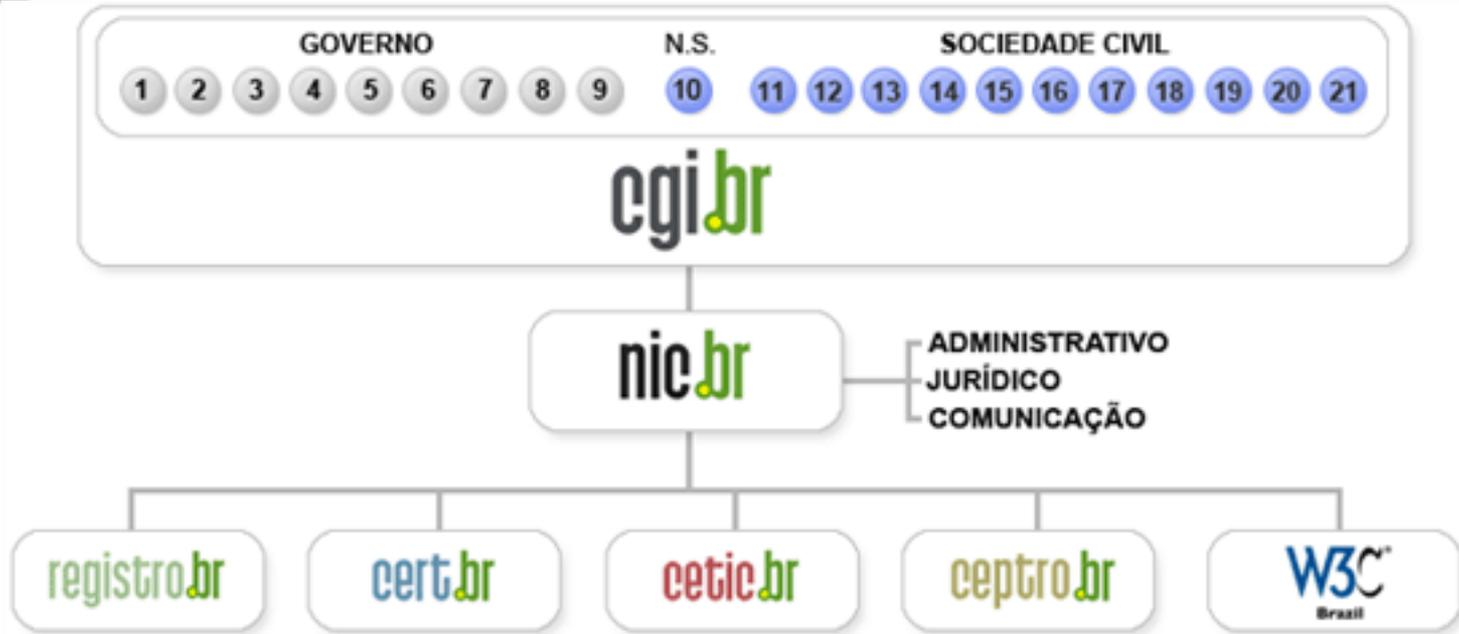
Comitê Gestor da Internet no Brasil – CGI.br

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



Tratamento de Incidentes
<ul style="list-style-type: none"> – Articulação – Apoio à recuperação – Estatísticas

Treinamento e Conscientização
<ul style="list-style-type: none"> – Cursos – Palestras – Documentação – Reuniões

Análise de Tendências
<ul style="list-style-type: none"> – <i>Honeypots</i> Distribuídos – SpamPots



