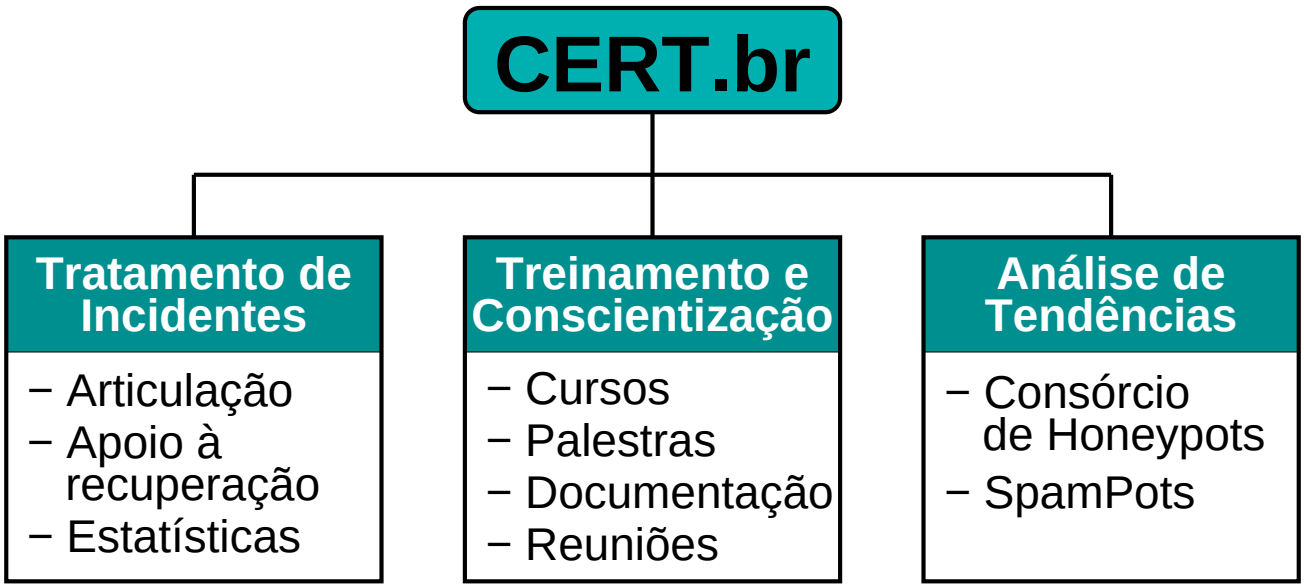
Incidentes de Segurança no Brasil: Principais Ameaças e Recomendações para Prevenção

Luiz Eduardo Roncato Cordeiro
cordeiro@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

