

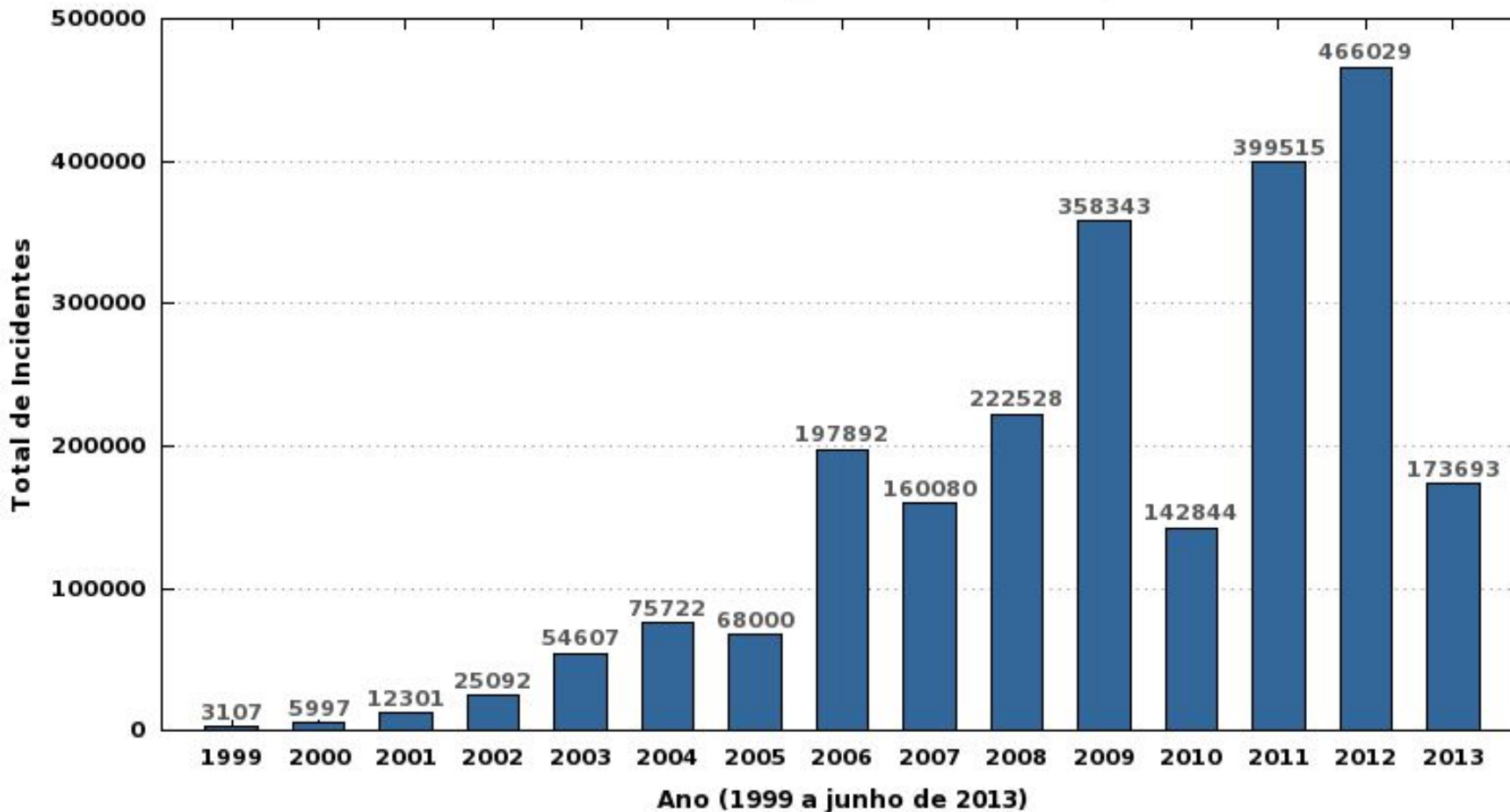
Cenários Atuais

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



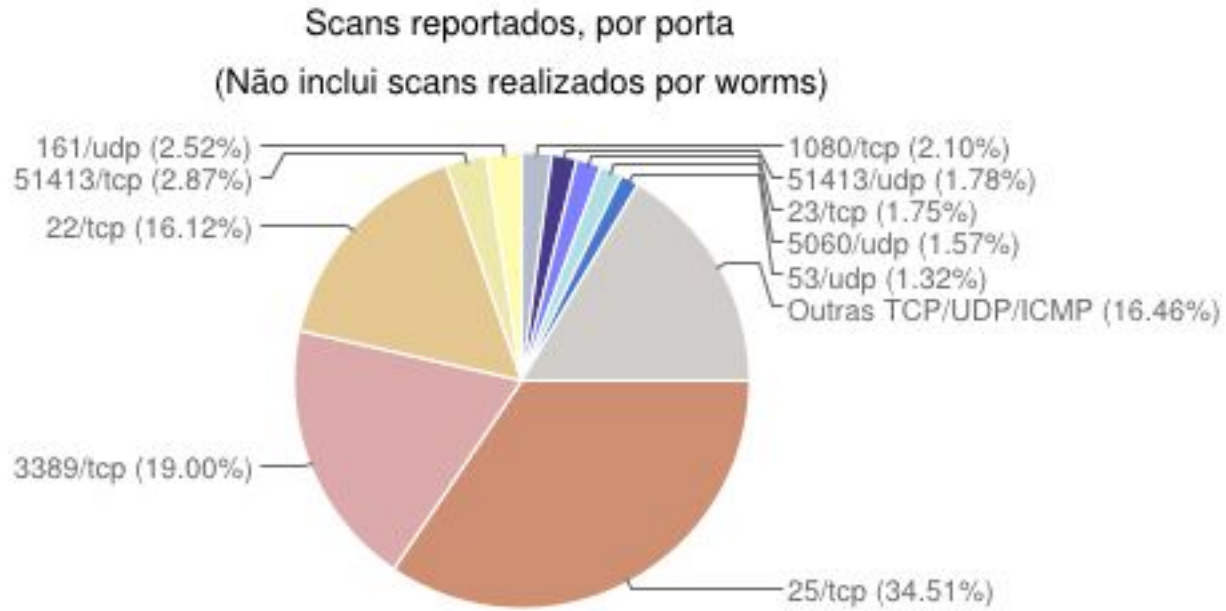
