Evolução dos Problemas de Segurança e Formas de Proteção

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/

Comitê Gestor da Internet no Brasil – CGI.br

http://www.cgi.br/

Roteiro

- Sobre o CGI.br e o CERT.br
- Evolução histórica dos ataques
- Situação atual
- Perfil dos ataques
- Formas de proteção

Sobre o CGI.br

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 coordenação da atribuição de endereços internet (IPs) e do registro de nomes de domínios usando <.br>;
- **a promoção de estudos e padrões técnicos para a segurança das redes e serviços no país**;
- 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 coleta, organização e disseminação de informações sobre os serviços internet, incluindo indicadores e estatísticas.

Sobre o CGI.br / NIC.br

Sobre o CERT.br

Atividades do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (antigo NBSO)

- 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
- cursos do CERT/CC sobre tratamento de incidentes
- coordena o Consórcio Brasileiro de Honeypots – Projeto Honeypots Distribuídos (mais de 30 participantes)

Evolução Histórica dos Ataques

Evolução dos Ataques: Anos 80

- Invasores com
  - alto conhecimento
  - dedicação por longos períodos para realização de poucos ataques

- *"Cookoo's Egg: Tracking a Spy Through the Maze of Computer Espionage"*, Cliff Stoll

http://www.bookfinder.us/review4/0743411463.html

Evolução dos Ataques: Anos 80 (cont.)

- Primeiro *worm* com implicações de segurança
  - criado por Robert Morris Jr.
  - explorava a combinação de vulnerabilidades no `sendmail`, `finger` e em configurações dos *"r" services*
  - mais de 6000 computadores atingidos (aprox. 10% da Internet na época)
- 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`

Glossário de Termos (1)

Vírus: programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador. O vírus **depende** da execução do programa ou arquivo hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção.

Worm: programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o *worm* não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar. Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em computadores.

Fonte: http://cartilha.cert.br/glossario/

Evolução dos Ataques: 1991-2001

- Início da utilização da “engenharia social” em grande escala
- Primeiros ataques remotos aos sistemas
- Popularização de: cavalos de tróia, furtos de senhas, varreduras em busca de máquinas vulneráveis, captura de informações digitais (*sniffers*), ataques de negação de serviço, etc
- Primeiras ferramentas automatizadas
  - para realizar invasões
  - para ocultar a presença dos invasores (*rootkits*)
- Sofisticação no processo de controle das ferramentas

Evolução dos Ataques: 2002-2004

- Explosão no número de códigos maliciosos com diversos fins
  - *worms*, *bots*, cavalos de tróia, vírus, *spywares*
- Códigos com múltiplas funcionalidades
  - múltiplos vetores de ataque, código eficiente, aberto e facilmente adaptável
- Permitem controle remoto
- Praticamente não exigem interações por parte dos invasores

Glossário de Termos (2)

Cavalo de Tróia: programa, normalmente recebido como um "presente", que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.

***Bot*:** programa que, além de incluir funcionalidades de *worms*, sendo capaz de se propagar automaticamente através da exploração de vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em um computador, dispõe de mecanismos de comunicação com o invasor, permitindo que o programa seja controlado remotamente.

***Spyware*:** termo utilizado para se referir a uma grande categoria de *software* que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros. Podem ser utilizados de forma legítima, mas, na maioria das vezes, são utilizados de forma dissimulada, não autorizada e maliciosa.

Fonte: http://cartilha.cert.br/glossario/

Situação Atual

Características dos Ataques

- Crime Organizado
  - aliciando *spammers* e invasores
  - injetando dinheiro na "economia *underground*"
- Botnets
  - usadas para envio de scams, *phishing*, invasões, esquemas de extorsão
- Redes malconfiguradas sendo abusadas para realização de todas estas atividades – sem o conhecimento dos donos
- **Alvo migrando para usuários finais**

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*, etc

Perfil dos Ataques

Principais Ameaças

- vulnerabilidades freqüentes
- códigos maliciosos explorando essas vulnerabilidades, em curto espaço de tempo
- ferramentas automatizadas de ataque
- vírus / *worms* / *bots*
- atacantes + *spammers*
- fraudes / *scams* / *phishing* / crime organizado
- ataques de força bruta