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

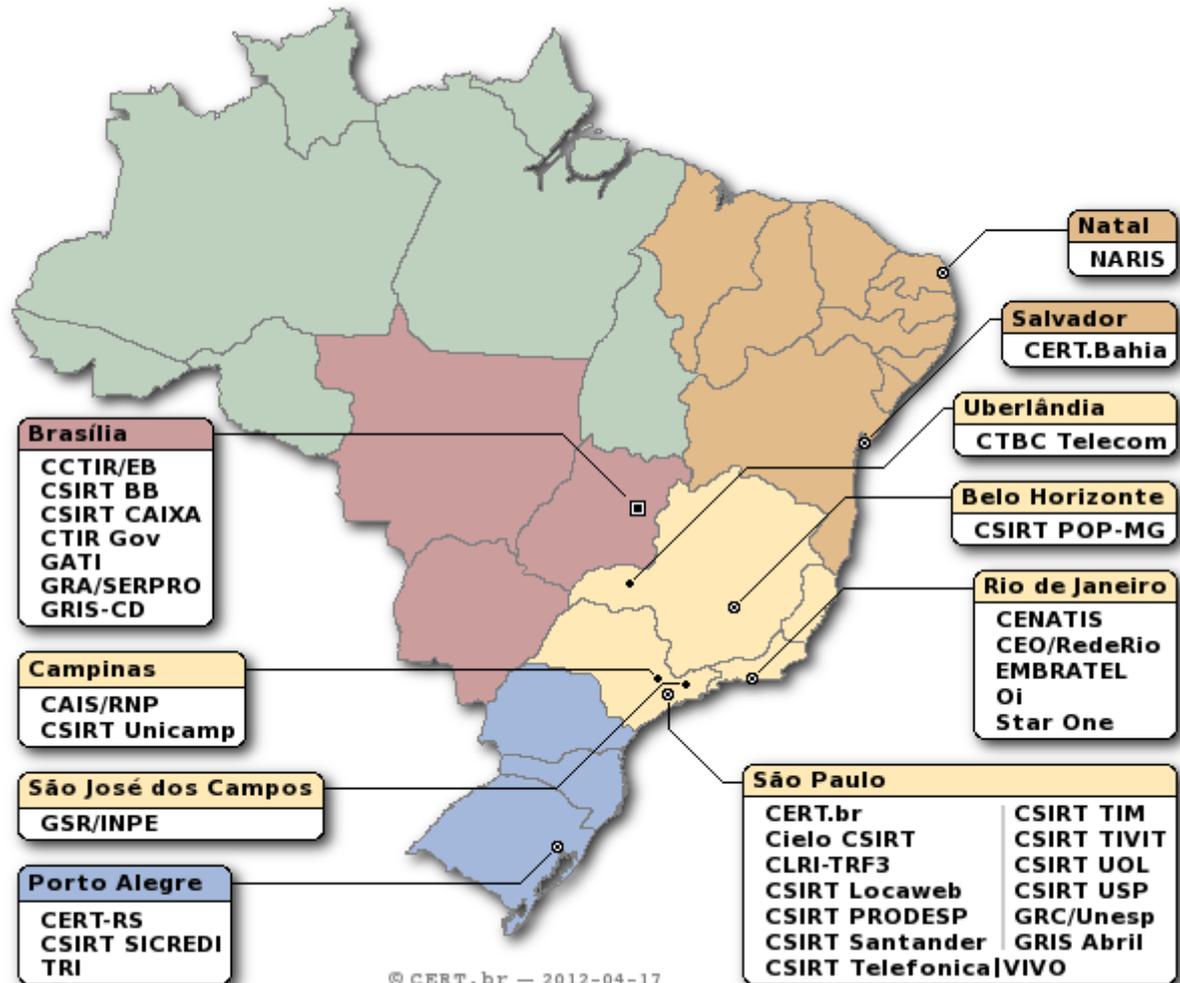
Rumo a Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil

<http://www.nic.br/grupo/historico-gts.htm> | <http://www.cert.br/sobre/>

CSIRTs Brasileiros

34 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 VIVO, CSIRT Locaweb, CSIRT TIM, CSIRT UOL, 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



