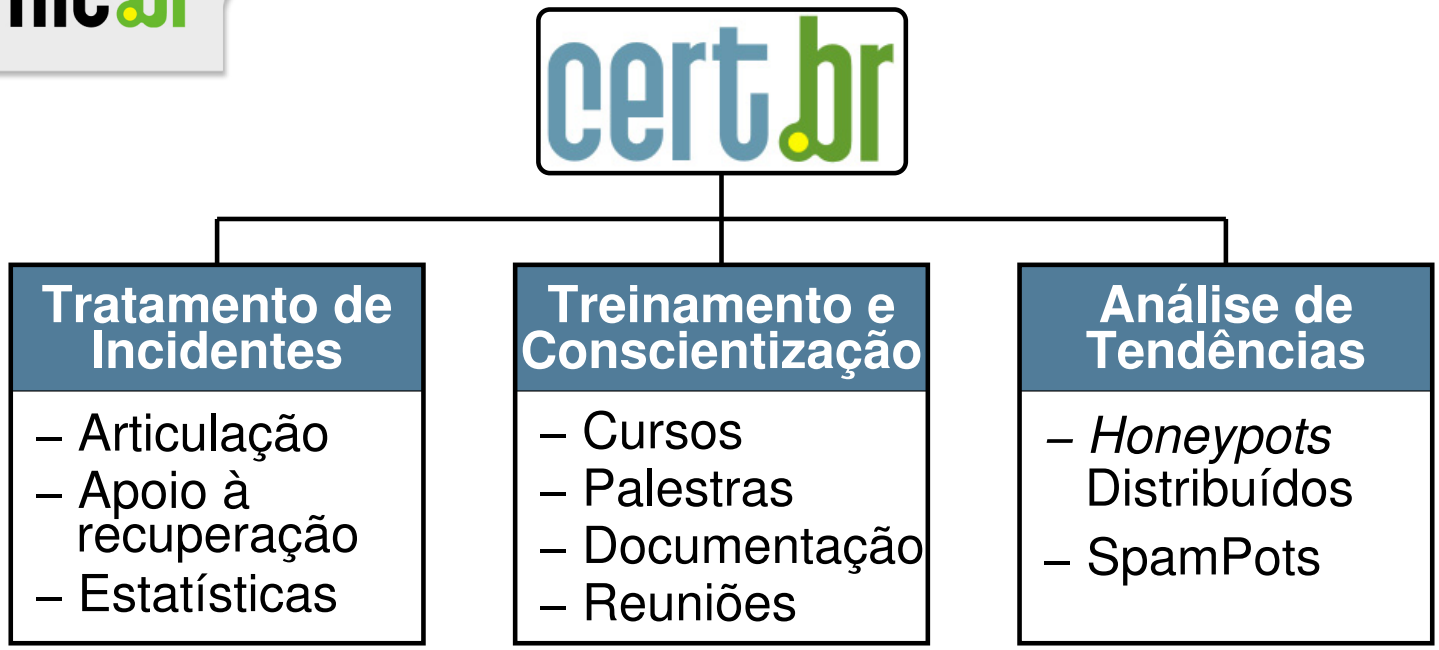
Códigos maliciosos e o (sub)mundo *das botnets*

