

Cartilha de Segurança para Internet

versão 3.0

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

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

Comitê Gestor da Internet no Brasil – CGI.br

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

- Sobre o CGI.br / NIC.br / CERT.br
- Tendências
- Novidades dessa versão da Cartilha
- Destaques
- Apresentação do site

Sobre o CGI.br / NIC.br



Sobre o CGI.br (cont)

Comitê Gestor da Internet no Brasil

- Comitê criado pela Portaria Interministerial 147 de 31/05/1995, alterada pelo Decreto Presidencial 4.829 de 03/09/2003
 - 9 representantes do Governo Federal
 - 4 representantes do setor empresarial
 - 4 representantes do terceiro setor
 - 3 representantes da comunidade científica e tecnológica
 - 1 representante de notório saber em assuntos de Internet

Sobre o CGI.br (cont)

Algumas atribuições:

- 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.

Sobre o CERT.br

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (antigo NBSO, criado em 1997)

- articulação das ações para resposta a incidentes envolvendo redes brasileiras
- manutenção de estatísticas sobre incidentes de segurança
- desenvolvimento de documentação sobre segurança para usuários de Internet e administradores de redes
- fomento à criação de novos Grupos de Resposta a Incidentes (CSIRTs) no Brasil e oferecimento de cursos

Sobre a Cartilha de Segurança

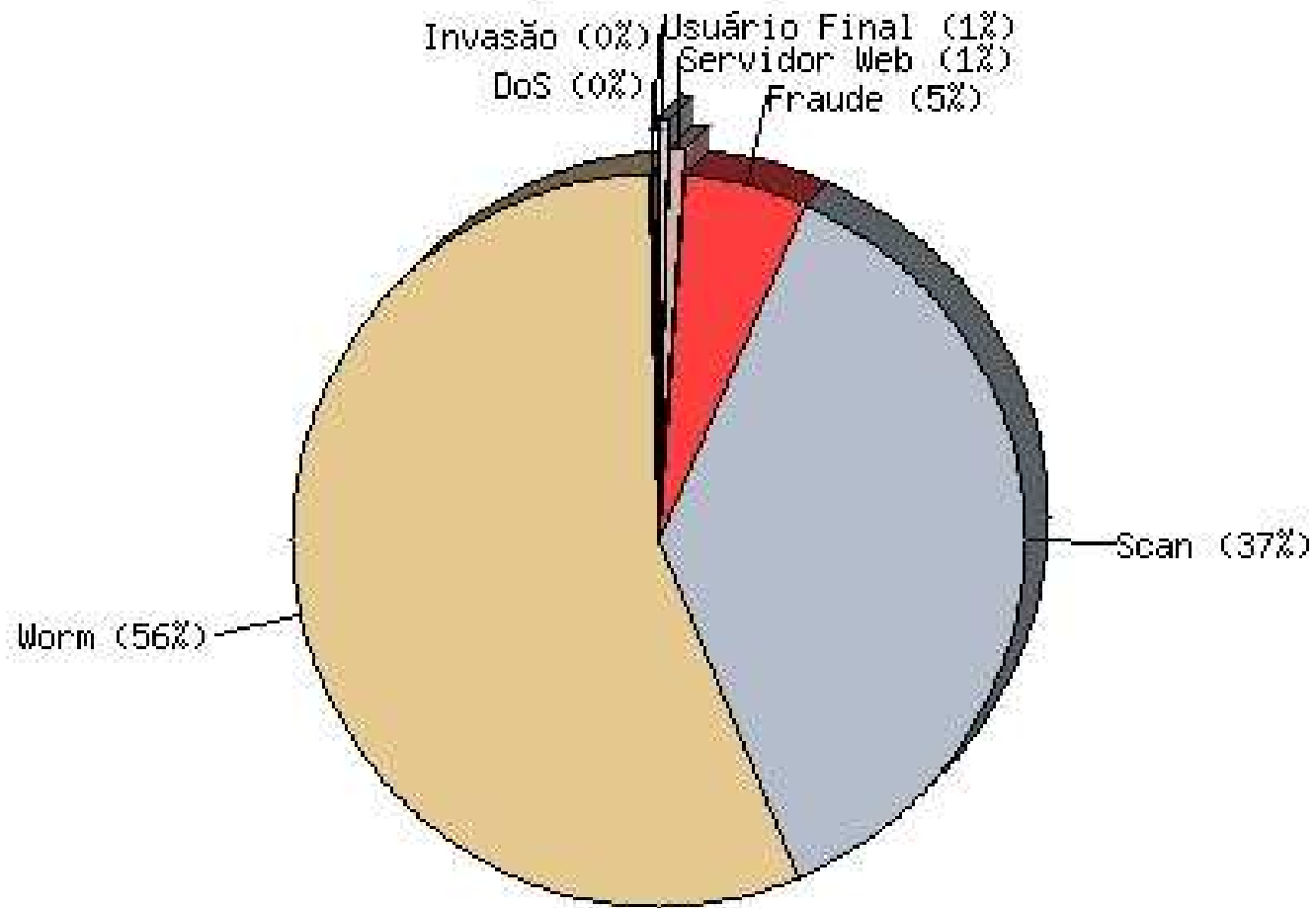
Documento com recomendações e dicas para aumentar a segurança e proteção do usuário de ameaças na Internet.