© CERT.br — 2012-04-17

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

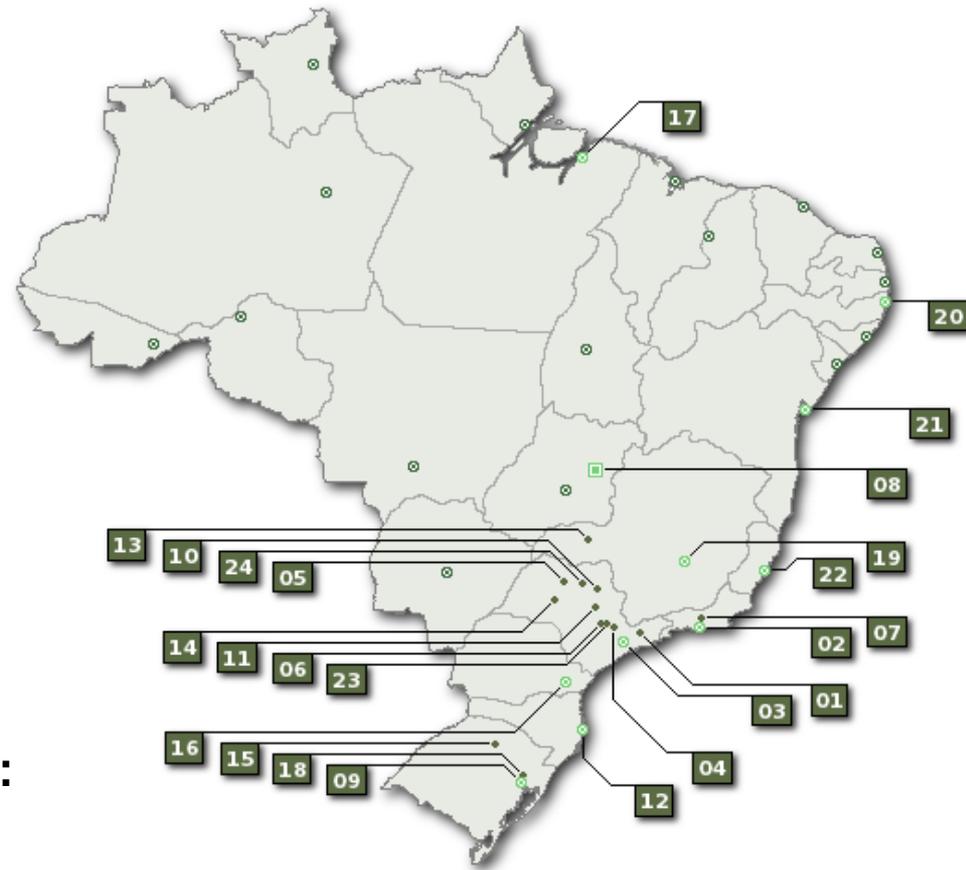
Honeypots Distribuídos

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

