Importância dos Grupos de Resposta a Incidentes de Segurança em Computadores

Cristine Hoepers

cristine@nic.br

NIC BR Security Office – NBSO

Comitê Gestor da Internet no Brasil

http://www.nbso.nic.br/

Roteiro

- NBSO
- Cenário Atual
- Grupos de Resposta a Incidentes (CSIRTs)
  - Definição, Papel e Serviços
- CSIRTs em auxílio a operadores da justiça
- Considerações sobre a situação no Brasil
  - O que vemos hoje
  - Cenário desejável

NBSO – NIC BR Security Office

- Mantido pelo Comitê Gestor da Internet no Brasil
- Grupo de Resposta a Incidentes para a Internet Brasileira
  - coordena ações
  - dá suporte ao processo de análise e recuperação de sistemas invadidos
  - trabalha na conscientização sobre os problemas de segurança
  - ajuda na criação de novos CSIRTs

NBSO (cont.)

- Membro do FIRST (Forum of Incident Response and Security Teams)
  - Reúne CSIRTs de todo o mundo
  - Desenvolve e dissemina práticas de segurança
  - Promove e facilita a comunicação entre seus membros

Cenário Atual

- Aumento dos incidentes de segurança
- Sensação de impunidade por parte dos invasores
- Redes Brasileiras sendo utilizadas como ponto de partida para ataques a outros países

Cenário Atual (cont.)

- Complexidade crescente dos sistemas
- Grande número de vulnerabilidades
- Ataques não são barrados pela maioria dos firewalls (e.g.: IIS, DNS, Vírus)
- Facilidade em ocultar os passos de uma invasão
- Falta de administradores experientes
- Poucos CSIRTs estabelecidos

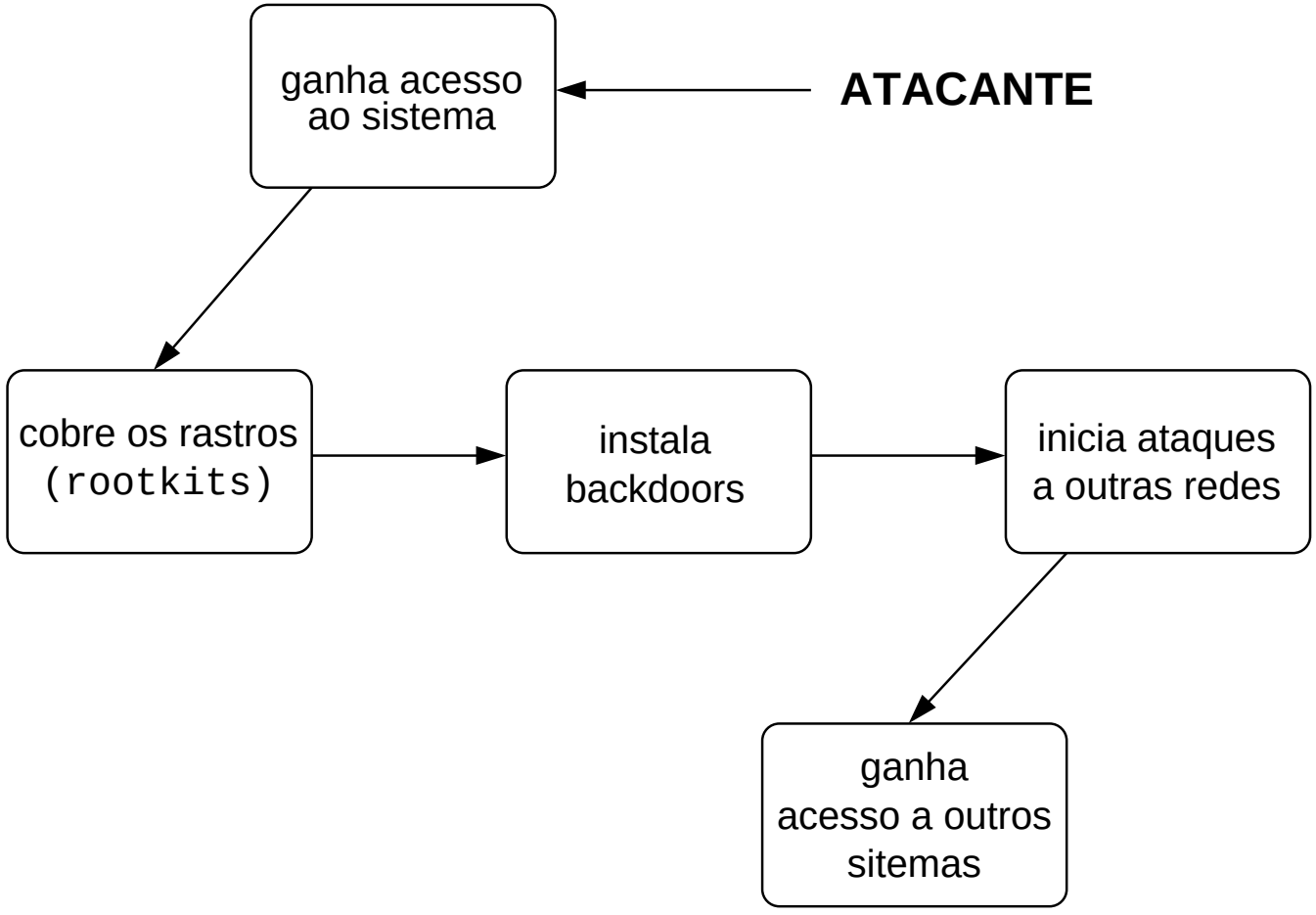
Cenário Atual (cont.)