- 2000: primeira versão, em conjunto com a Abranet
- 2003: segunda versão: ampliada, dividida em partes e disponível também em HTML
- 2005: terceira versão

Por que uma nova versão?

- nos últimos anos surgiram novas ameaças:
 - aumento no número e nos tipos de fraudes
 - uso em grande escala de códigos maliciosos (bots, worms, spywares, etc)
- e novas tecnologias:
 - WPA, aumento da disponibilidade de dispositivos ligados em rede (celulares, PDAs), etc

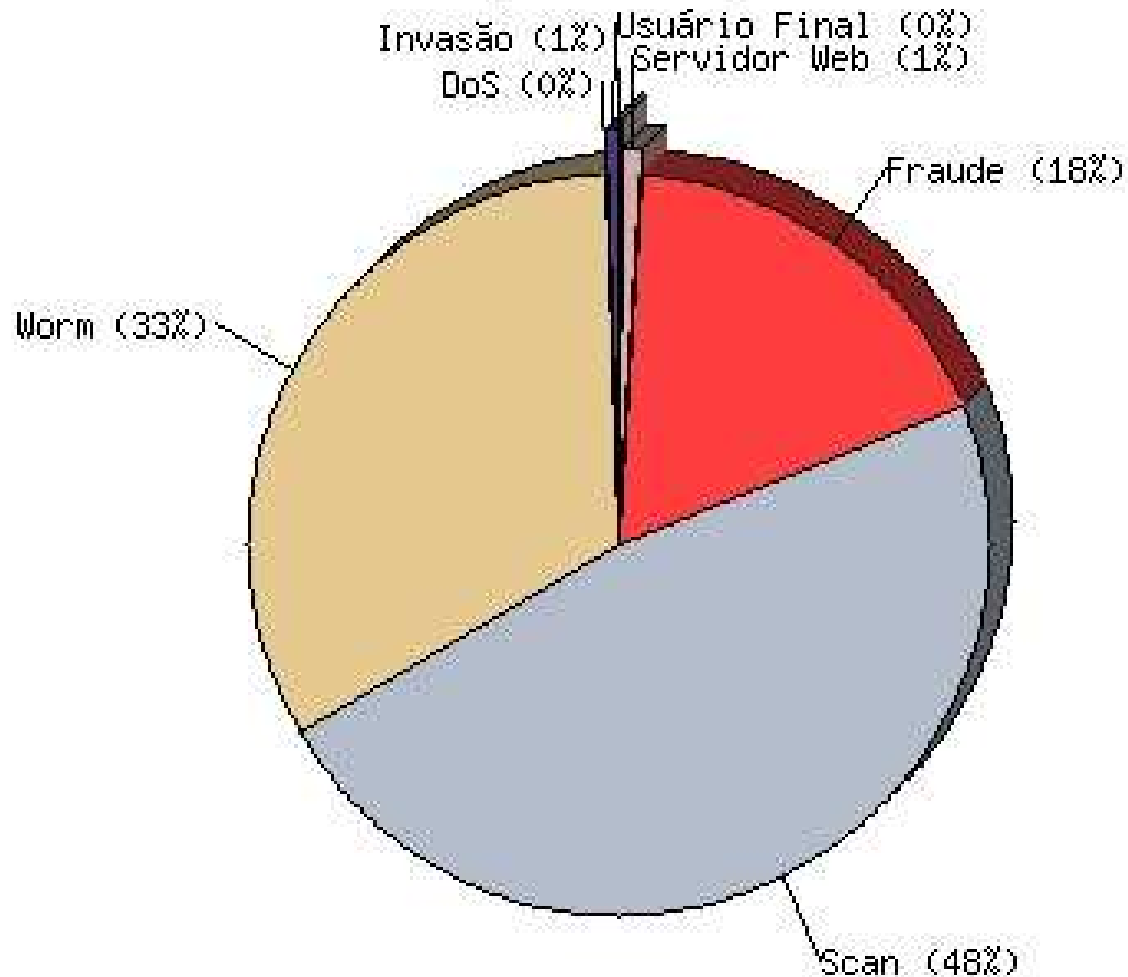
Incidentes Reportados (Tipos de Ataque)