Lucimara Desiderá
lucimara@cert.br

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



SEI Partner
Carnegie Mellon

FIRST
Improving Security Together
MEMBER

APWG
RESEARCH PARTNER
www.antiphishing.org

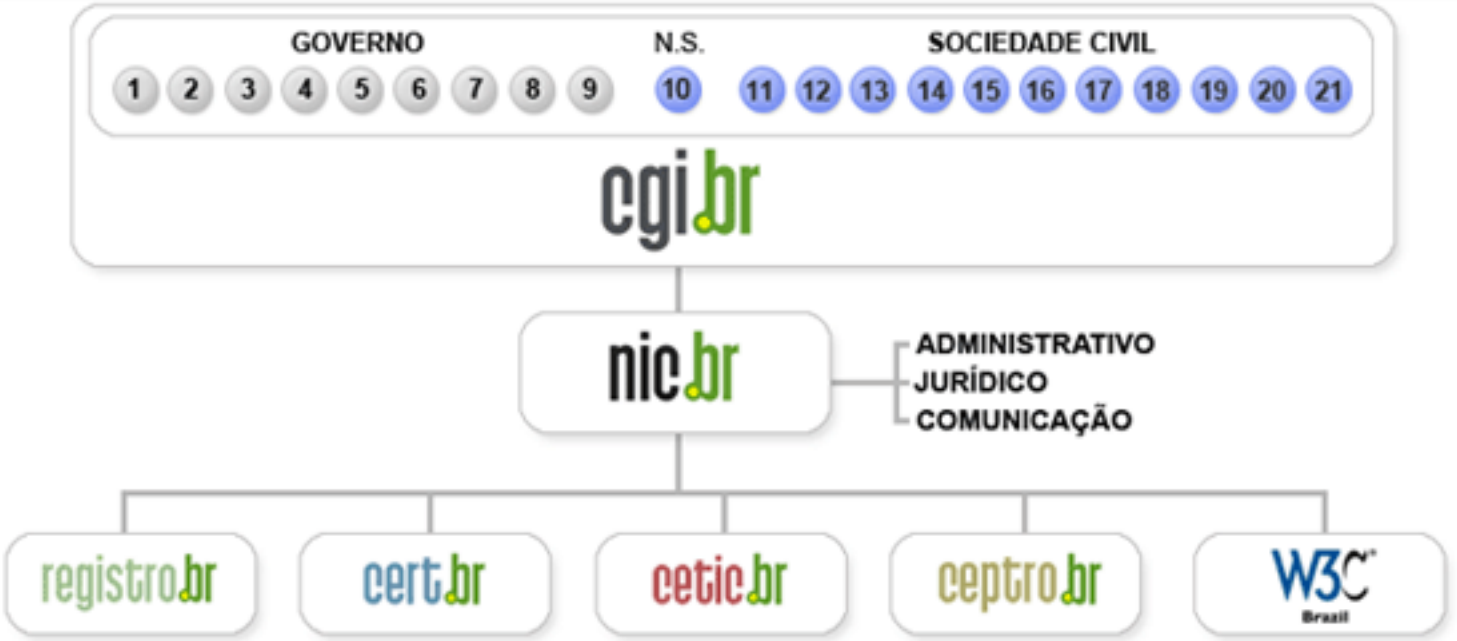
The Honeynet PROJECT

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**

http://www.cert.br/sobre/

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

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/

Agenda

- Códigos maliciosos
- *Botnets*
  - Motivações
- Cenário de Incidentes de Segurança
- Combate a *botnets*
- Como se proteger
  - Boas práticas

Códigos maliciosos (*malware*)

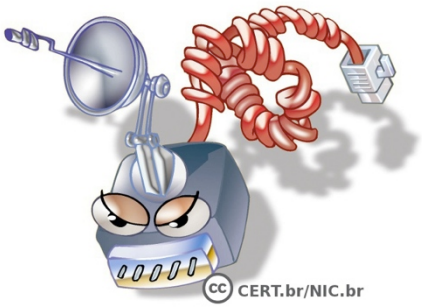
Códigos Maliciosos

Programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador

- **principais tipos:**

Vírus	***Backdoor***
Worm	***Trojan***
Spyware	***Rootkit***
Bot	***Botnet***

Bot



Programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador

Dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente

- **computador infectado = zumbi**

Propagação

- Exploração de vulnerabilidades

  Ex: página *Web* com navegador vulnerável

- Ação direta de atacantes

- Execução de arquivos
  - *download* na *Web*
  - redes sociais
  - *links* ou anexos de mensagens eletrônicas (*e-mail*, IM)
  - compartilhamento de recursos (ex: P2P, mídias removíveis)
  - auto-execução de mídias removíveis infectadas

Resumo Comparativo (1/4)

Códigos Maliciosos							
	Vírus	*Worm*	*Bot*	*Trojan*	*Spyware*	*Backdoor*	*Rootkit*
Como é obtido:							
Recebido automaticamente pela rede		✔	✔				
Recebido por *e-mail*	✔	✔	✔	✔	✔		
Baixado de *sites* na Internet	✔	✔	✔	✔	✔		
Compartilhamento de arquivos	✔	✔	✔	✔	✔		
Uso de mídias removíveis infectadas	✔	✔	✔	✔	✔		
Redes sociais	✔	✔	✔	✔	✔		
Mensagens instantâneas	✔	✔	✔	✔	✔		
Inserido por um invasor		✔	✔	✔	✔	✔	✔
Ação de outro código malicioso		✔	✔	✔	✔	✔	✔

Resumo Comparativo (2/4)

Códigos Maliciosos							
	Vírus	*Worm*	*Bot*	*Trojan*	*Spyware*	*Backdoor*	*Rootkit*
Como ocorre a instalação:							
Execução de um arquivo infectado	✔						
Execução explícita do código malicioso		✔	✔	✔	✔		
Via execução de outro código malicioso						✔	✔
Exploração de vulnerabilidades		✔	✔			✔	✔

Resumo Comparativo (3/4)

Códigos Maliciosos							
	Vírus	*Worm*	*Bot*	*Trojan*	*Spyware*	*Backdoor*	*Rootkit*
Como se propaga:							
Insere cópia de próprio em arquivos	✔						
Envia cópia de si próprio automaticamente pela rede		✔	✔				
Envia cópia de si próprio automaticamente por *e-mail*		✔	✔				
Não se propaga				✔	✔	✔	✔

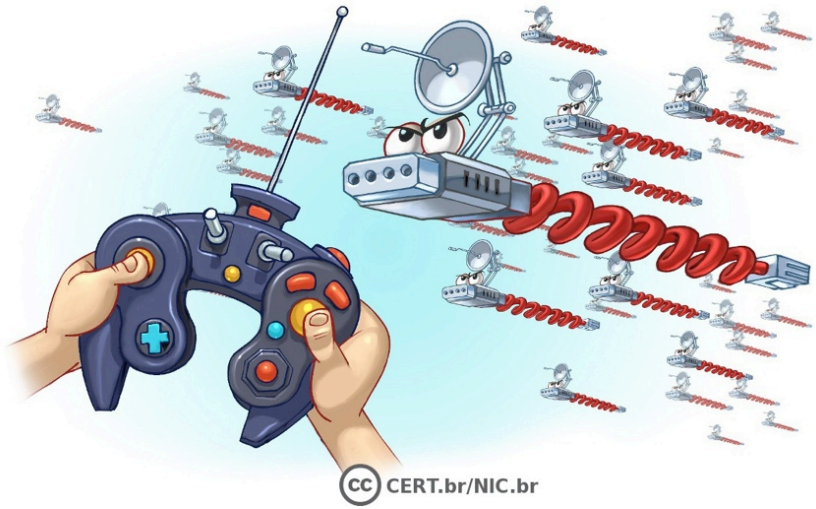
Resumo Comparativo (4/4)