- Comunicação rápida e eficiente entre invasores (email, Web, conferências, chats)
- Banalização do “Consultor de Segurança”
- “ex”-invasores vendendo “proteção”
- “saber” invadir = saber proteger?
  - invasores com baixo nível técnico
  - ferramentas automáticas (e.g. `rootkits`)
  - ataques coordenados em grande escala

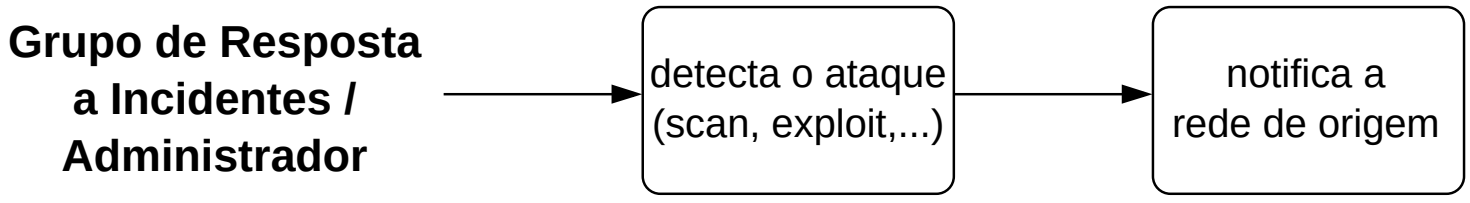
Cenário Atual (cont.)

- Ciclo de um Ataque
- Ciclos de Respostas a Incidentes
  - Tentativa de Invasão
  - Invasão

