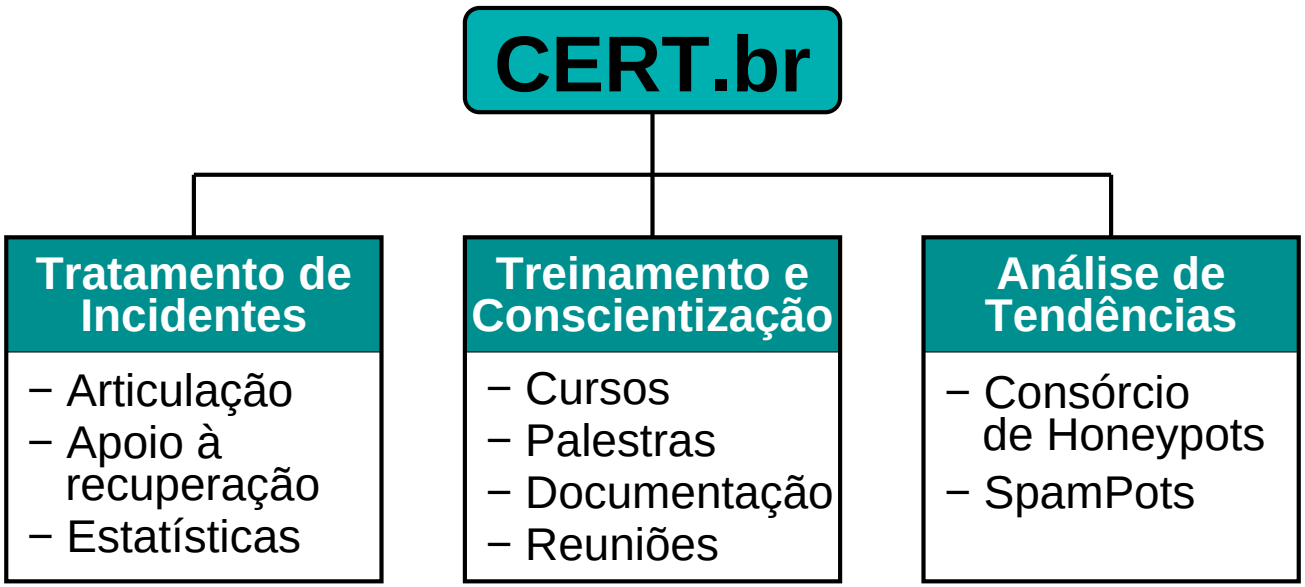
Principais Ameaças na Internet e Recomendações para Prevenção

Cristine Hoepers
Gerente Geral
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

Sobre o CERT.br

Criado em 1997 como ponto focal nacional para tratar incidentes de segurança relacionados com as redes conectadas à Internet no Brasil