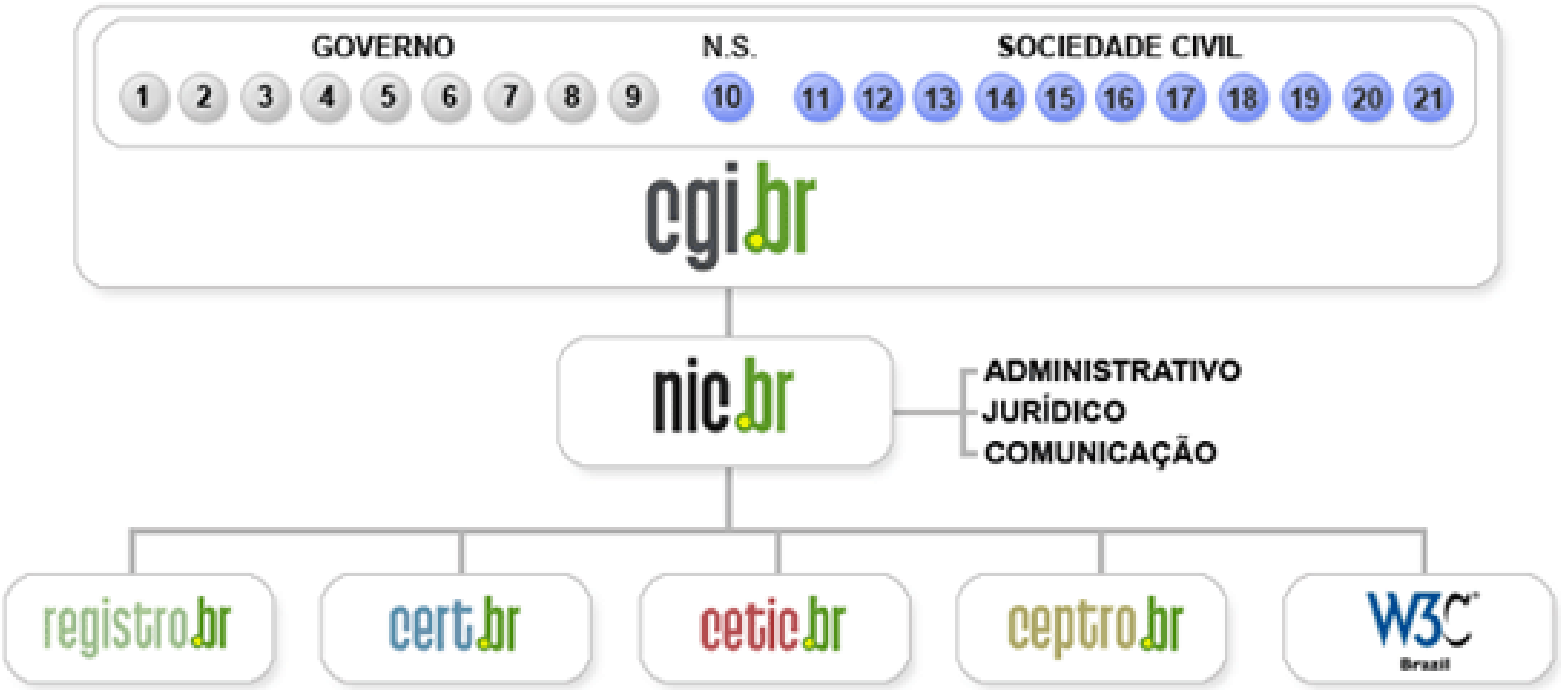
APWG RESEARCH PARTNER www.antiphishing.org