Códigos Maliciosos							
	Vírus	*Worm*	*Bot*	*Trojan*	*Spyware*	*Backdoor*	*Rootkit*
Ações maliciosas mais comuns:							
Altera e/ou remove arquivos	✔			✔			✔
Consome grande quantidade de recursos		✔	✔				
Furta informações sensíveis			✔	✔	✔		
Instala outros códigos maliciosos		✔	✔	✔			✔
Possibilita o retorno do invasor						✔	✔
Envia *spam* e *phishing*			✔				
Desfere ataques na Internet		✔	✔				
Procura se manter escondido	✔				✔	✔	✔

Botnet

Botnet

Rede formada por centenas/milhares de computadores zumbis



- **permite potencializar as ações danosas dos *bots***
- **quanto mais *bots* mais potente é a *botnet***
- **controlador: *Command and Control (C&C)***

Comando e Controle

- **Comunicação**
  - **IRC**
  - **HTTP**
  - **P2P**
- **Tendências de gerenciamento e defesa**
  - **Novos mecanismos de troca de mensagens**
    - **DNS *covert channel***
    - ***ICMP***
    - **Twitter / Facebook**
  - **Criptografia**
  - **Ofuscação**
  - **Autenticação**
  - ***Fast-flux service networks***
  - ***Domain Generation Algorithms (DGA)***

Usos

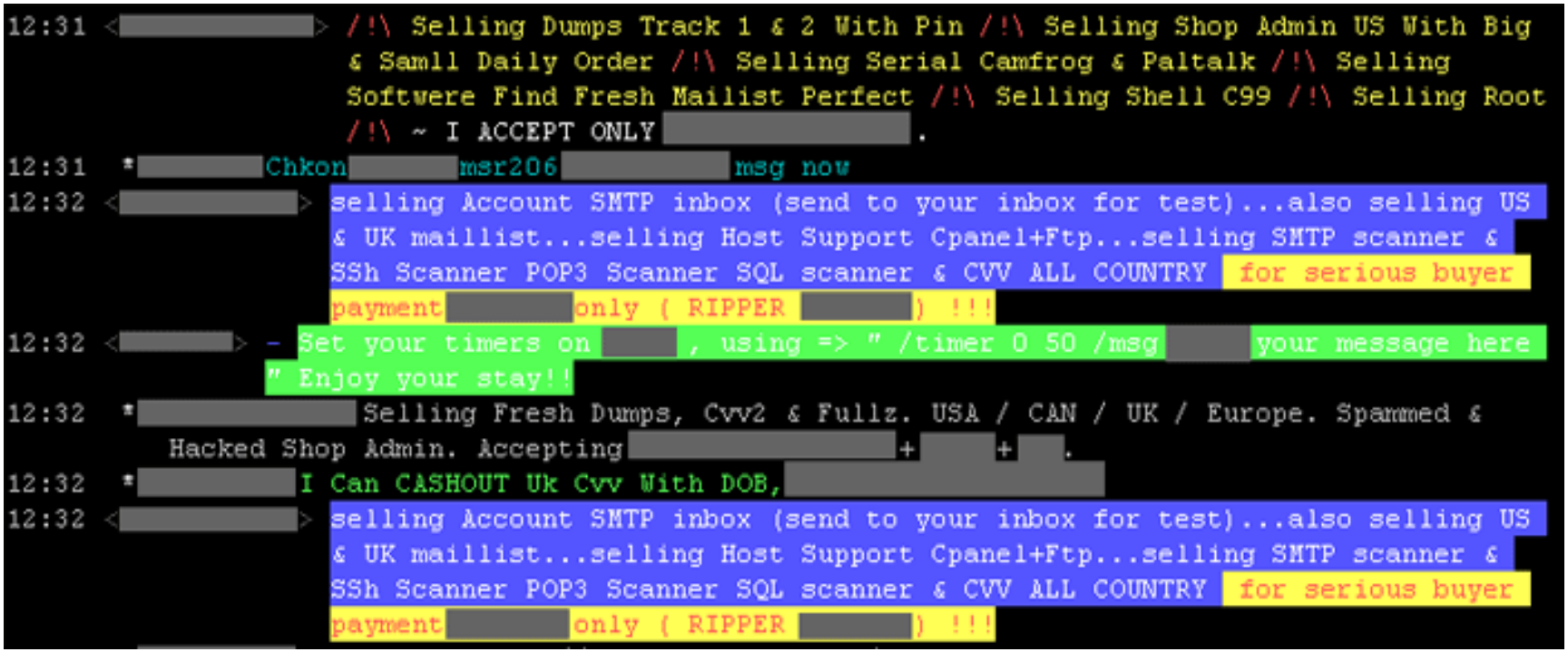
- **Coleta de informações**
  - **dados pessoais**
  - **espionagem**
- **Ataques de negação de serviço (DDoS)**
  - **ativismo político**
  - **extorsão**
- **Envio de *spam* e *phishing***

- **Propagação de código malicioso**
  - ***Pay per Install (PPI)***
  - ***Trojan*, *worm*, *spyware*, *adware***
- ***Click Fraud***

Motivações

Motivações

- Desejo de autopromoção
- Política / Ideológica
- **FINANCEIRA**
  - **mercado negro**



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

Motivações - Mercado Negro (cont.)

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

Motivações - Mercado Negro (cont.)