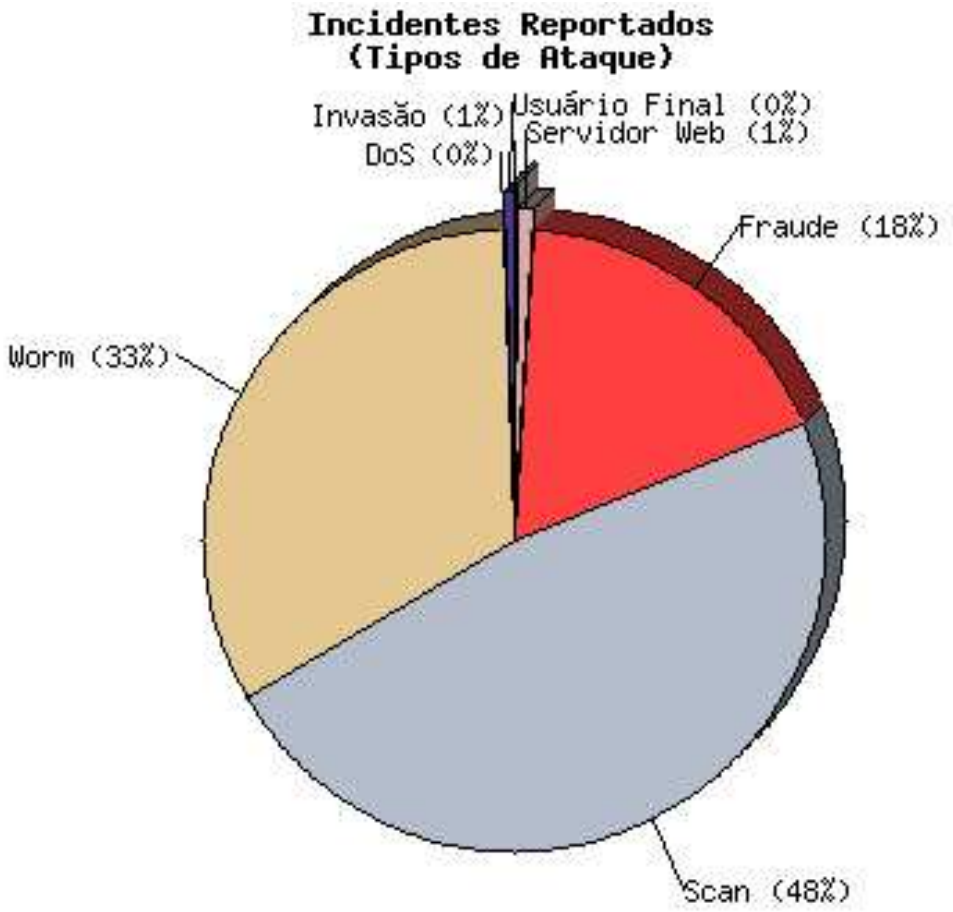
Glossário de Termos (3)

***Scam*:** Esquemas ou ações enganosas e/ou fraudulentas. Normalmente, têm como finalidade obter vantagens financeiras.

***Phishing*:** Mensagem não solicitada que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou site popular, e que procura induzir usuários ao fornecimento de dados pessoais e financeiros. Inicialmente, este tipo de mensagem induzia o usuário ao acesso a páginas fraudulentas na Internet. Atualmente, o termo também se refere à mensagem que induz o usuário à instalação de códigos maliciosos, além da mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros.

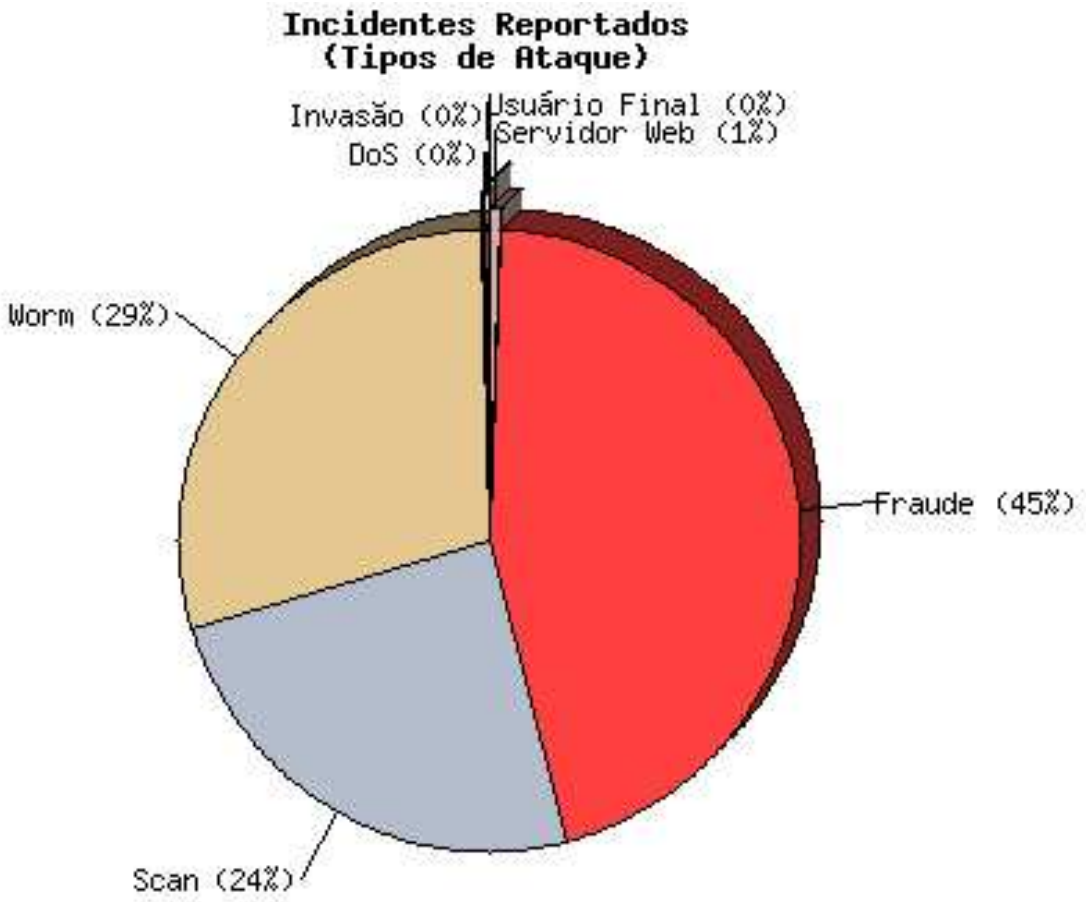
Fonte: http://cartilha.cert.br/glossario/