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

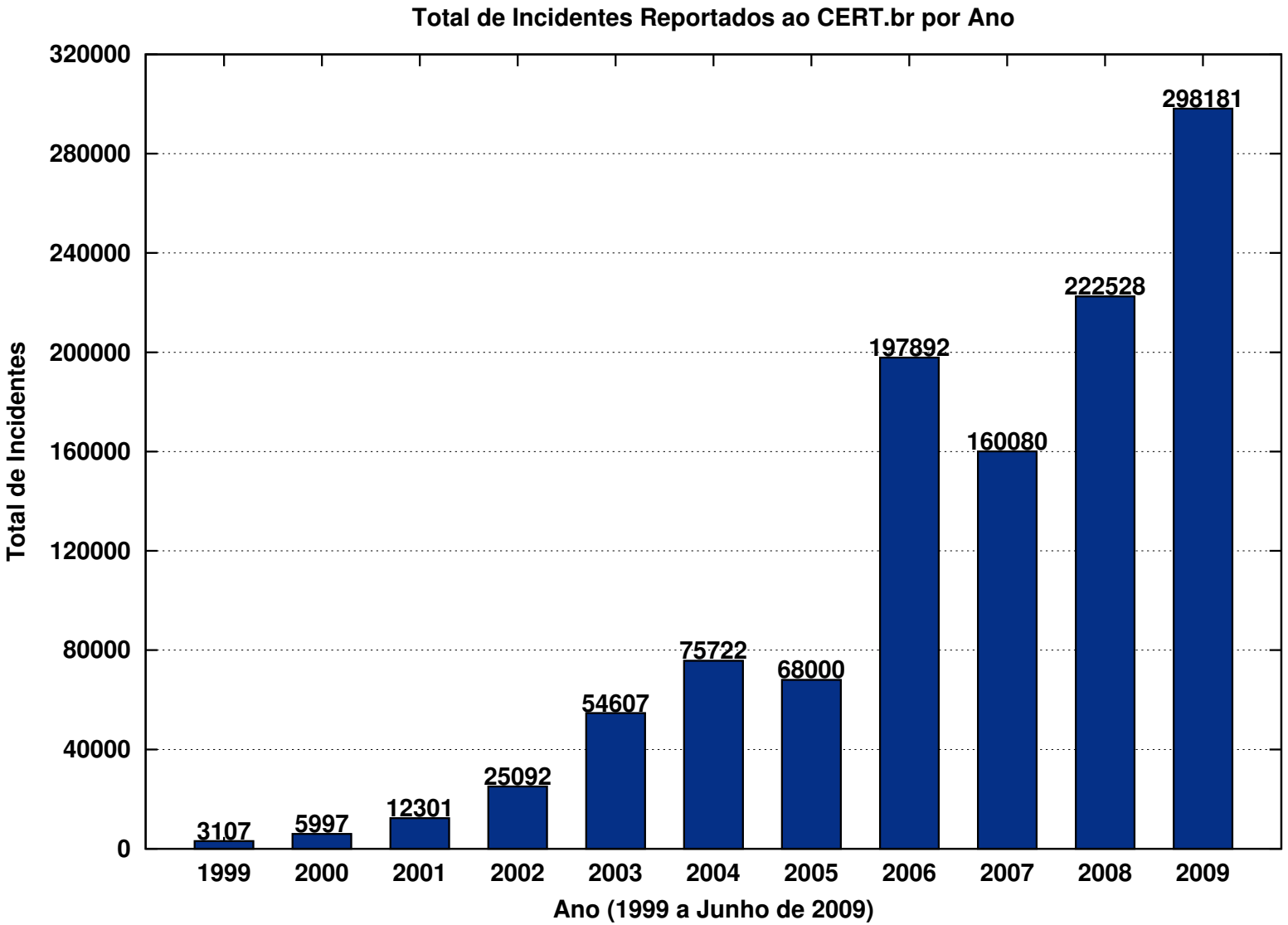
Motivação

- 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
- Apresentar o que o CERT.br tem feito na área de resposta a incidentes
- Discutir possíveis formas de proteção, isto é, o que podemos fazer para usar a Internet de modo mais seguro

Agenda

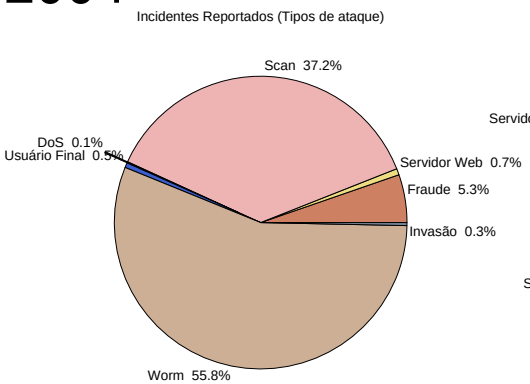
- Incidentes de Segurança
- Pesquisa TIC Domicílios
- Evolução dos Problemas de Segurança
- Situação Atual
  - Características dos Ataques
  - Características dos Atacantes
  - Facilitadores para este Cenário
- Fraudes no Brasil
- Incidentes sendo Tratados
  - Tentativas de Fraude
  - Ataques de Força Bruta
  - DNS
- Prevenção
- Referências