Total de incidentes: 75.722

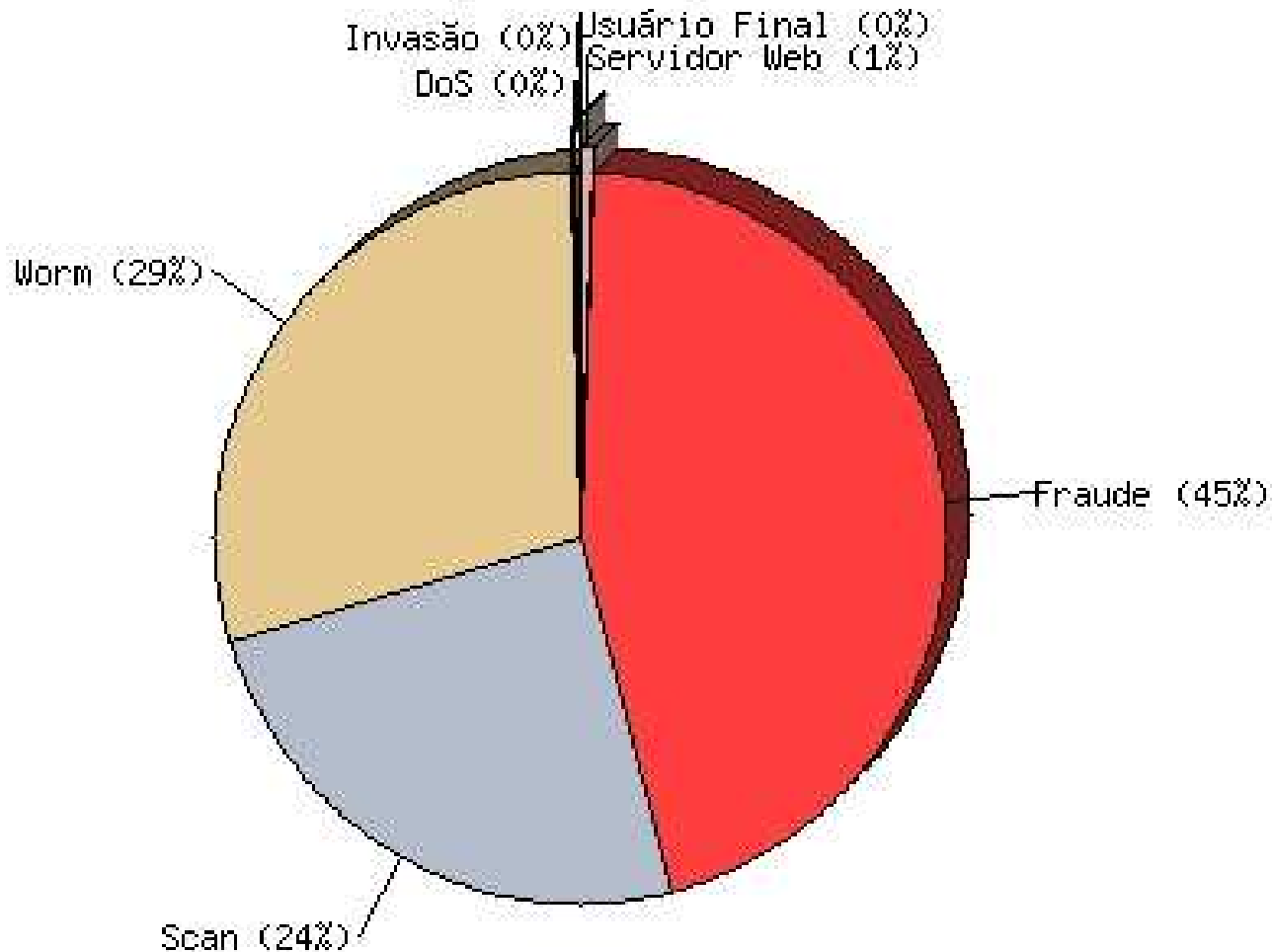
Incidentes 2005/01

Incidentes Reportados (Tipos de Ataque)



Total de incidentes: 12.438

Incidentes Reportados (Tipos de Ataque)



Total de incidentes: 17.542

Tendências

- continuidade dos ataques focados em usuários finais
 - worms, bots, fraudes, etc
 - novas maneiras de induzí-lo a erro
- número de notificações de incidentes envolvendo fraudes continua alto:
 - 2.730 em julho
 - 2.954 em agosto