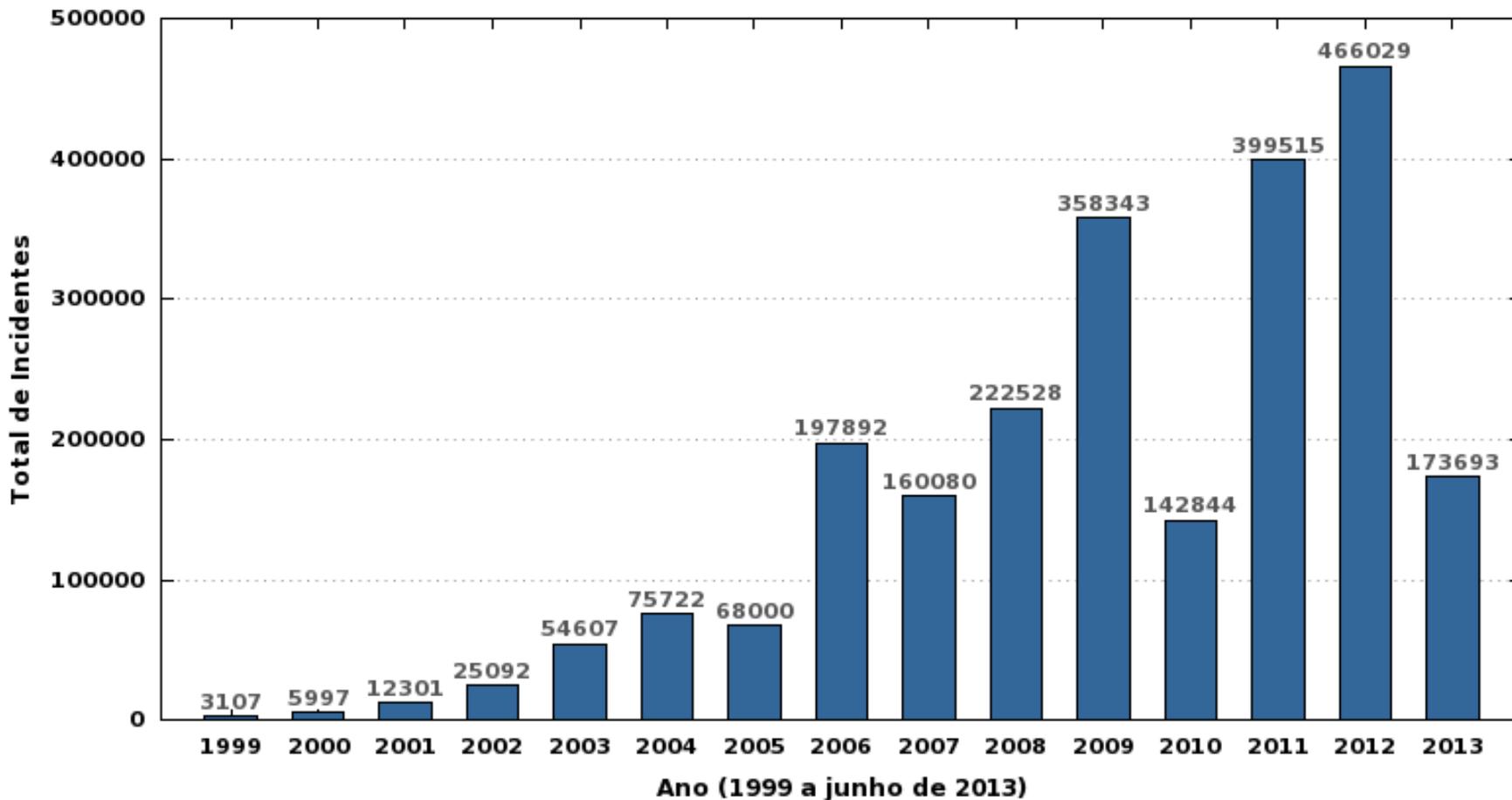


Cenário Brasileiro Incidentes de Segurança

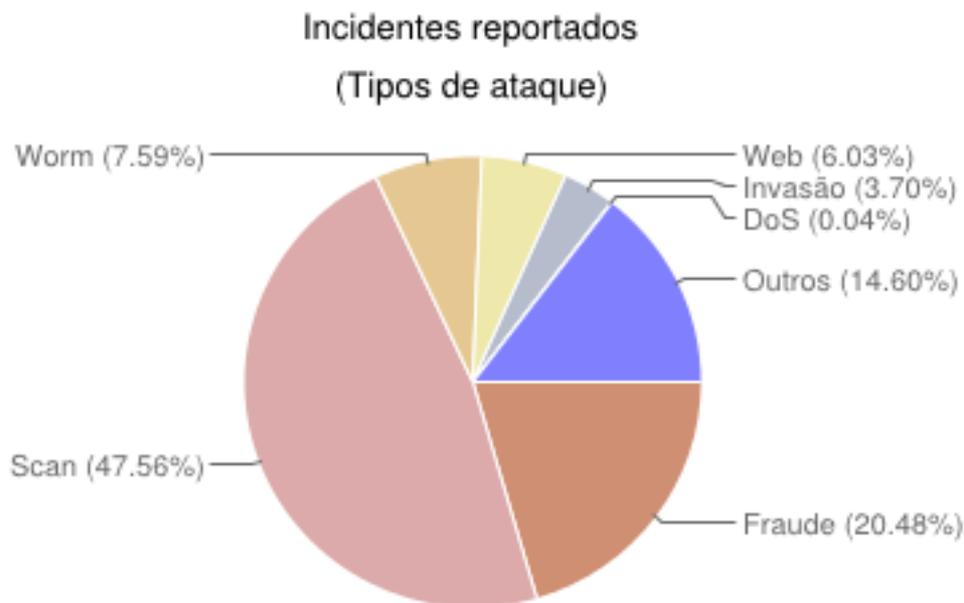
Fonte: Estatísticas CERT.br
<http://www.cert.br/stats/incidentes/>