Incidentes de Segurança: 1999–2009

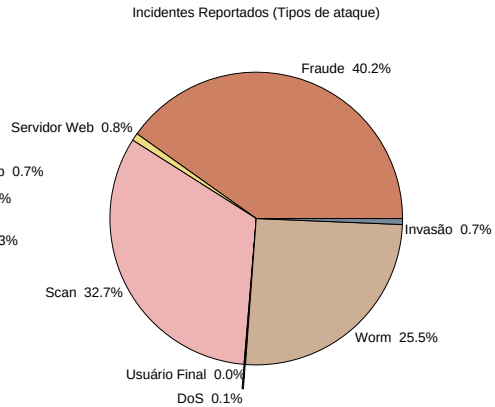


Incidentes de Segurança: Categorias

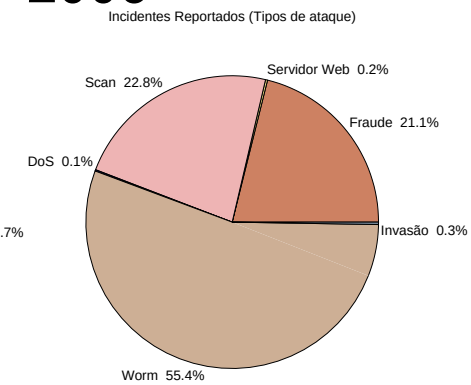
2004



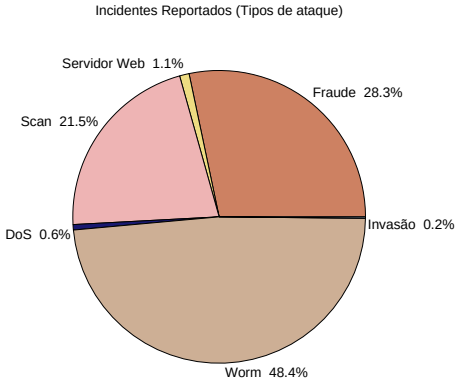
2005



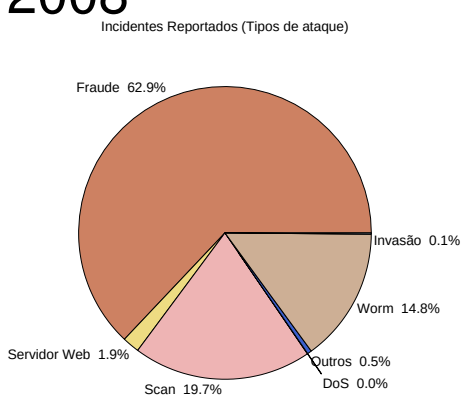
2006



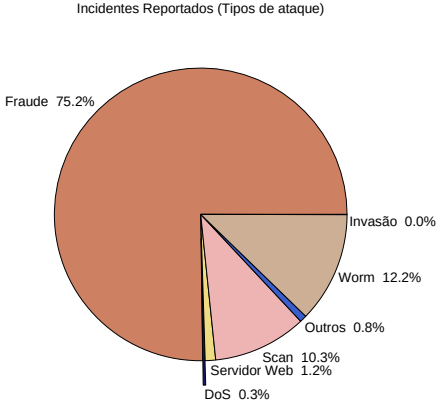
2007



2008



2009



Totais da categoria fraude:

2004	**4.015 (05%)**
2005	**27.292 (40%)**
2006	**41.776 (21%)**
2007	**45.298 (28%)**
2008	**140.067 (62%)**
2009/S1	**239.022 (75%)**

Totais da categoria *worm* (engloba *bots*):

2004	**42.267 (55%)**
2005	**17.332 (25%)**
2006	**109.676 (55%)**
2007	**77.473 (48%)**
2008	**32.960 (14%)**
2009/S1	**38.852 (12%)**

Pesquisa TIC Domicílios

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

Frequência 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: CETIC.br (http://www.cetic.br/)

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*
  - 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 frequentes
  - 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 intuitivos para o usuário
- Falta de treinamento

Fraudes no Brasil

Fraudes: histórico e cenário atual

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

2008–hoje *links* patrocinados, modificações no arquivo *hosts*
- Continuidade das tendências de 2005–2007
- *Malware* modificando arquivo *hosts* – antigo, mas ainda efetivo
- *downloads* involuntários pouco vistos, mas ocorrem
- *links* patrocinados do Google
  - usam a palavra “banco” e nomes de instituições como “AdWords”
  - direcionam o usuário para *sites* contendo *malware*

Incidentes sendo Tratados

Tentativas de Fraude (1/3)

Notificações tratadas:

2004	2005	2006	2007	2008	2009/S1
4.015 (5%)	27.292 (40%)	41.776 (21%)	45.298 (28%)	140.067 (62%)	239.022 (75%)