Tipos de ataque – abril a junho de 2013



- **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

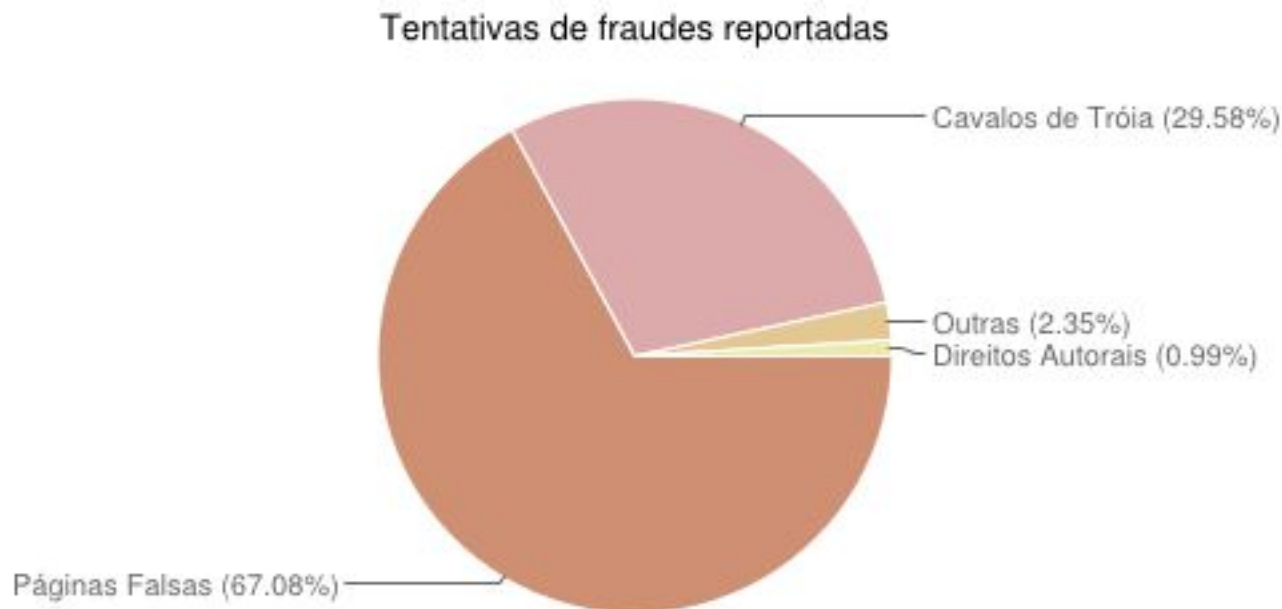
Scans reportados – abril a junho de 2013