FIRST Improving Security Together MEMBER

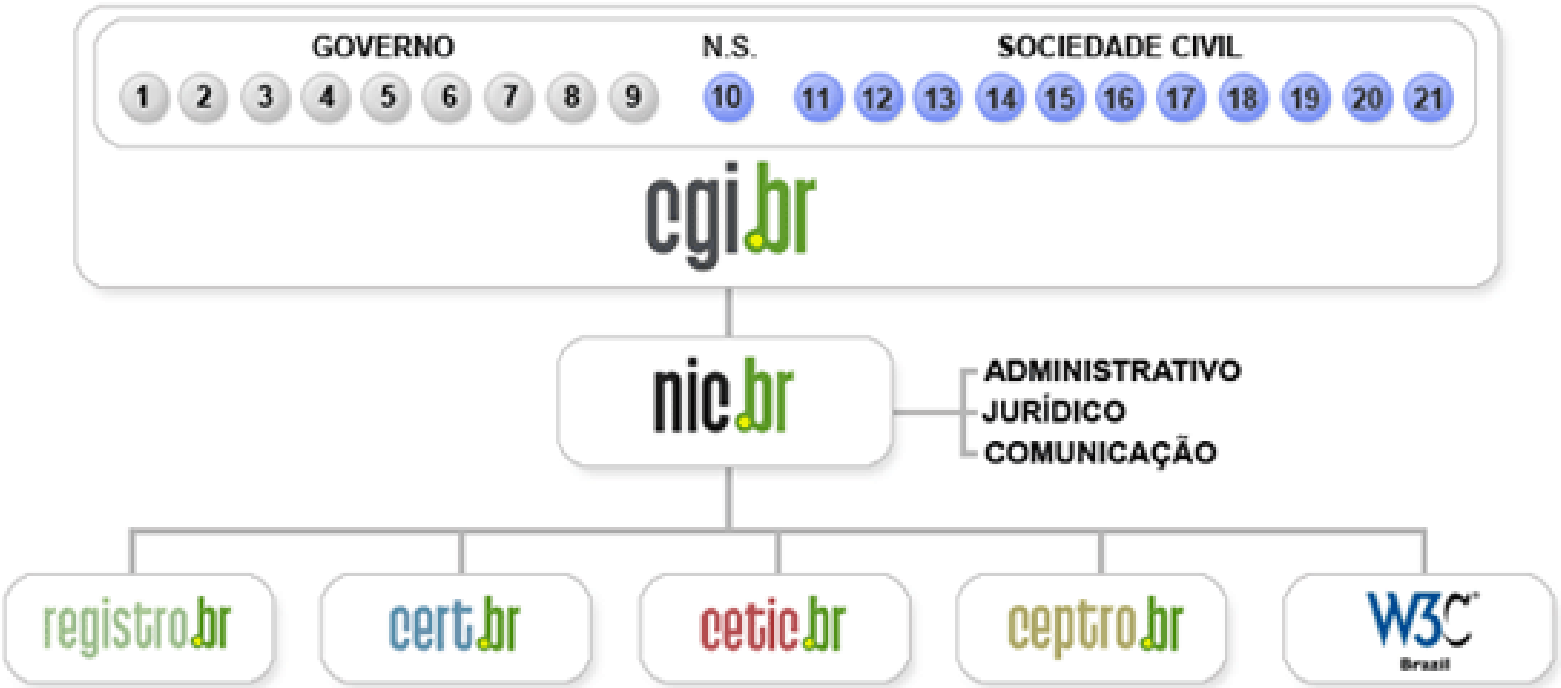
APWG RESEARCH PARTNER www.antiphishing.org

SEI Partner CERT Courses

The Honeynet PROJECT®

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

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

Motivação

- Analisar dados sobre segurança na Internet, para entendermos o problema
- Discutir a evolução dos problemas de segurança desde a concepção da Internet até os dias atuais
- Discutir possíveis formas de proteção, isto é, o que podemos fazer para usar a Internet de modo mais seguro

Agenda

- Evolução dos Problemas de Segurança
- Situação Atual
  - Características dos Ataques
  - Características dos Atacantes
  - Facilitadores para este Cenário
- Incidentes de Segurança no Brasil
  - Tentativas de Fraude Tratadas
  - Ataques a Smartphones
- Prevenção
- Referências

Evolução dos Problemas de Segurança

Problemas de Segurança (1/2)

Final dos Anos 60

- Internet – comunidade de pesquisadores
- Projeto não considera implicações de segurança

Anos 80

- Invasores com alto conhecimento
- Dedicação por longos períodos – poucos ataques
- Primeiro *worm* com maiores implicações de segurança
  - Aproximadamente 10% da Internet na época
  - Mobilização em torno do tema segurança
  - Criação do CERT/CC 15 dias após

ftp://coast.cs.purdue.edu/pub/doc/morris_worm/
http://www.cert.org/archive/pdf/03tr001.pdf
http://www.ietf.org/rfc/rfc1135.txt

Problemas de Segurança (2/2)

Anos 1991–2001

- Uso da “engenharia social” em grande escala
- Ataques remotos aos sistemas
- Popularização de: cavalos de tróia, furto de senhas, varreduras, *sniffers*, DoS, etc
- Ferramentas automatizadas para realizar invasões e ocultar a presença dos invasores (*rootkits*)

