Desmistificando as Ações dos Invasores

Cristine Hoepers
cristine@nic.br

NIC BR Security Office – NBSO
Brazilian Computer Emergency Response Team
http://www.nbso.nic.br/

Comitê Gestor da Internet no Brasil
http://www.cg.org.br/

Roteiro

- Evolução histórica das atividades de invasão
- Situação Atual
  - Perfil dos Ataques
  - Perfil dos Atacantes
- Considerações finais

Evolução Histórica

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

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

Considerações Finais

- É possível ensinar conhecimentos técnicos
- Não é possível ensinar ética
- Conhecimentos para proteger uma rede não são obtidos através do uso das ferramentas de invasão disponíveis atualmente
- Para invadir são necessários
  - contatos no IRC
  - alguns cliques de mouse

Referências Adicionais

- Esta palestra
  http://www.nbso.nic.br/docs/palestras/
- NBSO - NIC BR Security Office
  Brazilian Computer Emergency Response Team
  http://www.nbso.nic.br/
- Comitê Gestor da Internet no Brasil
  http://www.cg.org.br/
- SANS ISC - Formas de Combate a Bots e Botnets
  http://www.nbso.nic.br/docs/ssi2004/ssi2004-wtis-nbso-pbueno.pdf