- SOCKS bot (to get around firewalls): $100
- Email spam: $10 per one million emails
- Email spam (using a customer database): $50-$500 per one million emails
- SMS spam: $3-$150 per 100-100,000 messages
- ZeuS source code: $200-$500
- Windows rootkit (for installing malicious drivers): $292
- Hacking Facebook or Twitter account: $130
- Hacking Gmail account: $162
- Hacking corporate mailbox: $500

Botnet Prices

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

Distributed Denial-of-Service Service Prices

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

Pay-per-Install Service Prices

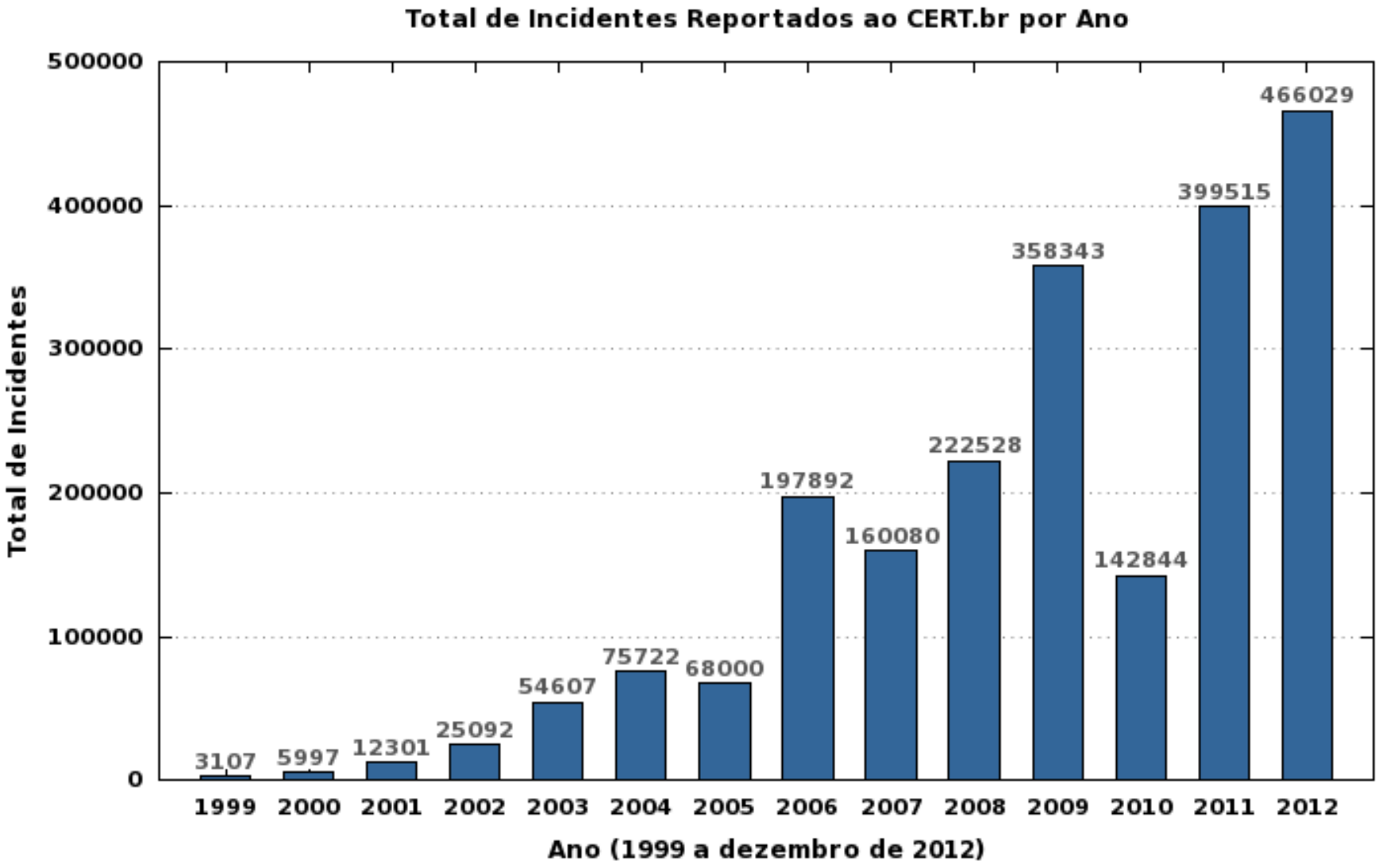
Offering	Price per 1,000 Downloads
Australia (AU)	US$300-550
Great Britain (UK)	US$220-300
Italy (IT)	US$200-350
New Zealand (NZ)	US$200-250
Spain (ES), Germany (DE), or France (FR)	US$170-250
United States (US)	US$100-150
Global mix	US$12-15
European mix	US$80
Russia (RU)	US$100

Fonte:Read Russian Underground 101 - Trend Micro
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf

Incidentes de Segurança

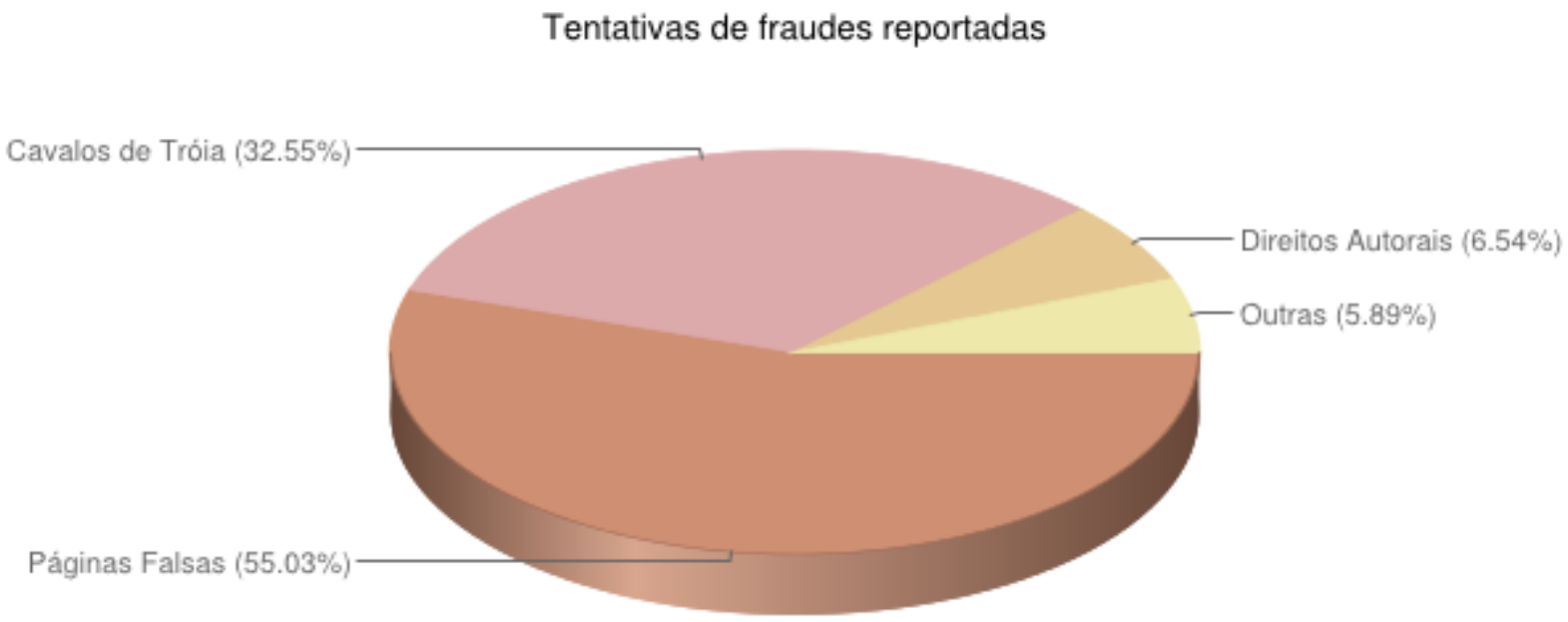
Fonte: Estatísticas CERT.br
http://www.cert.br/stats/incidentes/