Incidentes reportados ao CERT.br – até junho/2013

Total de Incidentes Reportados ao CERT.br por Ano



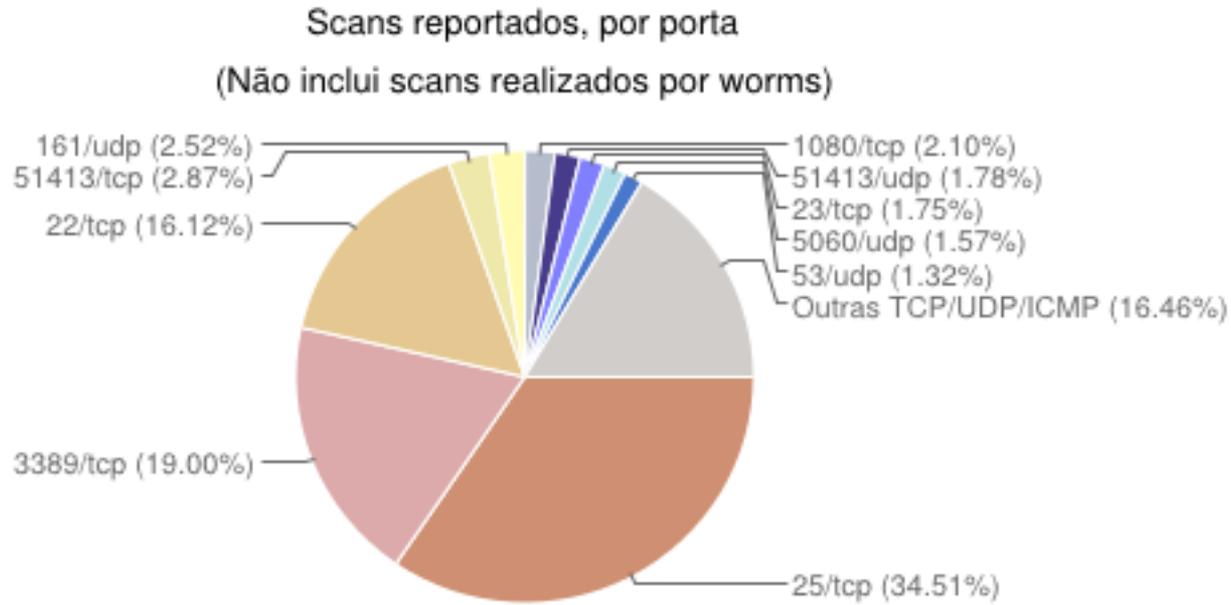
Tipos de ataque – abril a junho de 2013



- **Contra usuários finais**

- mais fácil e rentável
- motivações: financeira, espionagem, sabotagem
- aplicações Web vulneráveis com rápido crescimento nos últimos anos
- *drive-by download*: sites principais da Vivo, Oi e Ambev

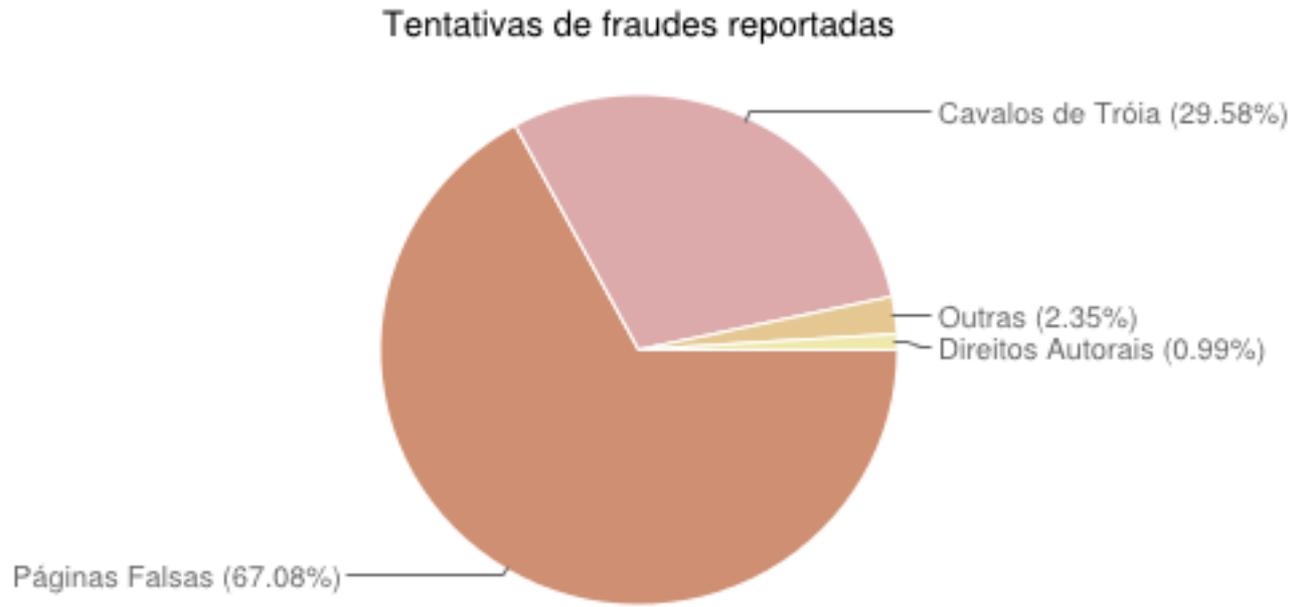
Scans reportados – abril a junho de 2013



- **Força bruta**

- **contra serviços de rede: SSH, FTP, Telnet, VNC, etc.**
- **alvos: senhas fracas, senhas padrão, contas temporárias**
- **acesso a servidores, roteadores, modems banda larga, etc.**
- **pouca monitoração permite ao ataque perdurar por horas/dias**

Tentativas de fraudes – abril a junho de 2013



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

Outros ataques em rápido crescimento

- **“Modems” e roteadores banda larga (CPEs)**
 - *botnets* usadas para ataques diversos
 - comprometidos via força bruta (telnet)
 - comprometimento para alteração do serviço DNS para:
 - DDoS
 - fraudes financeiras
 - redirecionamento para obter “cliques” de propaganda
- **Dispositivos com sistema Android**
 - *botnets*
 - fraudes e outros tipos de *malware*
- **Sistemas SIP**
 - força bruta para realização de ligações internacionais
 - fraude

Foco da maioria dos ataques continua sendo

Serviços *Online*

- Grande demanda por *e-services*
- Dados sensíveis mais expostos
 - por necessidade, comodidade ou descuido
- Segurança não é prioridade
- Impactos não são compreendidos
- Sistemas críticos conectados à Internet
 - controle de infraestruturas críticas
 - caixas automáticos (ATMs)
 - sistemas de imigração e identificação