Anos 2002–2007

- Explosão no número de códigos maliciosos
  - *worms*, *bots*, cavalos de tróia, vírus, *spyware*
  - múltiplas funcionalidades e vetores de ataque, eficiente, aberto, adaptável, controle remoto
  - Praticamente não exige interação com o invasor

Situação Atual

Situação Atual (1/3)

Características dos Ataques

- Amplo uso de ferramentas automatizadas de ataque
- *Botnets*
  - Redes formadas por diversos computadores infectados, controlados remotamente
  - Usadas para envio de *scams*, *phishing*, invasões, esquemas de extorsão
- Redes mal configuradas sendo abusadas para realização de todas estas atividades
  - sem o conhecimento dos donos
- **Usuários finais passaram a ser alvo**

Situação Atual (2/3)

Características dos Atacantes

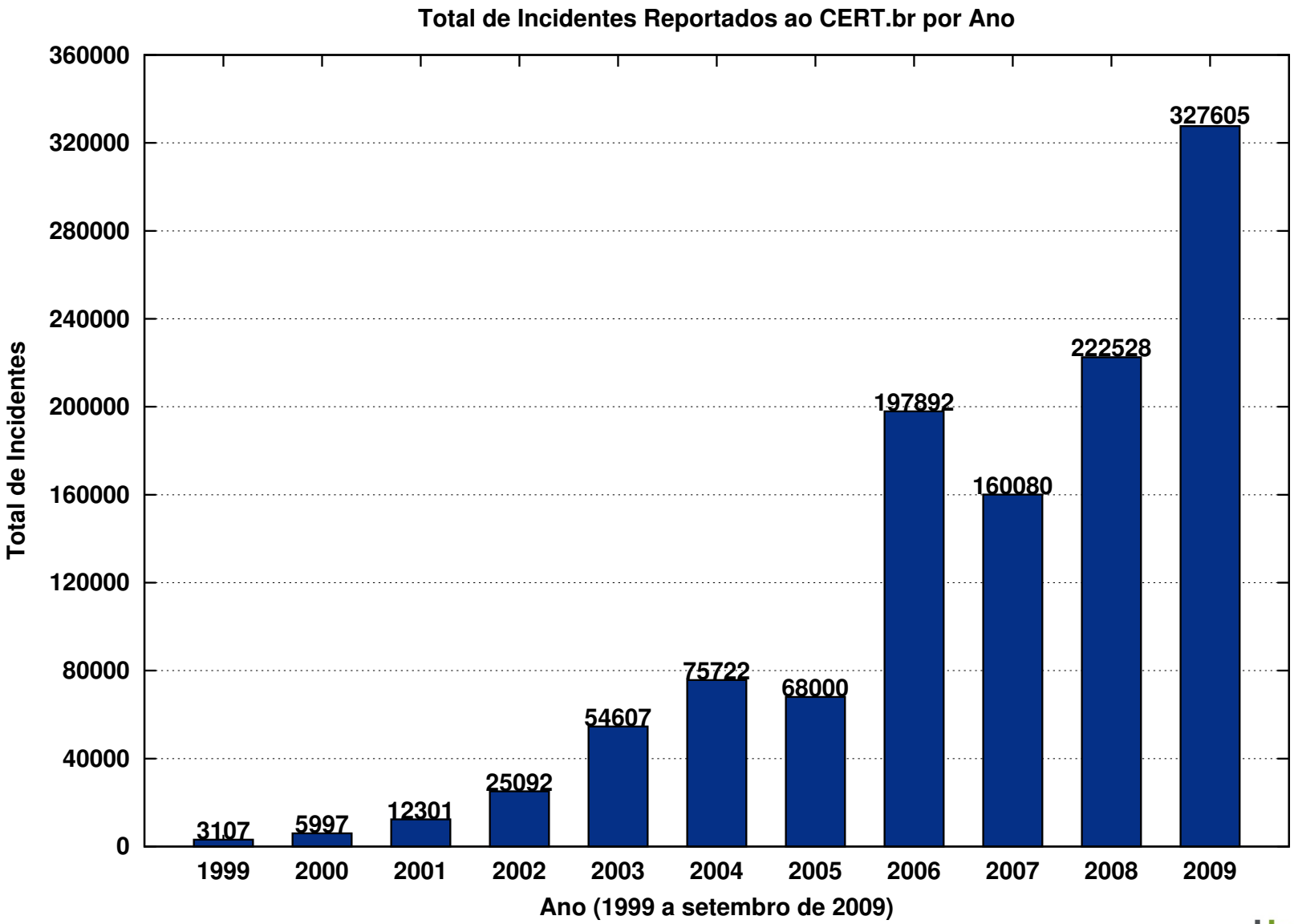
- Em sua maioria pessoal com pouco conhecimento técnico que utiliza ferramentas prontas
- Trocam informações no *underground*
- Usam como moedas de troca
  - senhas de administrador/`root`
  - novos *exploits*
  - contas/senhas de banco, números de cartão de crédito
  - *bots*/*botnets*
- Atacantes + *spammers*
- Crime organizado
  - Aliciando *spammers* e invasores
  - Injetando dinheiro na "economia *underground*"