Incidentes reportados ao CERT.br



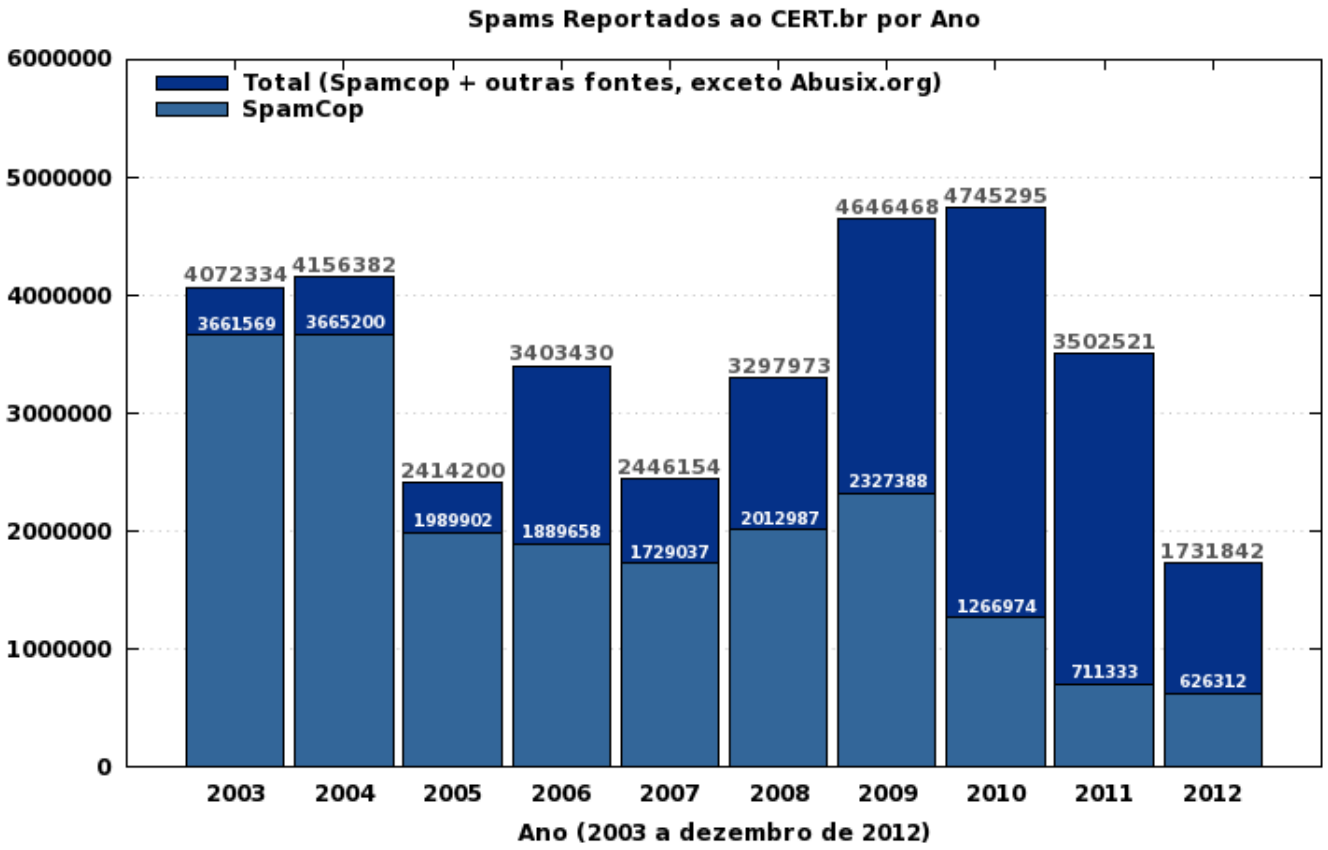
Tipos de ataque – 2012

Tentativas de fraudes – 2012



Combate a *botnets*

Combate

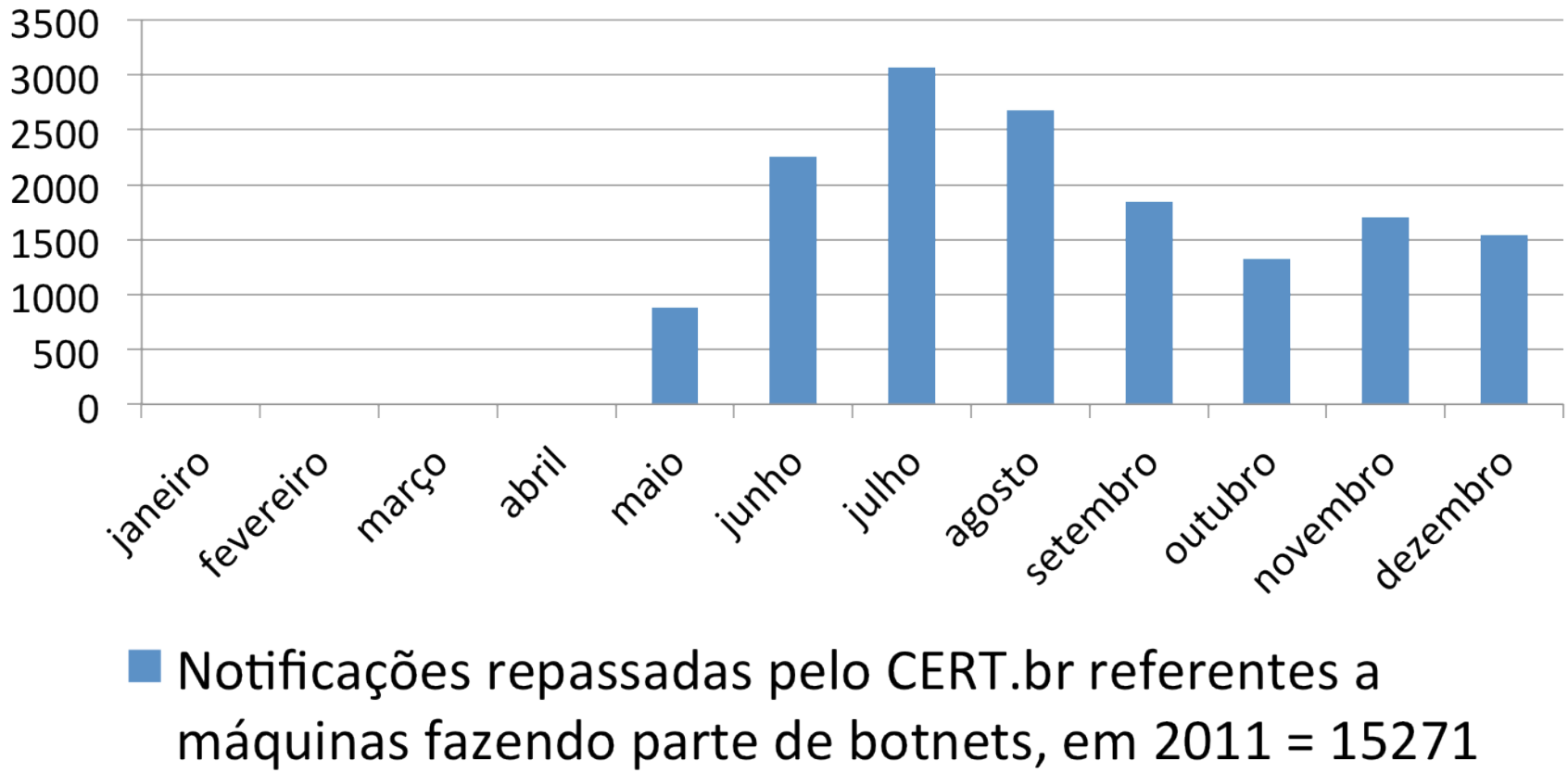


Fonte: Estatísticas CERT.br – http://www.cert.br/stats/spam/

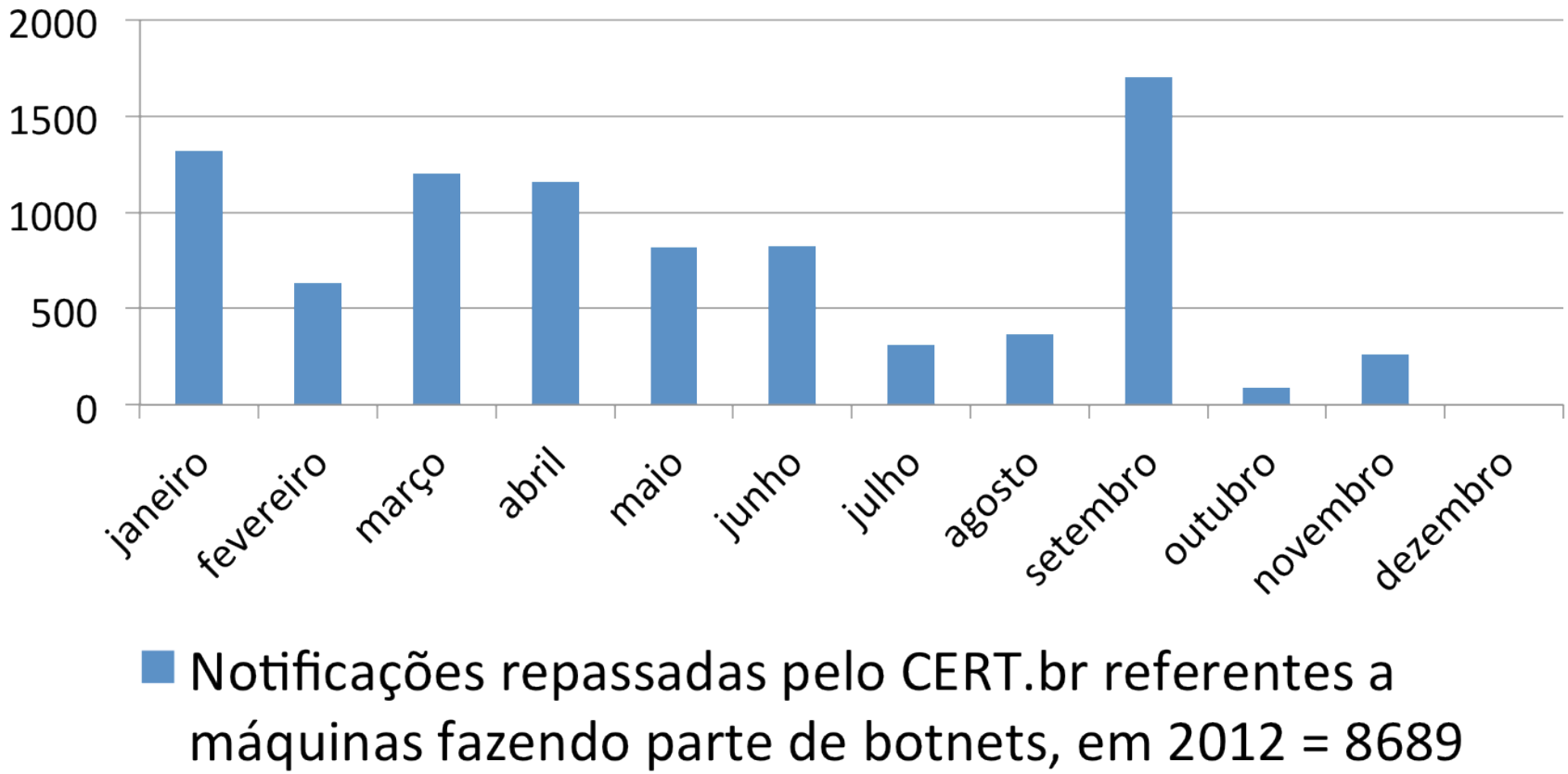
Derrubada de *botnets* diminui drasticamente número de *spams*

http://idgnow.uol.com.br/internet/2013/01/23/derrubada-de-botnets-diminui-drasticamente-numero-de-spams/

Notificações repassadas pelo CERT.br - 2011



Notificações repassadas pelo CERT.br - 2012



Como se proteger (como não fazer parte de uma *botnet*)

Proteção

- **O que torna as *botnets* tão potentes é a imensa quantidade de computadores infectados existentes**

- **quanto menos computadores infectados menos potentes elas serão e menores poderão ser os danos causados**

Faça a sua parte!!!!

Proteja seu Computador

- **Mantenha seu computador seguro:**
  - **com todas as atualizações aplicadas**
  - **com todos os programas instalados com as versões mais recentes**
- **Use mecanismos de segurança**
  - ***firewall* pessoal, *antimalware, antiphishing*, *antispam***
  - **complementos, extensões, *plugins***
- **Use apenas programas originais**
- **Use as configurações de segurança já disponíveis**
- **Seja cuidadoso ao instalar aplicativos desenvolvidos por terceiros**

Mantenha uma Postura Preventiva

- **Não acesse *sites* ou siga *links***
  - **recebidos de mensagens eletrônicas**
  - **em páginas sobre as quais não se saiba a procedência**
- **Não confie apenas no remetente da mensagem, pois ela pode ter sido enviada de:**
  - **máquinas infectadas**
  - **contas falsas ou invadidas**
- **Proteja sua privacidade, evite divulgar:**
  - **dados pessoais ou de familiares e amigos**
  - **informações sobre seu cotidiano**
  - **informações sensíveis, como:**
    - **senhas**
    - **números de cartão de crédito**

Proteja suas Contas e Senhas (1/2)

- **Utilize senhas contendo:**
  - **grande quantidade de caracteres**
  - **diferentes tipos de caracteres**
  - **números aleatórios**