- **Força bruta**

- **contra serviços de rede: SSH, FTP, Telnet, VNC, etc.**
- **alvos: senhas fracas, senhas padrão, contas temporárias**
- **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 infra-estruturas críticas
 - caixas automáticos (ATMs)
 - sistemas de imigração e identificação

Clientes/Usuários

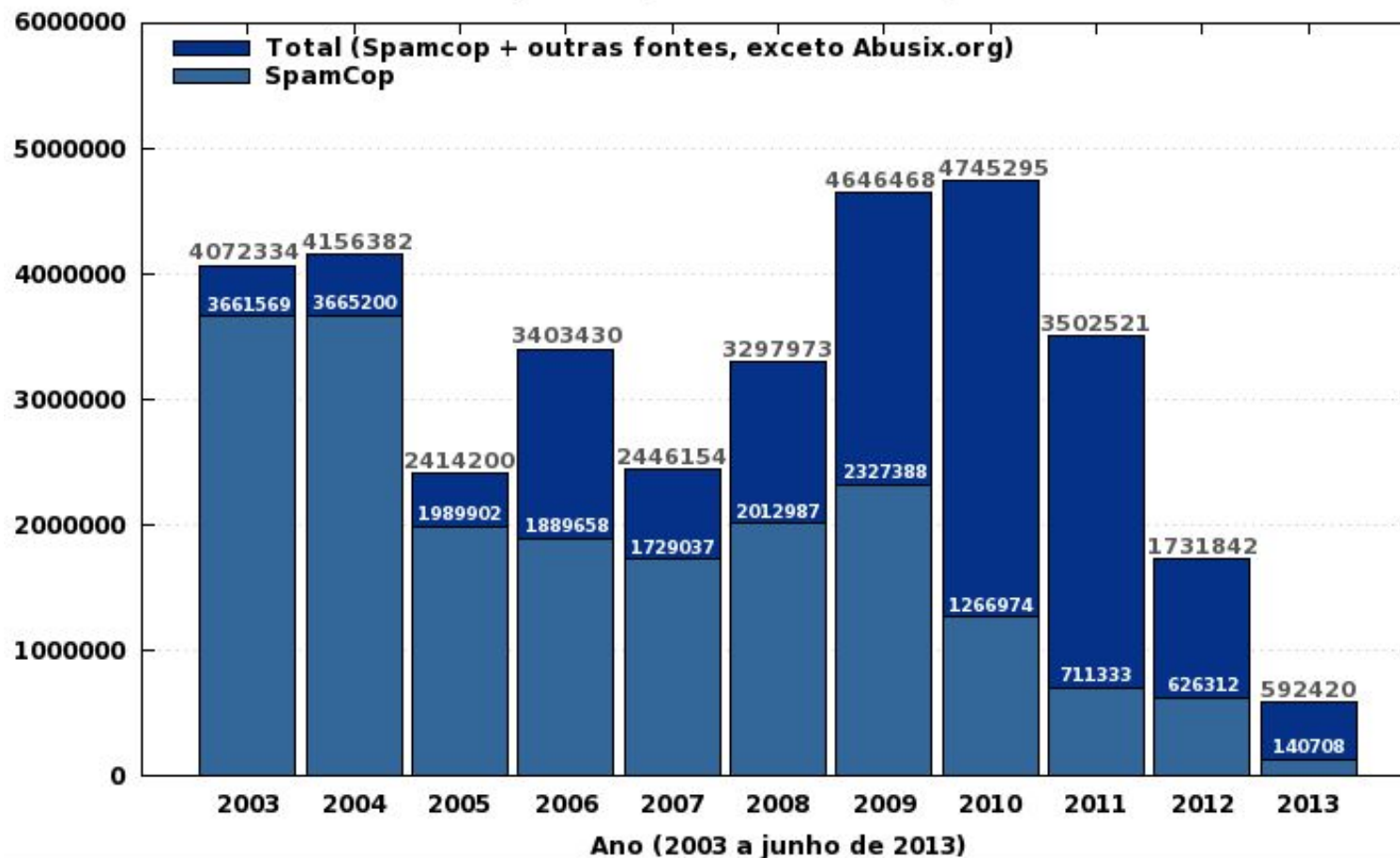
- Internet como parte do dia-a-dia
- Usuários não são especialistas
- Grande base
 - de dispositivos vulneráveis
 - com banda disponível
- Mais fáceis de atacar
- Possuem dados de valor
 - dados financeiros
 - endereços de *e-mail* válidos
 - credenciais de acesso
- BYOD
- Dispositivos podem ser usados 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/>

