

Segurança da Internet no Brasil e Atuação do CERT.br

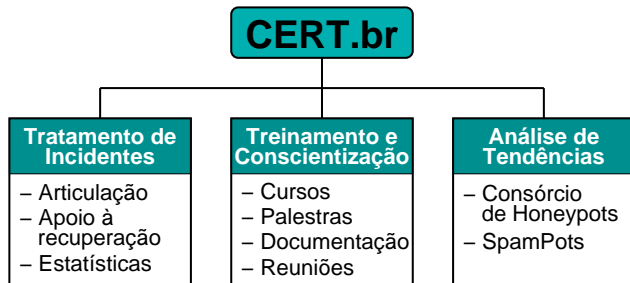
Aritana Pinheiro Falconi

falconi@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

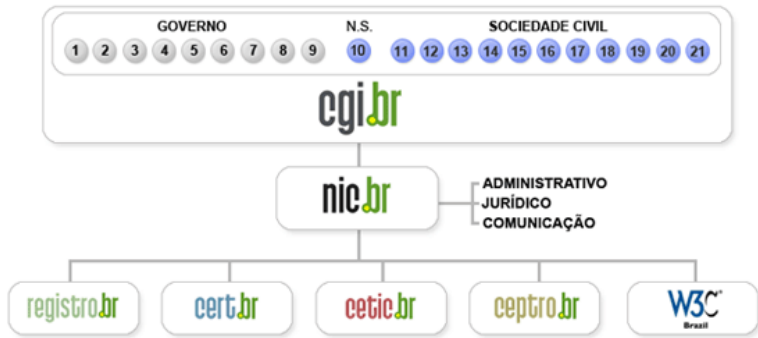


SEIPartner
CERT Courses



<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
- Dedicção 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

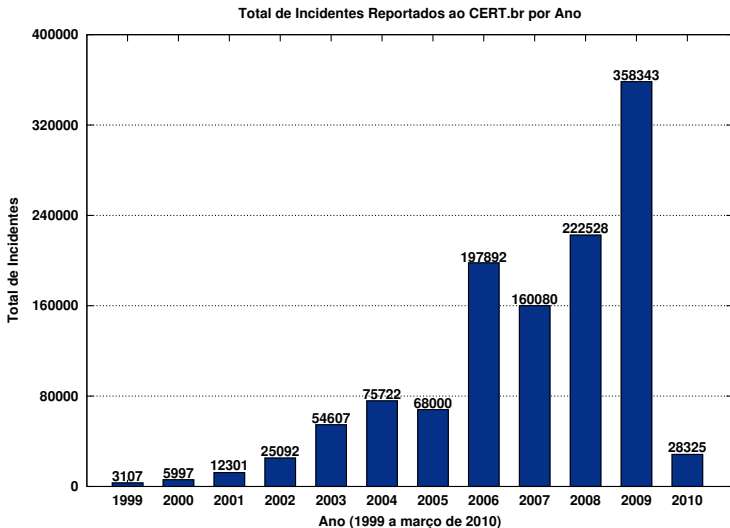
- Em sua maioria pessoal com pouco conhecimento técnico que utiliza ferramentas prontas
- Trocam informações no *underground*
- Usam como moedas de troca
 - senhas de administrador/`root`
 - novos *exploits*
 - contas/senhas de banco, números de cartão de crédito
 - *bots/botnets*
- Atacantes + *spammers*
- 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 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 intuitivo para o usuário
- Falta de treinamento

Incidentes de Segurança no Brasil



Ataques mais frequentes – 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 frequentes, 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 março de 2010:

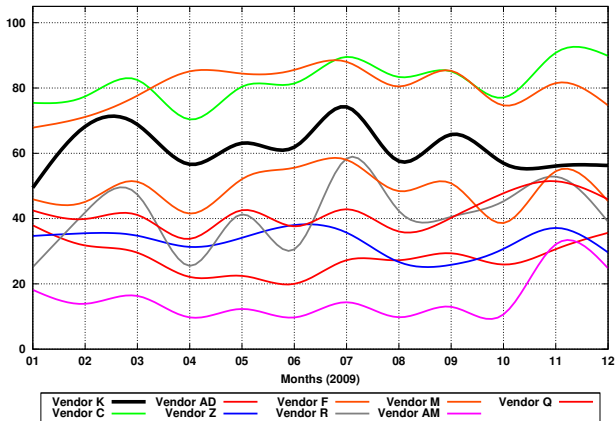
Categoria	2006	2007	2008	2009	2010-Q1
URLs únicas	25.087	19.981	17.376	10.864	2.798
Códigos maliciosos únicos (<i>hashes</i> únicos)	19.148	16.946	14.256	8.151	1.870
Assinaturas de Antivírus (únicas)	1.988	3.032	6.085	4.101	1.387
Assinaturas de Antivírus (“família”)	140	109	63	93	51
Extensões de arquivos usadas	73	112	112	100	46
Domínios	5.587	7.795	5.916	4.447	1.311
Endereços IP únicos	3.859	4.415	3.921	3.233	996
Países de origem	75	83	78	76	53
Emails de notificação enviados pelo CERT.br	18.839	17.483	15.499	9.935	2.236

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

Tentativas de Fraude Tratadas (2/3)

Taxas de Detecção dos Antivírus em 2009:

AV Vendors Detection Rate (%) [2009-01-01 -- 2009-12-31]



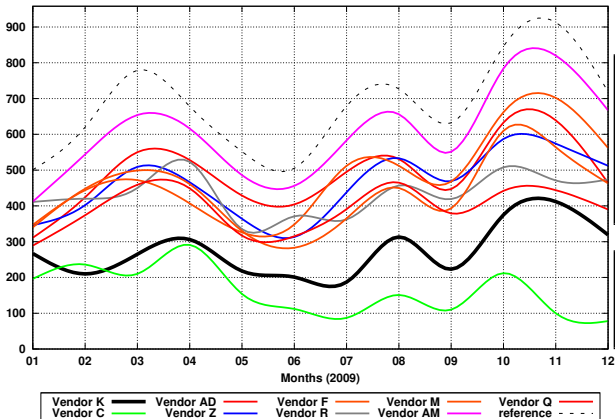
11% dos antivírus detectaram **mais** de 80% dos exemplares

75% dos antivírus detectaram **menos** de 50% dos exemplares

Tentativas de Fraude Tratadas (3/3)

Malwares enviados para 25+ Antivírus em 2009:

Trojan Samples Sent [2009-01-01 -- 2009-12-31]



Casos de fraude relacionados a *malware* reduziram 23% entre 2008 e 2009, mas aumentaram 14% do terceiro para o quarto trimestre de 2009

Casos de páginas de *phishing* aumentaram 112% entre 2008 e 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 Usando a Internet (%):

	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
2009	63	35	1	1	ND	1

Medidas de Segurança Adotadas:

	Antivírus	Firewall pessoal	Outro programa	Nenhuma medida
2007	75	11	6	22
2008	70	10	4	28
2009	75	9	4	22

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
2009	22	17	13	5	34	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)



Cartilha de Segurança para Internet

Núcleo de Informação e Coordenação do Ponto br

Início Dicas Download Checklist Glossário Livro

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.

Nós esperamos que esta Cartilha possa auxiliá-lo não só a compreender as ameaças do ambiente Internet, mas também a manter seu sistema mais seguro. Gostaríamos ainda de lembrar que é muito importante ficar sempre atento ao usar a Internet, pois somente aliando medidas técnicas a boas práticas é possível atingir um nível de segurança que permita o pleno uso da Internet.

Case você tenha alguma sugestão para este documento ou encontre algum erro, por favor, entre em contato através do endereço doc@cert.br.

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)

- **Site Antispam.br – Vídeos Educativos 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/>