Clientes/Usuários

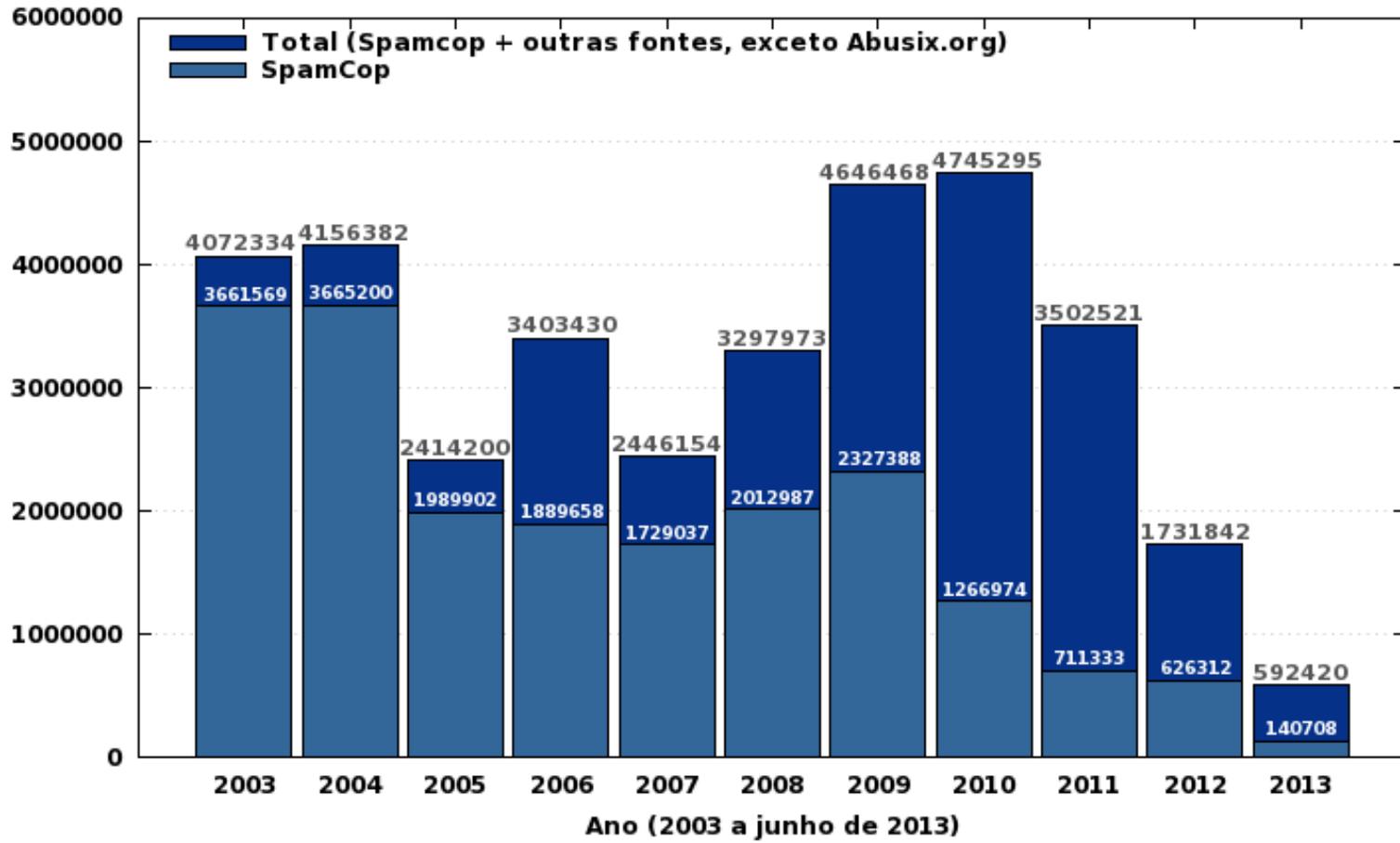
- Internet passou a fazer parte do dia-a-dia
- Usuários não são especialistas
- Grande base
 - de dispositivos vulneráveis
 - com banda disponível
- Mais fáceis de atacar
- Possuem dados de valor
 - dados financeiros
 - endereços de *e-mail* válidos
 - credenciais de acesso
- BYOD
- Dispositivos podem ser usados para ataques (spam, *botnets*)

Cenário Brasileiro *Spam*

Fonte: Estatísticas CERT.br
<http://www.cert.br/stats/spam/>

Spam – até junho de 2013

Spams Reportados ao CERT.br por Ano



Spam – Gerência de Porta 25 (1/2)