Incidentes Notificados – 1º Trimestre – 2005



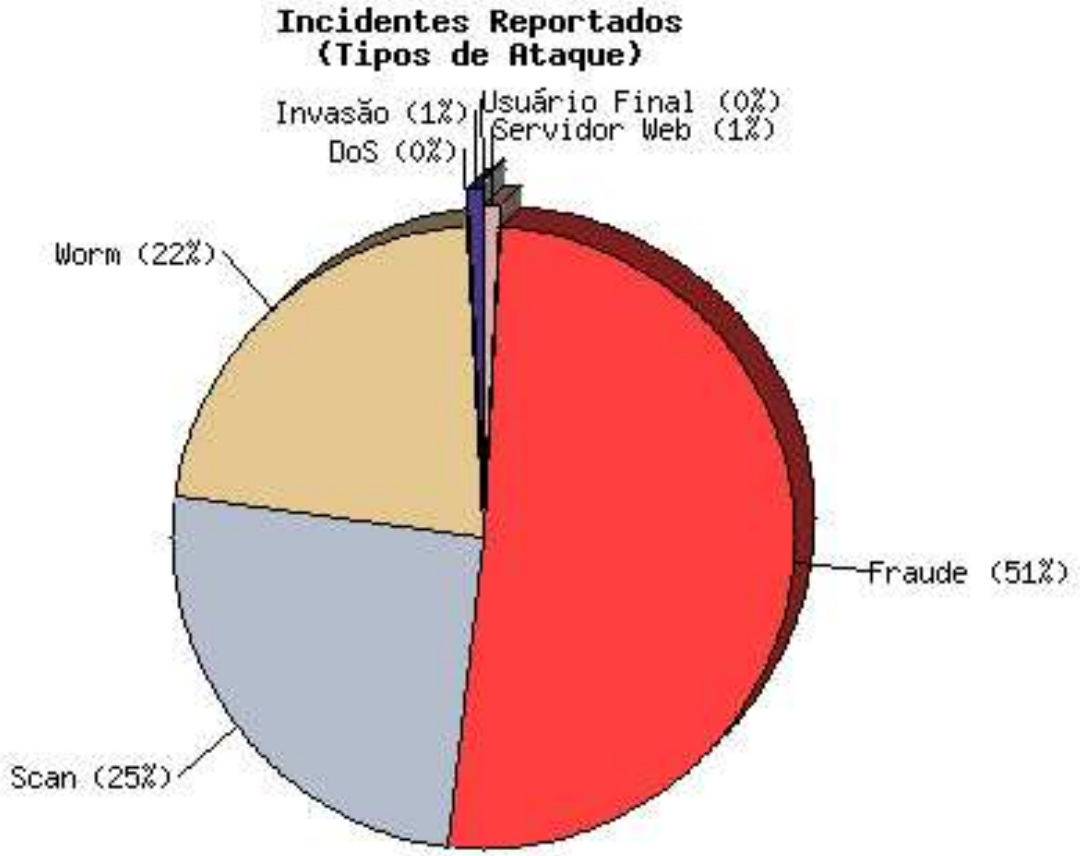
Total de incidentes: 12.438

Incidentes Notificados – 2º Trimestre – 2005



Total de incidentes: 17.542

Incidentes Notificados – 3º Trimestre – 2005



Total de incidentes: 16.225

Formas de Proteção

Segurança em Camadas

Não há uma solução única para resolver todos os problemas.

- combinar soluções
  - *firewall* pessoal
  - antivírus
  - anti-*spyware*
- sistemas atualizados
- aplicativos atualizados

Conscientização dos usuários

- usuários representam o elo mais fraco
- usuários podem ser vetores de disseminação de *worms*/vírus
- usuários são os alvos de:
  - ataques de engenharia social
  - *phishing/scam*
  - cavalos de tróia
  - furto de informações

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

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

http://cartilha.cert.br/

Links de Interesse

- CGI.br

  http://www.cgi.br/

- NIC.br

  http://www.nic.br/

- CERT.br

  http://www.cert.br/

- Cartilha de Segurança para Internet

  http://cartilha.cert.br/