A Evolução dos Problemas de Segurança e Formas de Proteção

Cristine Hoepers
cristine@cert.br

Klaus Steding-Jessen
jessen@cert.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
- Principais ameaças
- Formas de proteção
  - políticas de atualização
  - segurança em camadas
  - proteção da rede interna
  - acompanhar as tendências de ataques
  - educação de usuários
- Considerações finais

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 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

Evolução Histórica 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

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`

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 à busca de máquinas vulneráveis, escutas telemáticas (*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

2002-2004

- Explosão no número de códigos maliciosos com diversos fins
  - worms, bots, trojans, 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

Situação Atual

Perfil 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 mal-configuradas sendo abusadas para realização de todas estas atividades – sem o conhecimento dos donos
- Alvo migrando para usuários finais

Perfil dos Atacantes

- Em sua maioria adolescentes
- Pouco ou nenhum conhecimento
  - trocam informações no *underground*
  - moedas de troca: senhas de administrador/root, novos *exploits*, contas/senhas de banco, números de cartão de crédito, bots/botnets, etc

Principais Ameaças

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

Formas de Proteção

Segurança desde o Princípio

- planejamento do ambiente e da instalação
- política de segurança
- política de uso aceitável
- investir em treinamento
  - administradores de redes
  - desenvolvedores
  - suporte, etc

Política de Atualização e Correção

- possuir uma política de atualização de sistemas e aplicação de patches
  - sistema operacional (servidores e desktops)
  - aplicativos
  - hardware de rede
- não aplicar apenas quando estiver sendo explorado
  - tarde demais
- seguir a política!

Proteção da Rede Interna

grande risco: propagação de códigos maliciosos de dentro para fora (worms e bots)

- compartimentalização da rede
- política de atualização e correção
- política de conexão de equipamentos na rede interna
  - terceirizados
  - notebooks de funcionários, etc

Segurança em Camadas

Não há uma solução única para resolver todos os problemas.

- combinar soluções
- firewall, IDS, sistemas atualizados, antivírus
- múltiplas plataformas
- treinamento, atualização dos profissionais

Ataques de Força Bruta Contra SSH

Dicas para defesa:

- utilizar senhas fortes em todas as contas
- reduzir o número de equipamentos com serviço aberto
- restringir a origem das conexões
- acessar via chaves públicas
- monitorar, monitorar, monitorar. . .

Mais Informações sobre Boas Práticas

Práticas de Segurança para Administradores de Redes Internet

http://www.cert.br/docs/seg-adm-redes/

- recomendações para obter o mínimo necessário de segurança
- planejada nova versão para o primeiro trimestre de 2006

Acompanhamento de Tendências

- acompanhar listas de discussão e sites que mantenham notícias e estatísticas sobre o assunto
- analisar logs
- acompanhar projetos de *Early Warning* nacionais e internacionais
  - http://www.arakis.pl/
  - http://www.jpcert.or.jp/isdas/index-en.html
  - http://www.ecsirt.net/
  - http://www.cymru.com/Darknet/
  - http://www.honeypots-alliance.org.br/stats/

Equipe de Segurança e Resposta a Incidentes (CSIRT)

Deve:

- ser altamente especializada
- ter relação com outras instituições
- ter interação com outras equipes
  - operação
  - redes
  - help desk
  - etc

Educação dos usuários

- usuários podem ser um risco para a organização
- vetores de disseminação de worms/vírus
- 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/