Situação Atual (3/3)

Facilitadores para este Cenário

- Pouco enfoque em segurança de *software* e programação segura
  - vulnerabilidades freqüentes
  - códigos maliciosos explorando vulnerabilidades em curto espaço de tempo
- Sistemas e redes com grau crescente de complexidade
- Organizações sem políticas de segurança ou de uso aceitável
- Sistemas operacionais e *softwares* desatualizados
  - pouco intuitivo para o usuário
- Falta de treinamento

Incidentes de Segurança no Brasil



Ataques mais freqüentes – 2009

- Ataques a usuários finais
  - Fraudes, *bots*, *spyware*, etc
- Motivação financeira

Fraudes: histórico e cenário atual (1/2)

2001 *Keyloggers* enviados por *e-mail*, ataques de força bruta

2002–2003 *Phishing* e uso disseminado de DNSs comprometidos

2003–2004 Aumento dos casos de *phishing* mais sofisticados
- *Sites* coletores: processamento/envio de dados p/ contas de *e-mail*

2005–2006 *Spams* em nome de diversas entidades/temas variados
- *Links* para cavalos de tróia hospedados em diversos *sites*
- Vítima raramente associa o *spam* com a fraude financeira

2007 *downloads* involuntários (via JavaScript, ActiveX, etc) - Continuidade das tendências de 2005–2006

Fraudes: histórico e cenário atual (2/2)

2008–hoje

- Continuidade das tendências de 2005–2007
- *downloads* involuntários mais freqüentes, inclusive em grandes sites
  - casos publicados na mídia nos últimos meses incluem: sites principais da Vivo, da Oi e da Ambev
- *links* patrocinados do Google usando a palavra “banco” e nomes de instituições como “AdWords”
- *Malware* modificando arquivo *hosts* – antigo, mas ainda efetivo
- *Malware* modificando configuração de *proxy* em navegadores (arquivos PAC)
- *Malware* se registrando como Browser Helper Objects (BHO) em navegadores
- *Malware* validando, no site real, os dados capturados

Tentativas de Fraude Tratadas(1/3)