- Conjunto de ações, aplicadas em redes residenciais
- Separar:
 - a submissão de *e-mails* por um usuário: 587/TCP com autenticação
 - do transporte de mensagens entre servidores de *e-mail*: 25/TCP
- Impacto:
 - permite filtrar o tráfego com destino à porta 25/TCP
 - *e-mails* legítimos, que usam uma porta diferente, não são afetados
 - *spams* enviados por máquinas infectadas/*botnets* direto para servidores de *e-mail* não saem da rede
- Mais informações: <http://www.antispam.br/>



Spam – Gerência de Porta 25 (2/2)



- **2009: 1º posição, mais de 1 milhão de IPs listados (17%)**
- **Março de 2013: 12º posição, menos de 200 mil IPs listados (2%)**
- **Agosto de 2013: 27º posição, menos de 50 mil IPs listados (0.73%)**
- **CBL - Composite Blocking List - <http://cbl.abuseat.org/country.html>**

Desafios

Mercado negro (1/2)

Overall Rank		Item	Percentage		2010 Price Ranges
2010	2009		2010	2009	
1	1	Credit card information	22%	19%	\$0.07–\$100
2	2	Bank account credentials	16%	19%	\$10–\$900
3	3	Email accounts	10%	7%	\$1–\$18
4	13	Attack tools	7%	2%	\$5–\$650
5	4	Email addresses	5%	7%	\$1/MB–\$20/MB
6	7	Credit card dumps	5%	5%	\$0.50–\$120
7	6	Full identities	5%	5%	\$0.50–\$20
8	14	Scam hosting	4%	2%	\$10–\$150
9	5	Shell scripts	4%	6%	\$2–\$7
10	9	Cash-out services	3%	4%	\$200–\$500 or 50%–70% of total value

Fonte: Underground Economy Servers—Goods and Services Available for Sale

http://www.symantec.com/es/es/threatreport/topic.jsp?id=fraud_activity_trends&aid=underground_economy_servers

Mercado negro (2/2)

Russian Underground – Serviços disponíveis

- Pay-per-Install (global mix or specific country): \$12–\$550
- Bulletproof-hosting with DDoS protection: \$2000 per month
- Styx Sploit Pack rental (affects Java and Adobe Acrobat and Flash Player) \$3000/month
- Programming: web server hacking \$250; browser-in-the-middle \$850; trojans \$1300
- Windows rootkit (for installing malicious drivers): \$292
- Linux rootkit: \$500
- Hacking Facebook or Twitter account: \$130
- Hacking Gmail account: \$162

“Proxy service: HTTP, HTTPS, SOCKS4, SOCKS5; prices: 5 days = US\$4; 10 days = US\$8; 30 days = US\$20; 90 days = US\$55”

Offering	Price
Bots (i.e., consistently online 40% of the time)	US\$200 for 2,000 bots
DDoS botnet	US\$700
DDoS botnet update	US\$100 per update

Offering	Price
1-day DDoS service	US\$30-70
1-hour DDoS service	US\$10
1-week DDoS service	US\$150
1-month DDoS service	US\$1,200

“Setup of ZeuS: US\$100, support for botnet: US\$200/month, consulting: US\$30.”

Fonte: Read Russian Underground 101 - Trend Micro

<http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf>

Tratamento de incidentes (1/2)

- **Dificuldade de identificação dos ataques:**
 - ataques partem de vítimas na maioria absoluta dos casos
- **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>
- **Criminosos estão apenas migrando para onde os negócios estão**

Tratamento de incidentes (2/2)

Mito de que só quem sabe invadir sabe proteger

- **A realidade:**
 - proteger é muito mais difícil que atacar
 - especialmente contra ataques ainda não conhecidos
 - 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
 - profissional com sólida formação tem mais sucesso em usar as ferramentas como auxiliares nos processos de análise de risco e proteção da infraestrutura que um invasor
- **Os riscos:**
 - colocar a segurança nas mãos de quem não está preparado
 - ter informações confidenciais comprometidas
 - ter *backdoors* e *trojans* instalados em sua infraestrutura

Desafios para a Melhora do Cenário como um Todo

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)
 - o 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)

- **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 preocupante
- **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*”**
- **Investir em treinamento e conscientização de usuários finais**

Dicas para usuários finais (1/3)

- **Manter computadores e dispositivos móveis seguros:**
 - com todas as atualizações aplicadas
 - com todos os programas instalados com as versões mais recentes
- **Usar:**
 - mecanismos de segurança
 - *firewall* pessoal, *antimalware*, *antiphishing*, *antispam*
 - complementos, extensões, *plugins*
 - apenas programas originais
 - configurações de segurança já disponíveis
- **Instalar aplicativos**
 - de fontes confiáveis
 - bem avaliados pelos usuários
 - com permissões coerentes