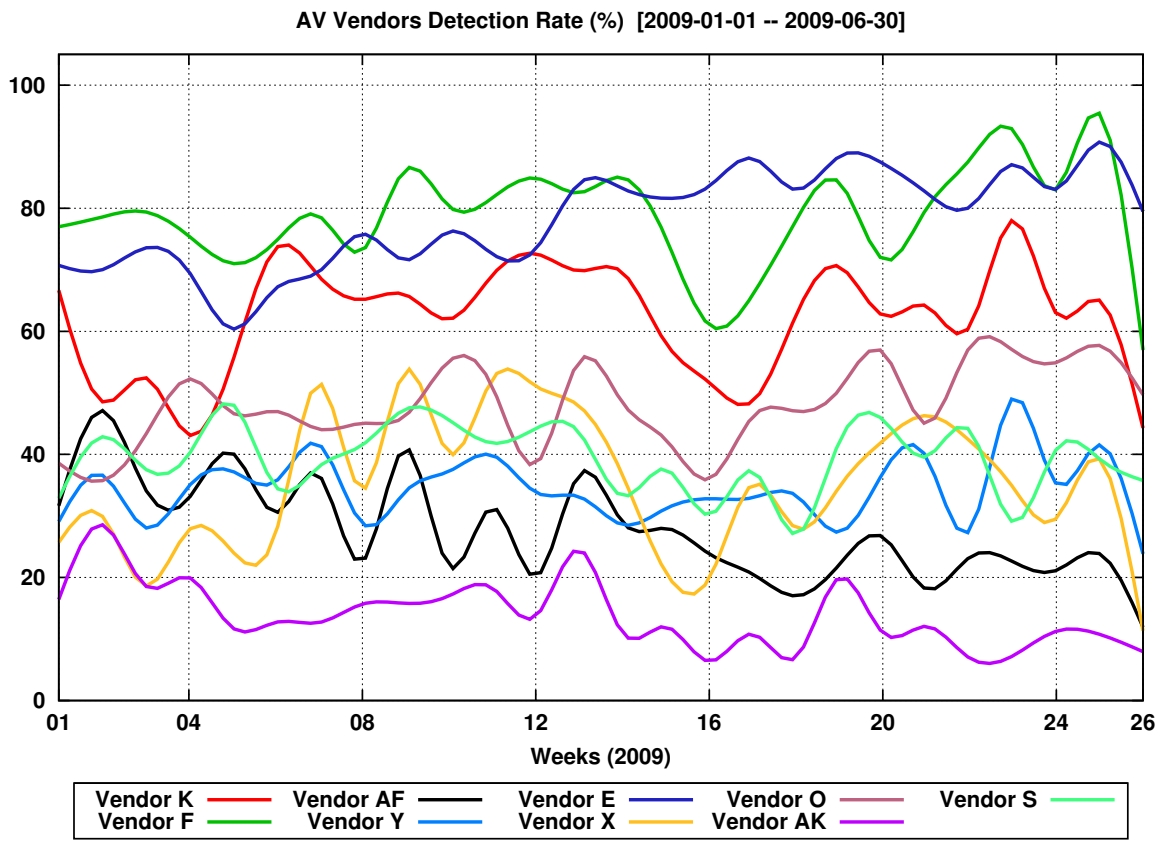
Estatísticas de *Malware** de 2006 a junho de 2009:

Categoria	2006	2007	2008	2009/S1
URLs únicas	25.087	19.981	17.376	4.973
Códigos maliciosos únicos (*hashes* únicos)	19.148	16.946	14.256	3.740
Assinaturas de Antivírus (únicas)	1.988	3.032	6.085	1.564
Assinaturas de Antivírus (“família”)	141	125	447	935
Extensões de arquivos usadas	73	112	112	65
Domínios	5.587	7.795	5.916	2.048
Endereços IP únicos	3.859	4.415	3.921	1.595
Países de origem	75	83	78	64
Emails de notificação enviados pelo CERT.br	18.839	17.483	15.499	4.354

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

Tentativas de Fraude (2/3)

Taxas de Detecção dos Antivírus em 2009/S1:



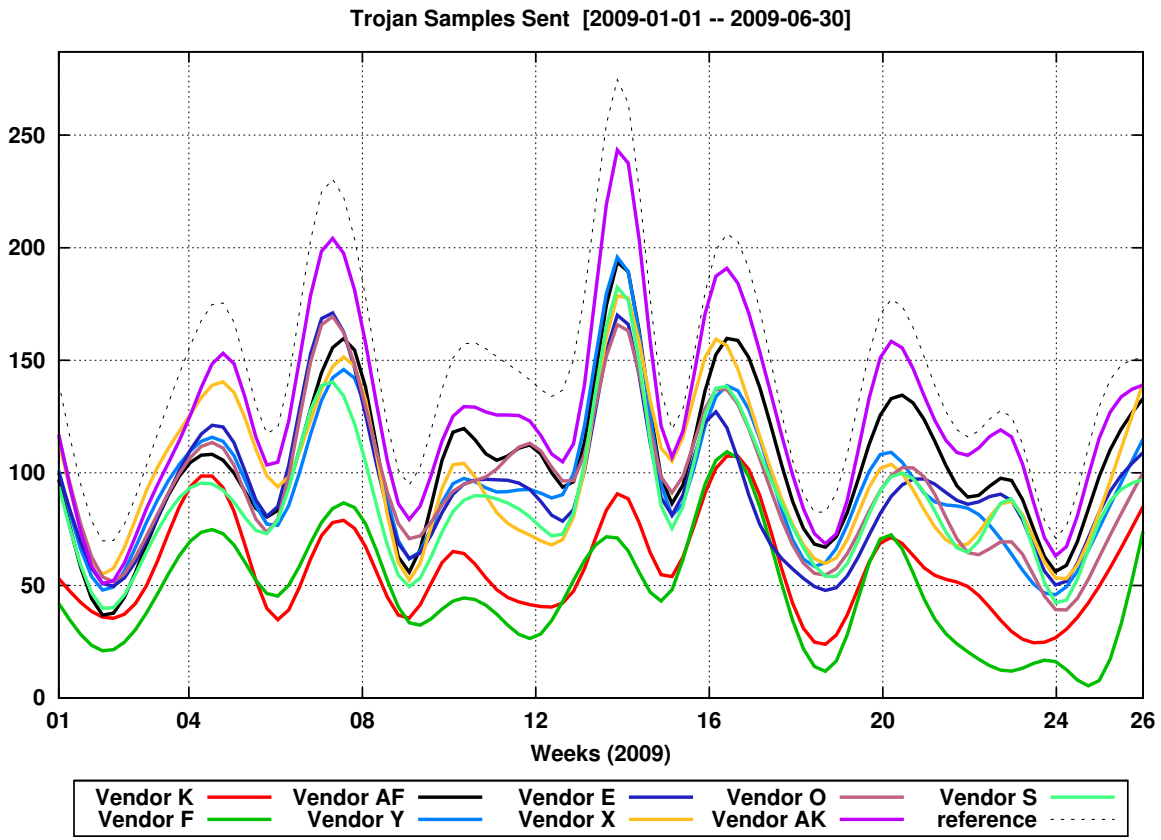
84% dos antivírus testaram mais de 90% dos exemplares

18% dos antivírus detectaram mais de 70% dos exemplares

75% dos antivírus detectaram menos de 50% dos exemplares

Tentativas de Fraude (3/3)

Malwares enviados para 25+ Antivírus em 2009/S1:



Casos de fraude relacionados a *malware* diminuiram ≈12% entre o primeiro e o segundo trimestre de 2009

Casos de páginas de *phishing* mantiveram-se estáveis

Ataques de Força Bruta

Serviço SSH

- Ampla utilização em servidores UNIX
- Alvos
  - senhas fracas
  - contas temporárias
- Pouca monitoração permite que o ataque perdure por horas ou dias

Outros serviços

- FTP
- TELNET
- Radmin
- VNC

DNS *Cache Poisoning*

- Leva um servidor recursivo a armazenar dados forjados
  - permite redirecionamento de domínios
- Facilitado pelo método descoberto por Dan Kaminsky
- Correções dos *softwares*: uso de portas de origem aleatórias nas consultas
  - Não elimina o ataque, apenas retarda seu sucesso
  - Adoção de DNSSEC é uma solução mais definitiva
    http://registro.br/info/dnssec.html
- Notificações enviadas pelo CERT.br: ≈11k

DNS Recursivo Aberto (1/3)

- Permite que qualquer máquina faça consultas [1,2]
- Configuração padrão da maioria dos *softwares* DNS
- Pode ser usado para amplificar ataques de DDoS
- Recursivos abertos no mundo:
  - Listados pelo *Measurement Factory* [3]: ≈350k
- Recursivos abertos no Brasil:
  - Notificações realizadas pelo CERT.br: ≈46k
  - Ainda listados pelo *Measurement Factory*: ≈14k