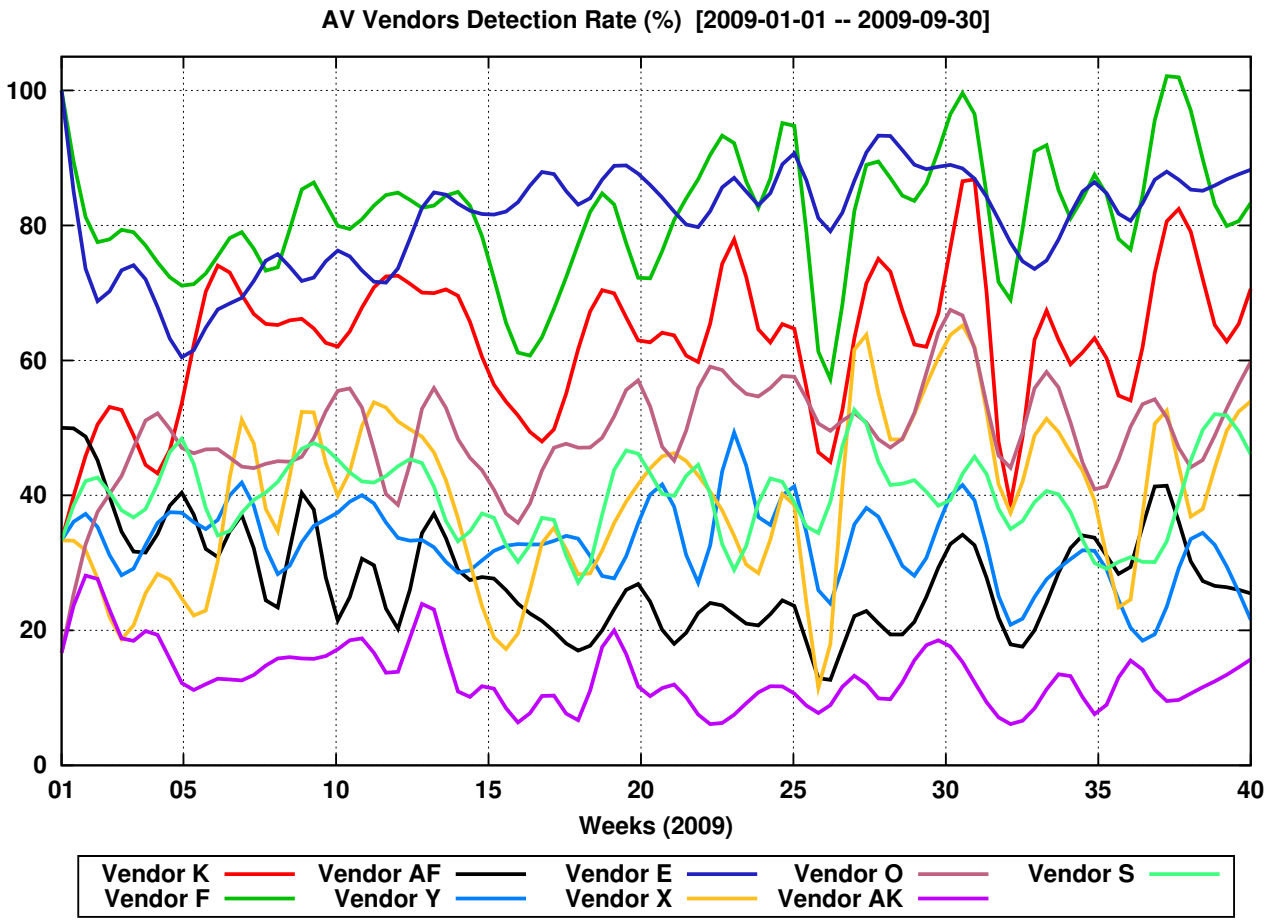
Estatísticas de *Malware** de 2006 a setembro de 2009:

Categoria	2006	2007	2008	2009/Q123
URLs únicas	**25.087**	**19.981**	**17.376**	**7.622**
Códigos maliciosos únicos (*hashes* únicos)	**19.148**	**16.946**	**14.256**	**5.705**
Assinaturas de Antivírus (únicas)	**1.988**	**3.032**	**6.085**	**2.647**
Assinaturas de Antivírus ("família")	**140**	**109**	**63**	**64**
Extensões de arquivos usadas	**73**	**112**	**112**	**79**
Domínios	**5.587**	**7.795**	**5.916**	**3.163**
Endereços IP únicos	**3.859**	**4.415**	**3.921**	**2.403**
Países de origem	**75**	**83**	**78**	**72**
Emails de notificação enviados pelo CERT.br	**18.839**	**17.483**	**15.499**	**6.879**

(*) Incluem *keyloggers*, *screen loggers*, *trojan downloaders* – não incluem *bots*/*botnets*, *worms*

Tentativas de Fraude Tratadas (2/3)

Taxas de Detecção dos Antivírus em 2009/Q123:

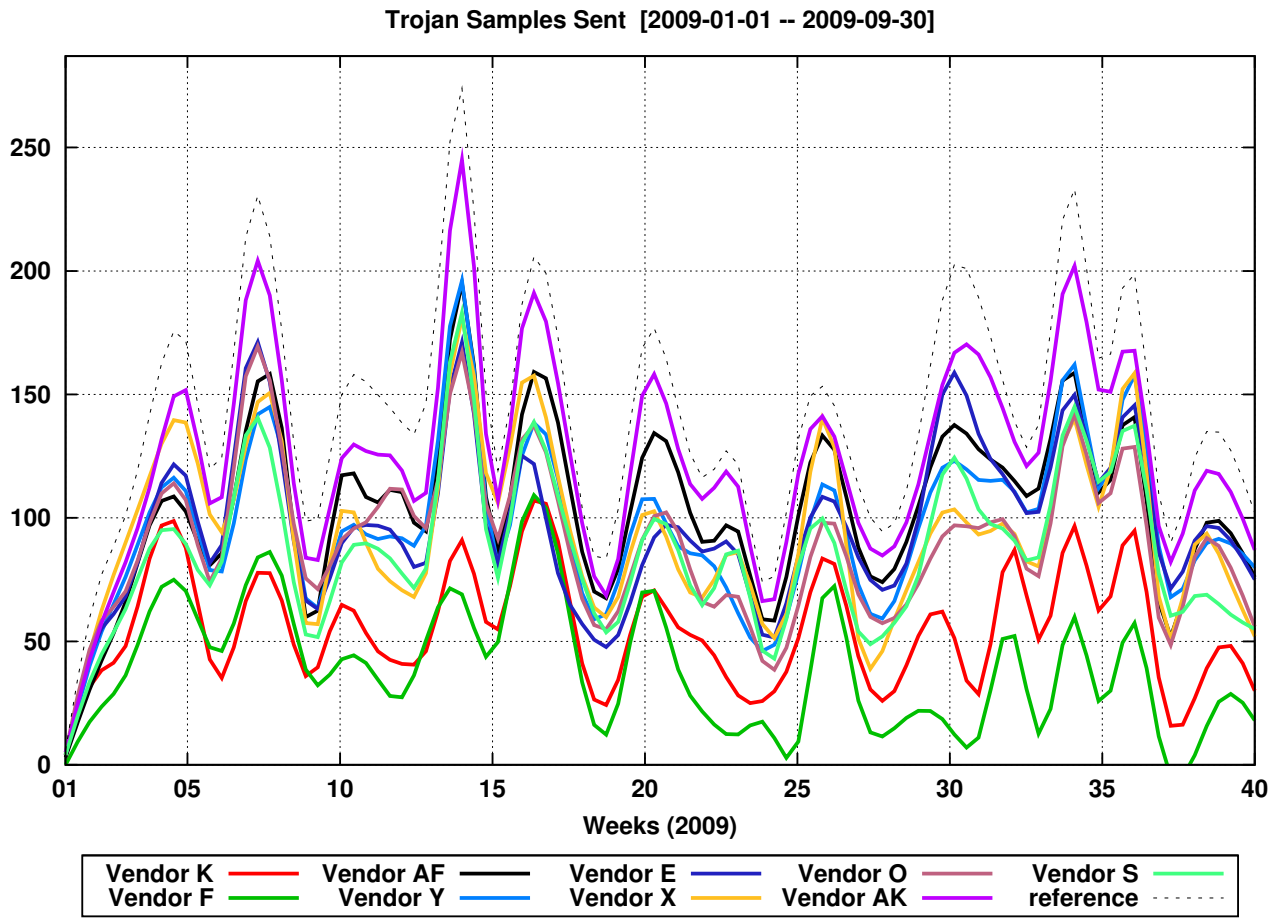


21% dos antivírus detectaram mais de 70% dos exemplares

70% dos antivírus detectaram menos de 50% dos exemplares

Tentativas de Fraude Tratadas (3/3)

Malwares enviados para 25+ Antivírus em 2009/Q123:



Casos de fraude relacionados a *malware* aumentaram ≈22% entre o segundo e o terceiro trimestre de 2009

Casos de páginas de *phishing* aumentaram ≈12% entre o segundo e o terceiro trimestre de 2009