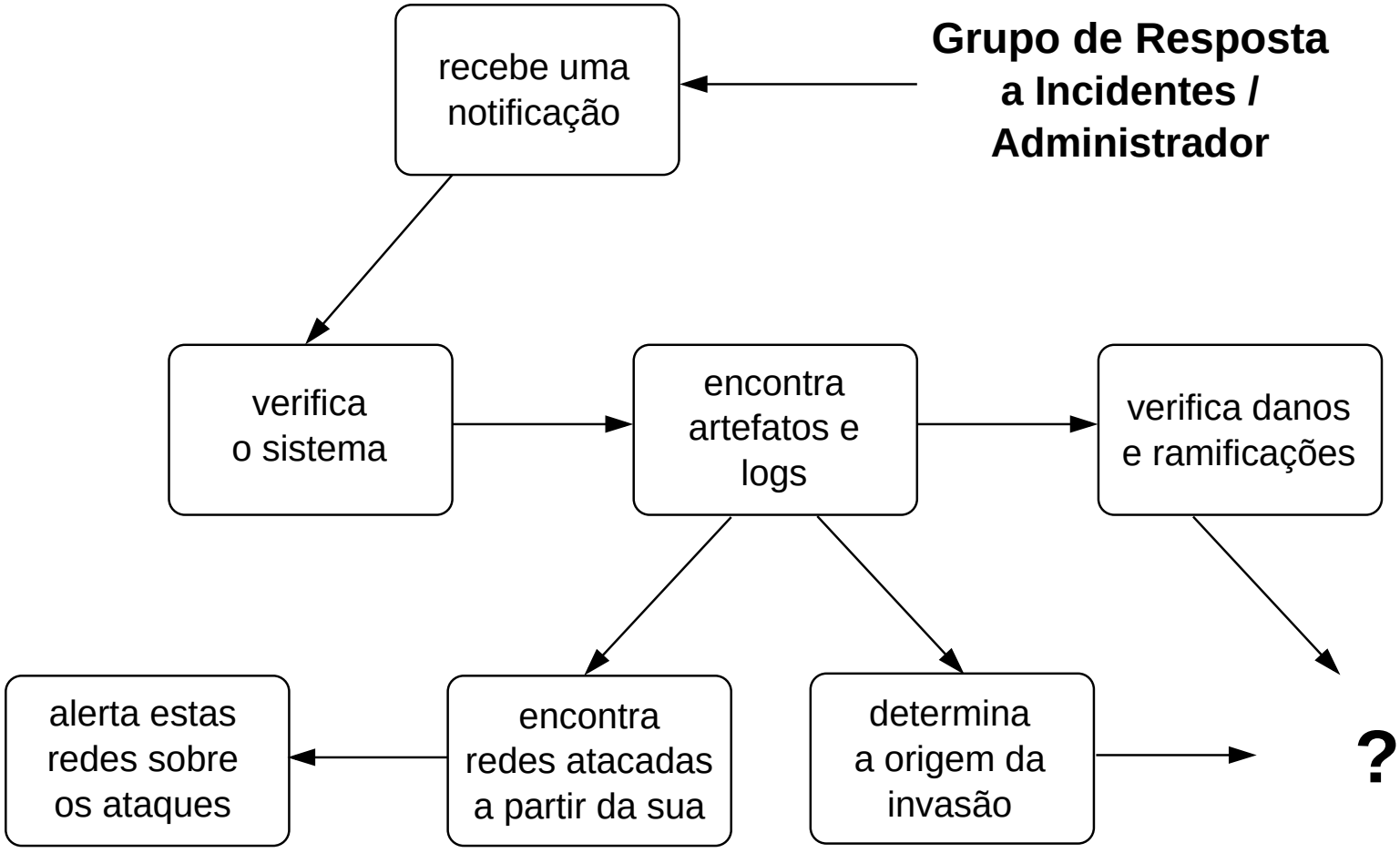
Ciclo de um Ataque



Resposta a Incidentes (1)



Resposta a Incidentes (2)



CSIRT – Computer Security and Incident Response Team

Um grupo ou organização que provê serviços e suporte para um público bem definido, para prevenção, tratamento e resposta a Incidentes de Segurança.

- Ponto central de contato
- Provê informações para o seu público
- Troca informações com outros CSIRTs

Papel do CSIRT

- Coordenar ações
- Determinar o impacto
- Prover recuperação rápida
- Preservar evidências
- Prover recomendações e estratégias
- Ser o ponto de contato com outros grupos, polícia, mídia, etc

Serviços Possíveis de um CSIRT

- Reativos
  - Tratamento de Incidentes
  - Detecção e Rastreamento de Invasões
  - Análise de Artefatos/Vulnerabilidades
- Pró-ativos
  - Configuração e Manutenção dos Sistemas
  - Desenvolvimento de Ferramentas
  - Provimento de documentação e orientação

Tipos de CSIRTs

- Empresas (Cisco PSIRT, VisaCIRT, Citigroup CIRT, Siemens-CERT)
- Países (NBSO, CERT/CC, AusCERT, CERTCC-KR, JPCERT/CC)
- Backbones (CERT-RS, CAIS/RNP, Embratel, Unicamp, SymCERT)
- Órgãos Governamentais (CIAC/DoE, NAVCIRT, DOD-CERT, CERTA/França, CERT-RO/Holanda)

Perfil do Pessoal

- Retidão de Caráter
- Não têm prévio envolvimento com atividades de “hacking”
- Conhecimento:
  - TCP/IP
  - Ambiente de TI da instituição

CSIRTs em Auxílio a Operadores da Justiça

- são os primeiros a ter contato com uma invasão ou uso abusivo dos recursos de informática
- possuem informações privilegiadas sobre o ambiente de rede e o perfil dos usuários
- são os principais responsáveis pela preservação de evidências em casos de invasões

CSIRTs em Auxílio a Operadores da Justiça (cont.)

- podem indicar contatos confiáveis em outras redes
- quem contactar:
  - Brasil: NBSO
  - Outros países: verificar no site do FIRST

Considerações
Sobre a Situação no Brasil

- O que vemos hoje
- Cenário desejável

Situação nos Dias de Hoje

- Não há delegacias especializadas em todos os estados
- Não está disseminada a informação sobre como proceder para noticiar um crime de informática

Situação nos Dias de Hoje (cont.)

- Declarações freqüentes
  - Vítimas: *"Não vou perder meu tempo levando para a polícia, pois no final não vai dar em nada"*
  - Atacantes: *"Não vai acontecer nada comigo mesmo, no máximo meu pai me proíbe de usar o computador e daí eu vou na casa do meu colega"*

Cenário Desejável

- Vários CSIRTs estabelecidos
- Massa de peritos especilizados em crimes de informática
- Operadores da Justiça e CSIRTs cooperando:
  - conferências
  - treinamentos
- Maior participação do Brasil em Fóruns Internacionais (FIRST, HTCIA, etc)

Leitura Recomendada

Secrets & Lies – Digital Security in a Networked World, Bruce Schneier, ISBN 0-471-25311-1, http://www.counterpane.com/sandl.html

Incident Response – Kenneth R. van Wyk, Richard Forno, ISBN 0-596-00130-4, http://www.oreilly.com/catalog/incidentres/

Sites de Interesse

- Material desta apresentação

  `http://www.nbso.nic.br/docs/palestras/`

- Documentação sobre CSIRTs

  `http://www.nbso.nic.br/csirts/`

- Documentação sobre Segurança e Administração de Redes

  `http://www.nbso.nic.br/docs/`

- Documentos, RFCs e sites relacionados

  `http://www.nbso.nic.br/links/`

Sites de Interesse (cont.)

- Comitê Gestor da Internet no Brasil

  http://www.cg.org.br/

- Forum of Incident Response and Security Teams

  http://www.first.org/

- High Technology Crime Investigation Association

  http://www.htcia.org/