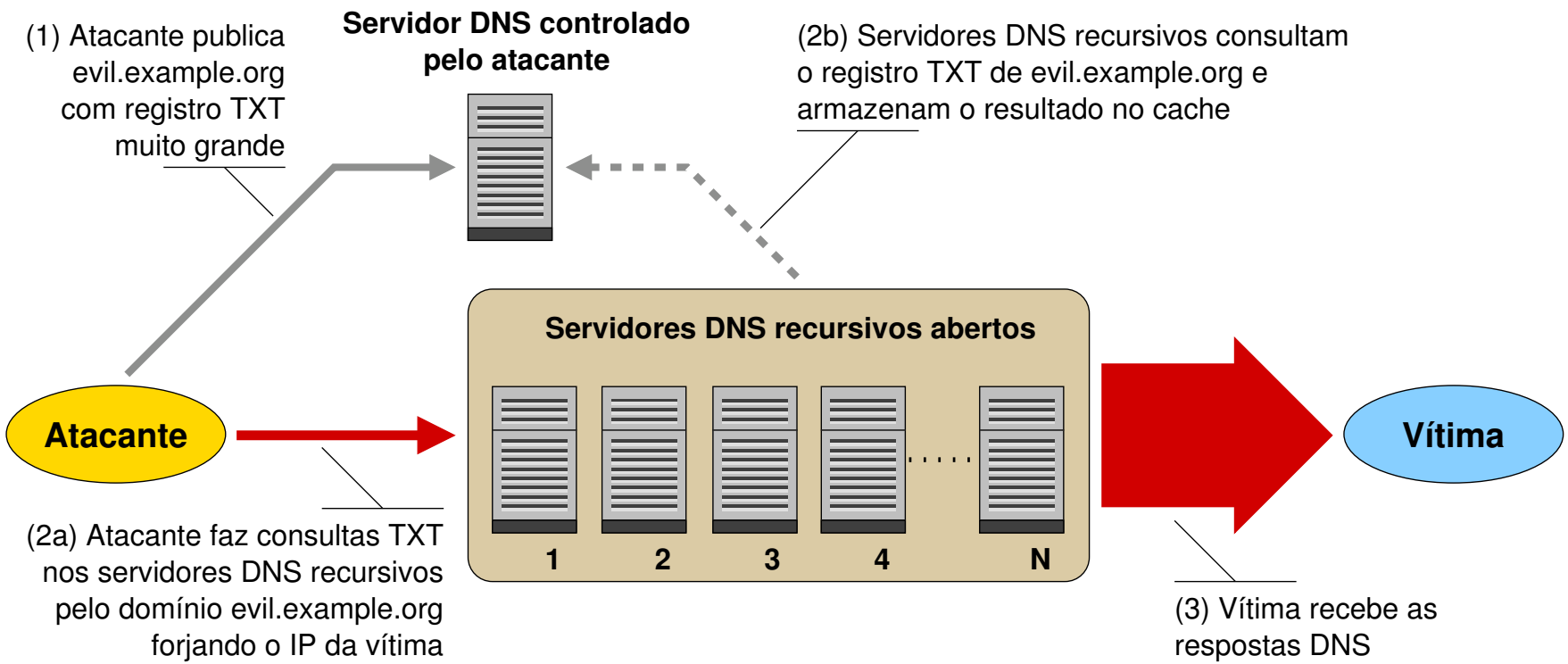
[1] http://www.cert.br/docs/whitepapers/dns-recursivo-aberto/