Configure a porta de envio de suas mensagens para **587!**

Com a Gerência da Porta 25, o Brasil vai reduzir o volume de spams enviados em nosso país.

Você ajuda o Brasil a melhorar a Internet e ainda evita dores de cabeça.

Conheça neste site mais detalhes do Gerenciamento da Porta 25.

Afinal, quem tem que ficar de fora são os spams, e não você!

Feche a porta para os spams!

Spam – Gerência de Porta 25 (2/2)



- **2009: 1º posição, mais de 1 milhão de IPs listados (17%)**
- **Março/2013: 12º posição, menos de 200 mil IPs listados (2%)**
- **Setembro/2013: 24º posição, cerca de 62 mil IPs listados (1.12%)**
- **CBL - *Composite Blocking List* - <http://cbl.abuseat.org/country.html>**

Cenário Geral Mercado Negro

Monetização – Informações e ferramentas

| 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

Monetização – Serviços

Russian Underground

- 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 up |

| 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>

Principais Desafios

Desafios – Tratamento de incidentes (1/3)

- **Identificação da origem dos ataques**
 - ataques partem de vítimas na maioria absoluta dos casos
- **Reais Causas dos Problemas**
 - 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>

Os criminosos estão apenas migrando para onde os negócios estão

Desafios – Tratamento de incidentes (2/3)

- 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
 - como funcionam as ferramentas que utilizam
 - maioria absoluta utiliza ferramentas disponíveis na Internet
 - um profissional com sólida formação tem mais sucesso em utilizar 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 – Tratamento de incidentes (3/3)

- **A redução do impacto de um incidente é consequência da:**
 - agilidade de resposta
 - redução no número de vítimas
- **O sucesso depende da confiabilidade**
- **O papel do CSIRT:**
 - auxiliar a proteção da infra-estrutura e das informações
 - prevenir incidentes e conscientizar sobre os problemas
- **O CSIRT não é um investigador**
- **Tratamento de incidentes não é perícia**
- **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

Desafios – Administradores de redes

- **Capacitação profissional**
 - falta de pessoal treinado para lidar com redes e com segurança em IPv4
 - situação ainda mais preocupante relativa ao IPv6
- **Implementação de melhores práticas:**
 - **BCP 38 / BCP 84** - <http://bcp.nic.br/entenda-o-antispoofing/>
 - filtrar pacotes com endereços “*spoofados*”
 - impedir a participação dos zumbis em:
 - ataques de DDoS, amplificação
 - outros ataques que usem pacotes *spoofados*
 - **Gerência de Porta 25** - <http://www.antispam.br/admin/porta25/>
 - impedir que zumbis sejam usados para entrega direta de *spam*
 - detectar máquinas infectadas
 - **Configuração adequada de servidores DNS recursivo** - <http://www.cert.br/docs/whitepapers/dns-recursivo-aberto/>
 - mitigar ataques como envenenamento de cache e DoS/amplificação