- **Evite usar:**
  - **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.**

Proteja suas Contas e Senhas (2/2)

- **Dicas de elaboração**
  - **selecione caracteres de uma frase**
    - **“O Cravo brigou com a Rosa debaixo de uma sacada” ➔ ”?OCbcaRddus”**
  - **utilize uma frase longa**
    - **“1 dia ainda verei os aneis de Saturno!!!”**
  - **faça substituições de caracteres:**
    - **“Sol, astro-rei do Sistema Solar” ➔ “SS0l, asstrr0-rrei d0 SSisstema SS0larr”**
- **Procure trocar regularmente suas senhas**
- **Evite usar o usuário “administrador”**

Informe-se e Mantenha-se Atualizado

Portal Internet Segura

http://www.internetsegura.br/

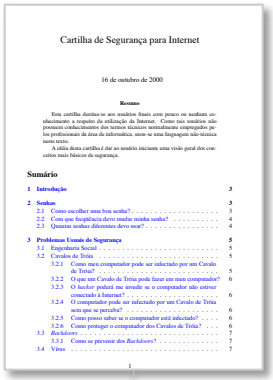
INTERNET SEGURA.BR

Campanha Antispam.br

http://www.antispam.br/

Cartilha de Segurança para Internet – Linha do Tempo

1.0


Cartilha de Segurança para Internet

16 de outubro de 2000

Resumo

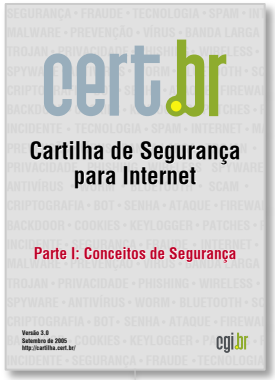
Esta cartilha destina-se aos usuários finais com pouco ou nenhum conhecimento a respeito da utilização da Internet. Como tais usuários não possuem conhecimentos dos termos técnicos normalmente empregados pelos profissionais da área de informática, neste se uma linguagem não-técnica neste texto.

A idéia desta cartilha é dar ao usuário iniciante uma visão geral dos conceitos mais básicos de segurança.

Sumário

- 20 páginas
- conceitos básicos
- dúvidas frequentes

3.0



- incluída parte sobre códigos maliciosos
- folder de dicas

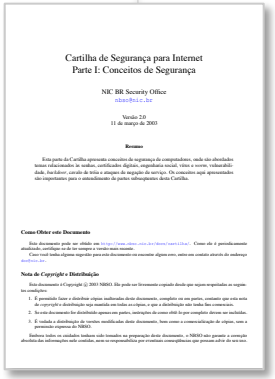
- ilustrada
- eBook (ePub)
- novos temas: redes sociais e dispositivos móveis

4.0

2000 2003 2005 2006 2012

- organizada em partes
- incluído o tema de fraudes na Internet

2.0


Cartilha de Segurança para Internet
Parte I: Conceitos de Segurança

NIC BR Security Office
nbso@nic.br

Versão 2.0
11 de março de 2003

Resumo

Como Obter este Documento

Nota de *Copyright* e Distribuição

3.1

- lançada como livro

- fascículos e *slides*

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:**

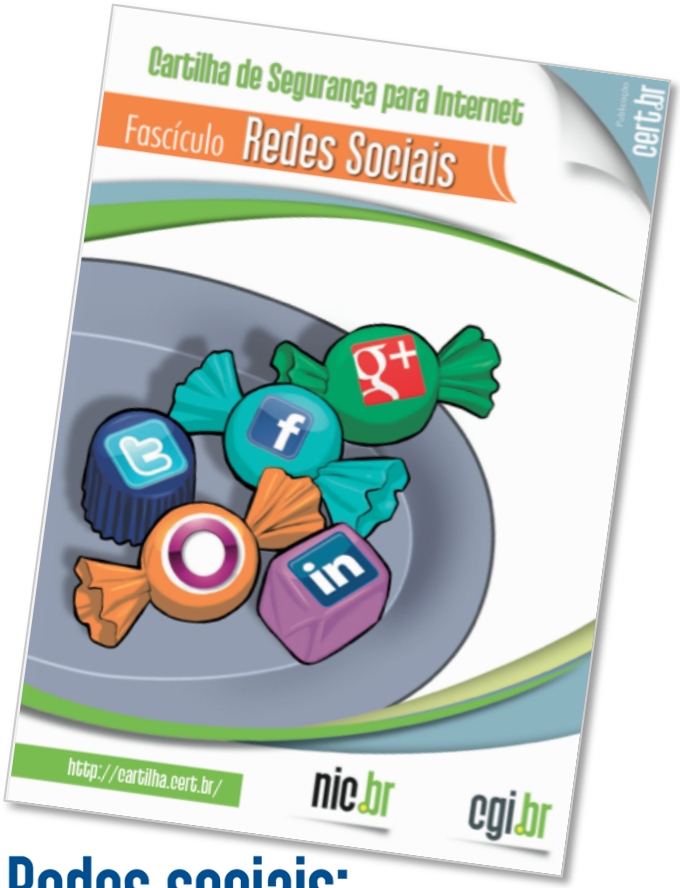
- **ministrar palestras e treinamentos**
- **complementar conteúdos de aulas**
- **licença CC BY-NC-SA 3.0 Brasil**

Redes Sociais – 08/2012

Senhas – 10/2012

Comércio Eletrônico – 11/2012

Privacidade – 02/2013



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?

Lucimara Desiderá - lucimara@cert.br
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/