Dicas para usuários finais (2/3)

- **Manter postura preventiva**
 - **não acessar *sites* ou seguir *links***
 - recebidos de mensagens eletrônicas
 - em páginas sobre as quais não se saiba a procedência
 - **não confiar apenas no remetente da mensagem**
 - ela pode ter sido enviada de:
 - máquinas infectadas
 - contas falsas ou invadidas

Dicas para usuários finais (3/3)

- **Proteger contas e senhas**
 - **utilizar:**
 - grande quantidade de caracteres
 - diferentes tipos de caracteres
 - números aleatórios
 - **não utilizar:**
 - sequências de teclado
 - dados pessoais:
 - nome, sobrenome, contas de usuário, números de documentos, placas de carros, números de telefones
 - informações que possam ser coletadas em *blogs* e redes sociais
 - palavras que façam parte de listas
 - nomes de músicas, times de futebol, personagens de filmes, dicionários de diferentes idiomas, etc.
- **Trocar regularmente as senhas**
- **Evitar usar o usuário “administrador”**

Informe-se e Mantenha-se Atualizado

Portal Internet Segura

<http://www.internetsegura.br/>



Campanha Antispam.br

<http://www.antispam.br/>

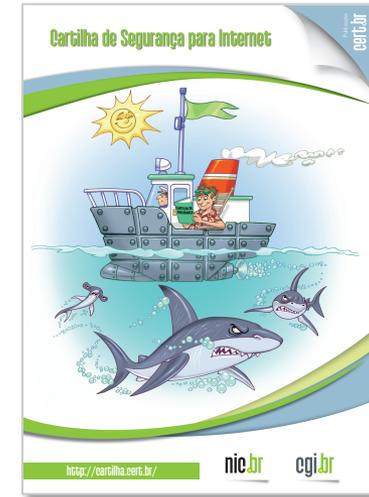


Cartilha de Segurança para Internet 4.0

2ª Edição do Livro

Novas recomendações, em especial sobre:

- segurança e privacidade em redes sociais
- segurança no uso de dispositivos móveis



Reestruturada

- ilustrada
- em HTML5
- formato EPub



Nova licença

- *Creative Commons (CC BY-NC-ND 3.0)*



Cartilha de Segurança para Internet – Fascículos

Organizados e diagramados de forma a facilitar a difusão de conteúdos específicos

Slides de uso livre para:

- ministrar palestras e treinamentos
- complementar conteúdos de aulas
- licença CC BY-NC-SA 3.0 Brasil

Redes Sociais – 08/2012

Senhas – 10/2012

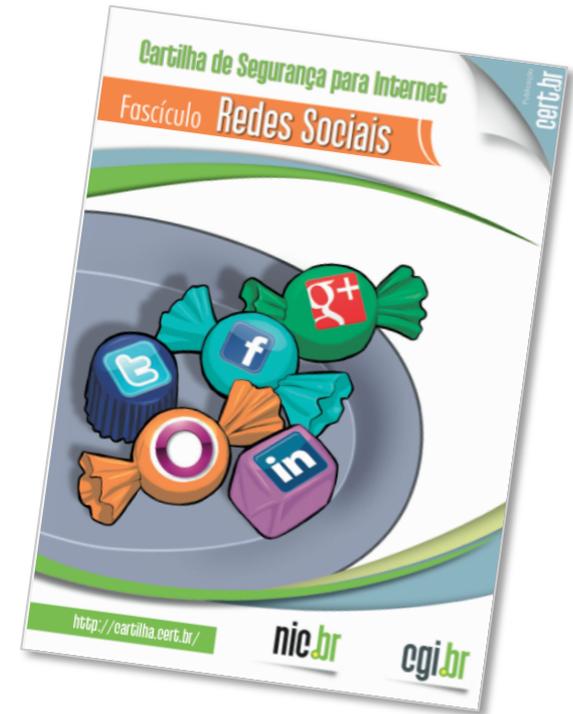
Comércio Eletrônico – 11/2012

Privacidade – 02/2013

Dispositivos Móveis – 04/2013

Internet Banking – 06/2013

Computadores – 08/2013



Cartilha de Segurança para Internet – Dica do Dia



RSS

<http://cartilha.cert.br/rss/cartilha-rss.xml>



Twitter

<http://twitter.com/certbr>

Site

<http://cartilha.cert.br/>

Perguntas?

Miriam von Zuben

miriam@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/>