Desafios – Instituições em geral

- **Vencer a cultura de que é melhor investir em tecnologia do que em treinamento e na implantação de boas políticas**
 - quantas instituições realmente implementam tecnologias com base em uma análise de risco?
- **Definir políticas de segurança**
 - direitos e responsabilidades de cada um em relação:
 - à segurança dos recursos computacionais que utiliza
 - as penalidades às quais está sujeito, caso não a cumpra
 - permite deixar claro o comportamento esperado de cada um
 - casos de mau comportamento, que estejam previstos na política, podem ser tratados de forma adequada pelas partes envolvidas
 - pode conter outras políticas específicas, como de: senhas, *backups*, privacidade, confidencialidade, uso aceitável
- **Ir além do “*compliance*”**
- **Investir em treinamento e conscientização de usuários finais**

Desafios – Como melhorar o cenário geral

- **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**

Conscientização de usuários finais (1/4)

Portal Internet Segura

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



Campanha Antispam.br

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



Conscientização de usuários finais (2/4)

Cartilha de Segurança para Internet 4.0

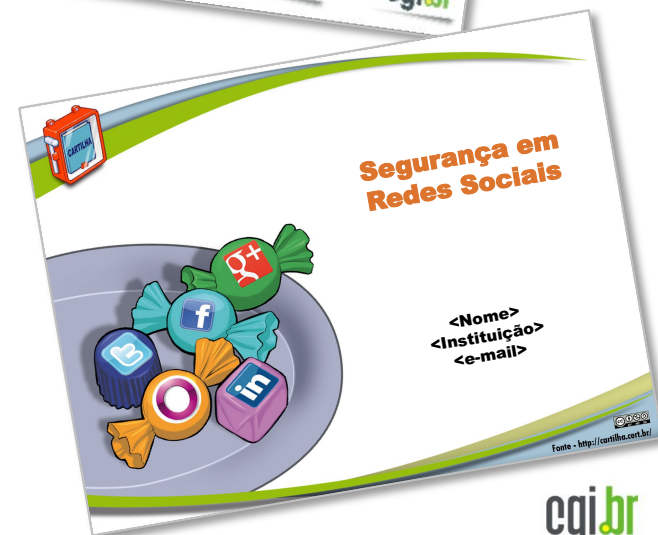
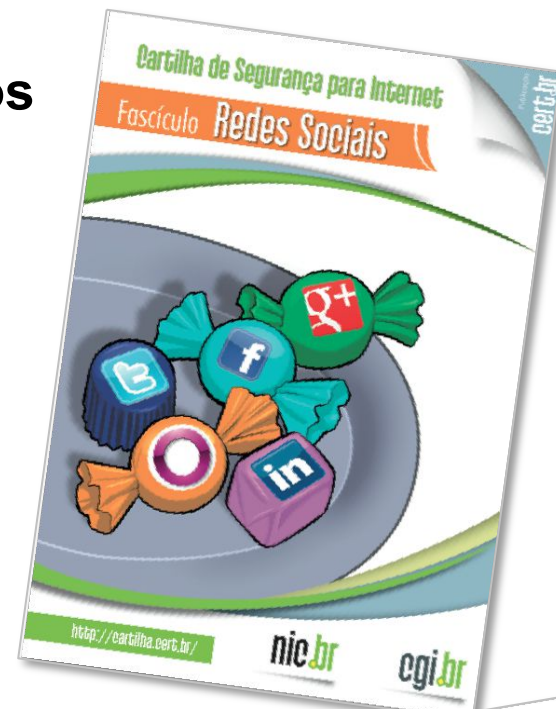
- 2ª Edição do Livro
- Novas recomendações, em especial sobre:
 - segurança e privacidade em redes sociais
 - segurança no uso de dispositivos móveis
- Reestruturada
 - ilustrada
 - em HTML5
 - formato EPub
- Nova licença
 - *Creative Commons (CC BY-NC-ND 3.0)*



Conscientização de usuários finais (3/4)

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



Conscientização de usuários finais (4/4)

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/>