Ataques a *Smartphones* (1/2)

Antigos vetores contra celulares

- *Bluetooth*
- MMS

Via 3G estão conectados diretamente à Internet

- possuem um Sistema Operacional completo
  - Windows CE, Linux, iPhone OS
- possuem aplicativos mais complexos
- permitem ler *e-mails*, abrir documentos, navegar, etc

Ataques a *Smartphones* (2/2)

Worm para iPhones abertos (*jailbrake*) já identificado

- o "desbloqueio" permite a instalação de qualquer *software*
- habilita uma senha padrão para o `root` (usuário administrador do sistema)
- o que o *worm* faz:
  - varre a Internet até encontrar um iPhone
  - tenta conectar no serviço SSH com a conta de `root` e a senha padrão
  - se tiver sucesso, tem controle total do sistema – troca a senha, furta a agenda e outros dados inseridos no telefone, e se junta a uma *botnet* para, então, continuar os ataques

Prevenção

Estamos nos Prevenindo?

Problemas de Segurança Encontrados:

	Nenhum	Vírus ou outro programa malicioso	Uso indevido de informações	Fraude financeira	Outro	Não sabe
2007	69	27	2	1	2	2
2008	68	28	1	1	ND	3

Medidas de Segurança Adotadas:

	Antivírus	*Firewall* pessoal	Outro programa	Nenhuma medida
2007	75	11	6	22
2008	70	10	4	28

Freqüência de Atualização do Antivírus:

	Diária	Semanal	Mensal	Trimestral	Automática	Não atualizou	Não sabe
2007	38	26	17	3	ND	8	7
2008	28	23	15	3	22	3	5

Fonte: Pesquisa TIC Domícilios – CETIC.br (http://www.cetic.br/)

O Que Fazer para se Prevenir

Instalar a última versão e aplicar as correções de segurança (*patches*)

- sistema operacional (checar horário da atualização automática)
- aplicativos (navegador, proc. de textos, leitor de *e-mails*, visualizador de imagens, PDFs e vídeos, etc)
- *Hardware* (*firmware* de *switches*, bases *wireless*, etc)

Utilizar Programas de Segurança

- *firewall* pessoal
- antivírus (atualizar as assinaturas diariamente)
- anti-*spyware*
- anti-*spam*
- extensões e *plugins* em navegadores (gerência de JavaScript, *cookies*, etc)

Melhorar a Postura On-line (1/2)

Não acessar *sites* ou seguir *links*

- recebidos por *e-mail* ou por serviços de mensagem instantânea
- em páginas sobre as quais não se saiba a procedência

Receber um *link* ou arquivo de pessoa ou instituição conhecida não é garantia de confiabilidade

- códigos maliciosos se propagam a partir das contas de máquinas infectadas
- fraudadores se fazem passar por instituições confiáveis

Não fornecer em páginas *Web*, *blogs* e *sites* de redes de relacionamentos:

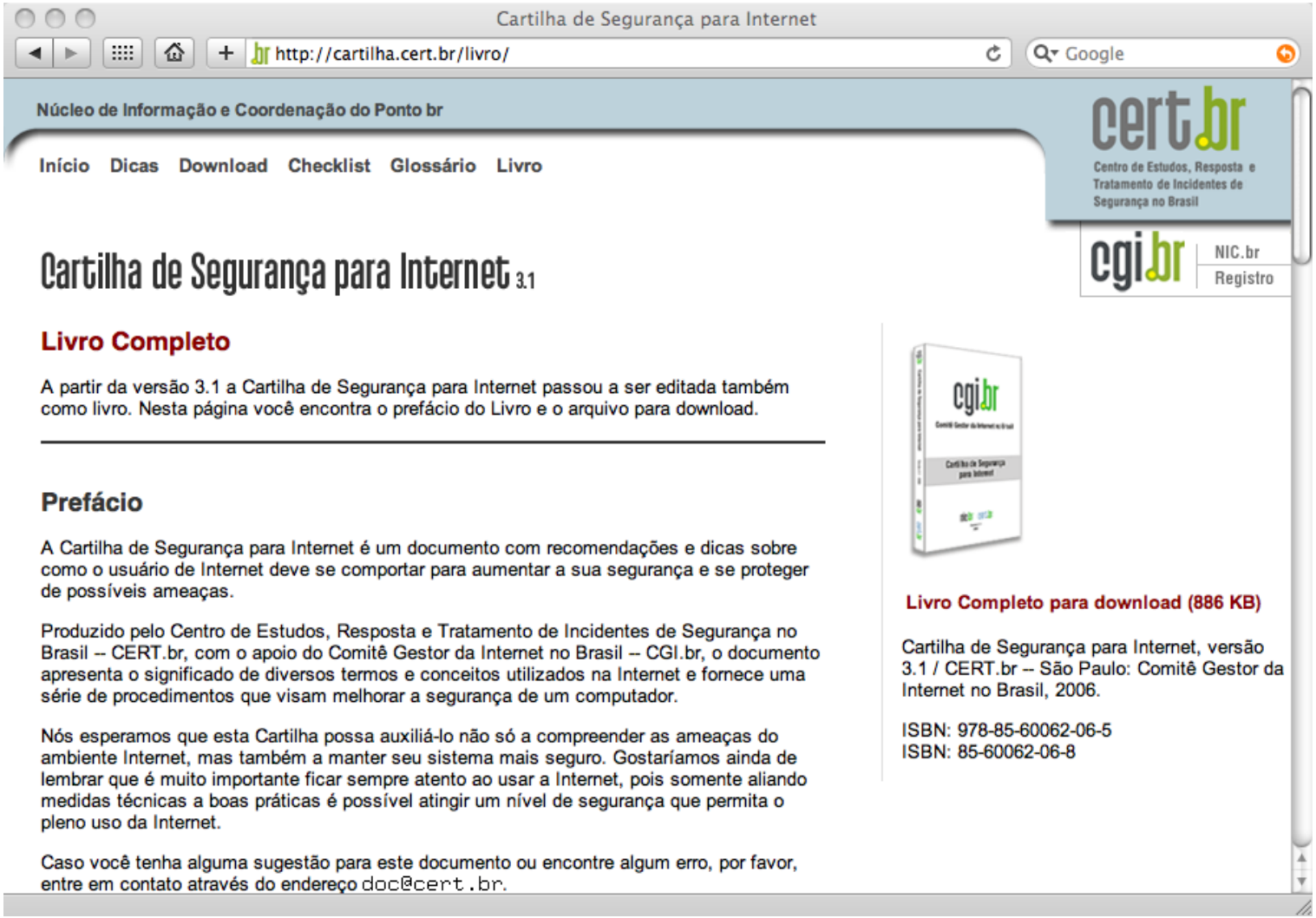
- seus dados pessoais ou de familiares e amigos (*e-mail*, telefone, endereço, data de aniversário, etc)
- dados sobre o computador ou sobre *softwares* que utiliza
- informações sobre o seu cotidiano
- informações sensíveis (senhas e números de cartão de crédito)

Melhorar a Postura On-line (2/2)

Precauções com contas e senhas

- utilizar uma senha diferente para cada serviço/*site*
- evitar senhas fáceis de adivinhar
  - nome, sobrenomes, números de documentos, placas de carros, números de telefones, datas que possam ser relacionadas com você ou palavras que façam parte de dicionários
- usar uma senha composta de letras, números e símbolos
- utilizar o usuário Administrador ou `root` somente quando for estritamente necessário
- criar tantos usuários com privilégios normais, quantas forem as pessoas que utilizam seu computador

Informar-se e Manter-se Atualizado (1/2)



http://cartilha.cert.br/

Informar-se e Manter-se Atualizado (2/2)

- **Site Antispam.br – Vídeos Educacionais no escopo das atividades da CT Anti-Spam do CGI.br**
  http://www.antispam.br/

Referências

- Esta Apresentação
  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 Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – CERT.br
  http://www.cert.br/
- Antispam.br
  http://www.antispam.br/
- Centro de Estudos sobre as Tecnologias da Informação e da Comunicação – CETIC.br
  http://www.cetic.br/