[2] RFC 5358: *Preventing Use of Recursive Nameservers in Reflector Attacks*

[3] http://dns.measurement-factory.com/surveys/openresolvers.html

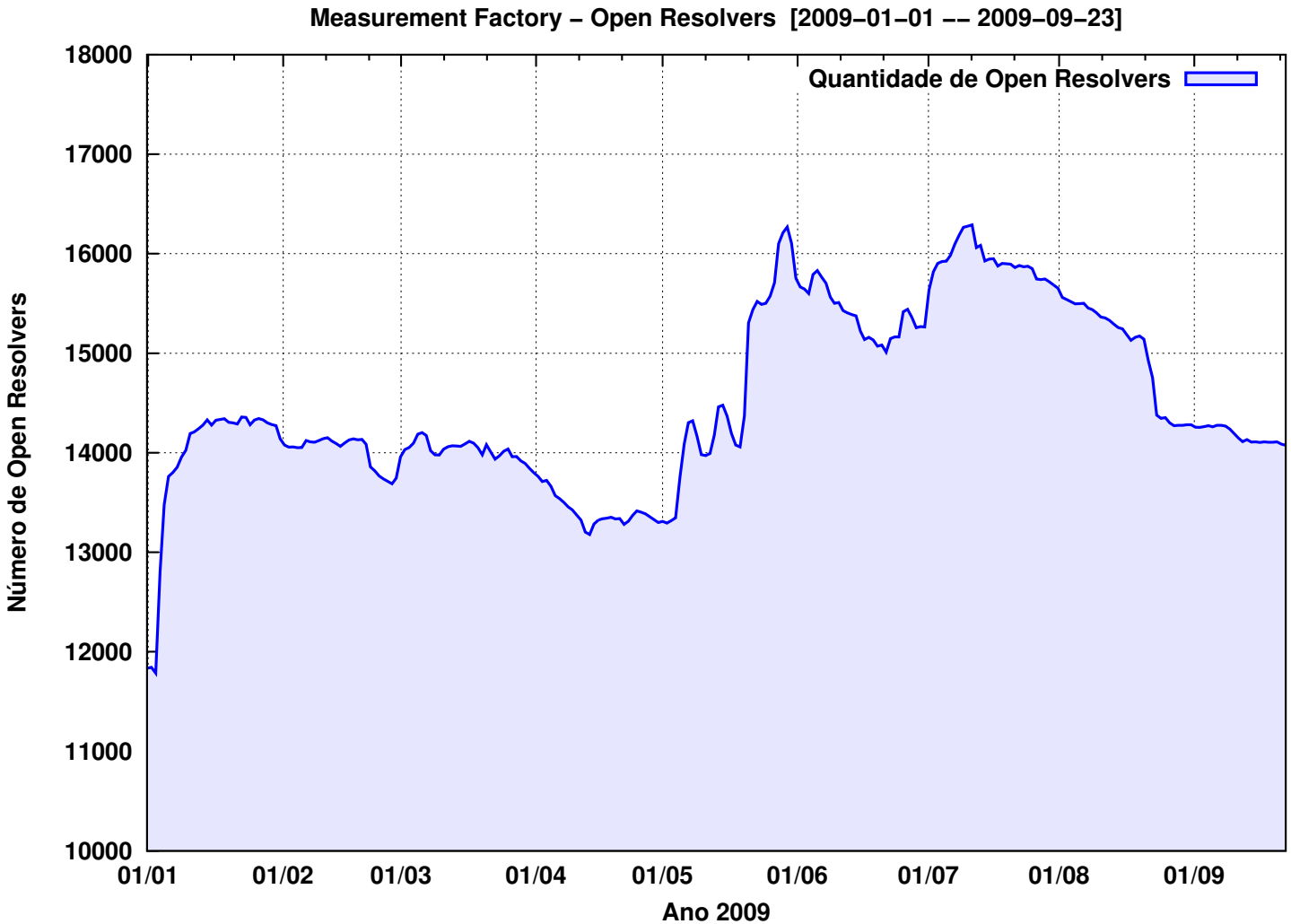
DNS Recursivo Aberto (2/3)

Ataque de Amplificação



DNS Recursivo Aberto (3/3)

Dados da Measurement Factory



Prevenção

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 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)

Núcleo de Informação e Coordenação do Ponto br

Início Dicas Download Checklist Glossário Livro

cert.br
Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

cgi.br NIC.br Registro

Cartilha de Segurança para Internet 3.1

Livro Completo

A partir da versão 3.1 a Cartilha de Segurança para Internet passou a ser editada também como livro. Nesta página você encontra o prefácio do Livro e o arquivo para download.

Prefácio

A Cartilha de Segurança para Internet é um documento com recomendações e dicas sobre como o usuário de Internet deve se comportar para aumentar a sua segurança e se proteger de possíveis ameaças.

Produzido pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – CERT.br, com o apoio do Comitê Gestor da Internet no Brasil – CGI.br, o documento apresenta o significado de diversos termos e conceitos utilizados na Internet e fornece uma série de procedimentos que visam melhorar a segurança de um computador.

Livro Completo para download (886 KB)

Cartilha de Segurança para Internet, versão 3.1 / CERT.br – São Paulo: Comitê Gestor da Internet no Brasil, 2006.

ISBN: 978-85-60062-06-5
ISBN: 85-60062-06-8

http://cartilha.cert.br/

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

http://www.antispam.br/videos/

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/