O futuro dos Backdoors

O pior dos mundos

Augusto Paes de Barros, CISSP-ISSAP®

XIV CNASI São Paulo – 15 de Setembro de 2005

Agenda

- Currículo
- O que são backdoors?
- Passado
- Presente
- Defesas utilizadas
- Futuro
- Novas estratégias
- Tendências de defesa
- Conclusão

Currículo

- Gerente de Segurança da :Certegy
- Outras empresas: BankBoston, Proteus, Módulo
- CISSP-ISSAP®, MCSE, CCSE
- Artigos em diversas publicações

http://www.paesdebarros.com.br

O que são Backdoors

- Definição comum:
  - Método de desviar de sistemas de autenticação ou obter acesso remoto não autorizado no acesso a sistemas de computadores
- Ampliando um pouco, podemos incluir o que é conhecido como *spyware* também

Passado

- BackOrifice, NetBus, SubSeven
  - Filosofia "Client/Server"
    - Server: Backdoor
    - Client: Aplicativo usado para controlar o backdoor
  - Conexão TCP comum
    - Firewall simples resolve o problema
  - Alguns contavam com sistema de aviso de infecção
    - e-mail, ICQ, IRC

Passado (cont.)

- Forma de infecção
  - Arquivo precisava ser executado
    - Subseven contava com "customizador" para montagem de trojan
  - Formas mais utilizadas: e-mail
    - Ainda era raro a filtragem de anexos potencialmente perigosos à época.

Demonstração

SubSeven

Presente

- Mudança notável: OBJETIVO
  - Antes: Brincadeira
  - Hoje: FRAUDE FINANCEIRA
- Filosofia “Coletor de informações”
  - Senhas, screenshots de teclados virtuais, chaves de certificados digitais
- Envio de informações por e-mail ou FTP
  - Ainda simples de evitar com firewalls

Presente (cont.)

- Forma de infecção
  - Arquivo executável
    - E-mail ainda é o veículo mais comum
    - Porém, não costumam trazer o arquivo, mas sim um link para ele
  - Vulnerabilidades de SO e Browser

Demonstração

Keylogger p/ bancos

Defesas utilizadas

- Antivírus
- Firewall
  - Entrada e Saída
- Bloqueio de anexos com extensões executáveis
- IPS
- Teclados virtuais, senhas dinâmicas, certificados digitais e outros.

Futuro

- Sistemas de autenticação cada vez mais elaborados
  - Já há consciência de que autenticação multifatorial é necessária
- Conectividade restrita
  - Está cada vez mais difícil estabelecer a conexão entre o Backdoor e seu "dono"
- Ações
  - Potencial de fraude/ganhos ilícitos em outros pontos ainda não explorados

Novas estratégias

- Autenticação forte
  - Não é mais prático tentar obter as informações necessárias para autenticação
    - Senhas dinâmicas, smartcards, tokens
- Por que não aproveitar a autenticação que o usuário faz?
  - "Session hijacking"
  - Man in the Middle
  - Alteração dinâmica de informações: a própria vítima executando as transações para o criminoso

Session Hijacking

- Controles de sessão
  - URL – Basta copia
  - Cookie – Com código na máquina da vítima é trivial roubá-lo
  - Apenas controle por IP traria dificuldades
    - Pode ser resolvido usando a máquina da vítima como Proxy...
- Não é “bala de prata”: transações costumam requerer nova autenticação

Man in the Middle

- Colocar-se entre a vítima e o sistema acessado (Internet Banking, por exemplo)
  - Certificados digitais
    - Requer a manipulação da verificação por parte do browser
    - Alternativa: inserir certificado de AC confiável
  - Já vêm sendo usado e já está sendo combatido
    - Verificação de endereço sendo acessado/URL
- É possível ser mais sutil

Alteração dinâmica de informações

- Backdoor altera dinamicamente informações enviadas e recebidas pela vítima
  - Qual a aplicação/potencial?

Alterar contas destino de transferências monetárias!

Alteração dinâmica de informações (cont.)

- Grande perigo:
  - Não há necessidade de comunicação com o "dono"
  - Não há necessidade de manter uma ponte (Man in the Middle)
  - Sistemas mais elaborados podem atuar uma vez e depois "sumir"

Alteração dinâmica de informações (cont.)

Demonstração

Conectividade

- Conexões TCP não são mais possíveis
  - Firewalls
  - IPS
  - IDS
- Diversas formas de tunelamento não convencionais disponíveis
  - ICMP
  - HTTP
  - DNS

Conectividade (cont.)

- HTTP
  - Quase todo usuário tem acesso à Internet
    - Autenticação em proxy pode ser aproveitada através da utilização de componentes do IE
- DNS
  - Não há controle sobre seu uso
    - Até mesmo hotspots com acesso restrito permitem queries DNS antes da autenticação

Conectividade (cont.)

Demonstração

Tendências de Defesa

- Hoje:
  - Firewalls
  - IPS/IDS
  - Antivírus
  - Autenticação Forte
- Algum deles pode impedir as técnicas que vimos há pouco?

Tendências de Defesa (cont.)

- Túneis
  - É cada vez mais difícil identificar o tráfego ilegítimo
- Alterações dinâmicas, session hijacking e MITM
  - Todos pressupõem execução de código na vítima

Tendências de Defesa (cont.)

- Monitoração de tráfego
  - Túneis são visíveis em análises de comportamento da rede
    - Exemplo: desvio de quantidade e tamanho das requisições DNS de uma estação
  - Problema: túneis podem evoluir para tentar ser mais sutis
    - Ao invés de trafegar protocolos, trafegar apenas instruções (pegue arquivo A, execute arquivo B, etc)

Tendências de Defesa (cont.)

- Monitoração de comportamento de aplicações
  - Abertura de portas
  - Hooks
  - Problema: potencial alto de falsos positivos
- IPS/IDS de estação
  - Problema: Muitas vezes rodam com o mesmo nível de privilégios que o código malicioso

Conclusão

- As tendências de defesa são boas?
  - Sim para os problemas de hoje
  - As técnicas apresentadas continuam funcionando
- Qual então a solução para os backdoors do futuro?
  - Dica: NÃO EXISTEM BALAS DE PRATA!

Conclusão (cont.)

- USUÁRIO

  (não é sempre nele que botamos a culpa?)
- Liberdade de execução de código + Acesso à Internet = Sucesso nos ataques
- Não podemos reduzir mais o acesso à Internet
  - Logo, devemos reduzir a liberdade de execução de código
  - DEVEMOS REDUZIR O NÍVEL DE PRIVILÉGIO
  - Boa notícia: Windows Vista deve facilitar essa tarefa

Conclusão (cont.)

- E para o usuário do qual não temos controle sobre a estação?
  - Usuários de Internet Banking, e-Commerce
  - AWARENESS
    - Não importa a quantidade de ferramentas que utilizamos, as decisões mais importantes continuam com ele

Conclusão (cont.)

- Para quem cochilou...
  - As ferramentas que estamos comprando não vão resolver o problema
  - As ferramentas que serão lançadas também não vão resolver
  - O usuário comum deve ter poucos privilégios em sua estação
  - O usuário comum deve saber evitar o código malicioso

Conclusão (cont.)

- Perguntas?

- Muito obrigado!