Novidades da Cartilha

Novidades na versão 3.0

- incluídas novas situações na parte sobre Fraudes na Internet
- novas tecnologias (WPA, celular, bluetooth)
- criada uma parte dedicada a códigos maliciosos
- mais de 50 novas entradas no Glossário
- reformulação da página e reorganização do conteúdo
- folders com dicas mais importantes
- dica do dia

As Partes da Cartilha

- Parte I: Conceitos de Segurança
- Parte II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção
- Parte III: Privacidade
- Parte IV: Fraudes na Internet
- Parte V: Redes de Banda Larga e Redes Sem Fio
- Parte VI: Spam
- Parte VII: Incidentes de Segurança e Uso Abusivo
- Parte VIII: Códigos Maliciosos
- Checklist
- Glossário

Destques de cada parte

Parte I: Conceitos de Segurança

- importância da preocupação com segurança
- senhas (cuidados no uso e elaboração)
- cookies
- engenharia social
- vulnerabilidade
- negação de serviço
- criptografia

- uso de browsers e leitores de e-mail
- bom uso de um antivírus
- importância dos firewalls
- cuidados com programas de troca de mensagens e distribuição de arquivos
- cuidados com compartilhamento de recursos
- importância das cópias de segurança

Parte III: Privacidade

- recursos, como a criptografia, para aumentar a privacidade no acesso a páginas web e na troca de e-mails
- cuidados com a disponibilização de dados pessoais e sensíveis em páginas web, blogs e sites de redes de relacionamento
- cuidados com telefones celulares, PDAs e outros aparelhos com bluetooth

Parte IV: Fraudes na Internet

- papel da engenharia social nas fraudes
- situações de fraudes na Internet (scam e phishing scam)
 - incluída tabela com extensa lista de possíveis ardis
- como se prevenir de fraudes
- dicas para verificar se um site usa conexão segura

- particularidades de segurança no uso de redes de banda larga
- cuidados ao montar uma rede doméstica ou de uma pequena empresa
- riscos adicionais e cuidados que devem ser tomados ao utilizar redes sem fio

Parte VI: Spam

- problemas causados pelo spam
- métodos usados por spammers para aquisição de endereços de e-mail
- mecanismos de filtragem

- conceitos de incidentes de segurança e uso abusivo da rede
- políticas de uso aceitável
- identificação de ataques e registros de atividades
- como e por que notificar incidentes

Parte VIII: Códigos Maliciosos

- como funcionam e como se proteger dos diversos códigos maliciosos:
 - vírus
 - cavalos de tróia
 - adware e spyware
 - backdoors
 - keyloggers
 - worms
 - bots e botnets
 - rootkits

Glossário

Código malicioso (malware) termo que se refere a todos os tipos de programa que executam ações maliciosas em um computador.

Cavalo de tróia (trojan) programa que além de executar funções para as quais foi aparentemente projetado, também executa outras funções sem o conhecimento do usuário.

Backdoor programa que permite a um invasor retornar a um computador comprometido.

Glossário (cont.)

Keylogger programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador.

Spyware categoria de software que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros.

Rootkit conjunto de programas que tem como finalidade esconder e assegurar a presença de um invasor em um computador comprometido.

Glossário (cont.)

Vírus programa que se propaga inserindo cópias de si mesmo em outros programas e arquivos de um computador. O vírus depende da execução do programa por parte do usuário.

Worm programa capaz de se propagar automaticamente, através da exploração de vulnerabilidades em softwares, enviando cópias de si mesmo de computador para computador.

Glossário (cont.)

Bot programa que se propaga como um worm, mas que dispõe de mecanismos de comunicação com o invasor, permitindo que o programa seja controlado remotamente.

Botnets redes formadas por diversos computadores infectados com bots.

Glossário (cont.)

Scam esquemas ou ações enganosas e/ou fraudulentas.

Normalmente, têm como finalidade obter vantagens financeiras.

Phishing também conhecido como phishing scam.

Mensagem não solicitada que se passa por comunicação de uma instituição conhecida e que procura induzir usuários ao fornecimento de dados pessoais e financeiros ou à instalação de códigos maliciosos.

Checklist

- resume as principais recomendações contidas na Cartilha de Segurança para Internet
- concentra-se nos métodos de prevenção

Dicas de Segurança

- principais dicas para aumentar a segurança na Internet
- as mesmas dicas foram agrupadas em:
 - 1 folheto em formato A4
 - 1 folder em formato A4
- além das dicas do folder, outras serão mostradas na dica do dia

Informações Adicionais

- Cartilha de Segurança para Internet
<http://cartilha.cert.br/>
- CERT.br
<http://www.cert.br/>
- CGI.br
<http://www.cgi.br/>