DoS, DDoS & Botnets

Alunos: Lucas Gomes, Marcos Seefelder, Vinicius Campos
Professor: Otto Carlos Muniz Bandeira Duarte

Contextualização

- Década de 90: primeiros ataques
  - 1996: SYN *Flood;*
  - Janeiro de 1998: *Smurf* (Redes IRC);
  - 1999: trinoo (Primeiro DDoS);

- 2000 ~ 2004:
  - Mafiaboy: Yahoo, eBay, Amazon, CNN, Dell -> 1 GB/s
  - Ataque a servidores raiz do DNS.

Contextualização

- 2004 ~ 2009:
  - Extorsão: The Million Dollar Page;
  - Aluguel de Botnets;
  - Muitos ataques com motivações políticas;

- Atualidade:
  - Uso de botnets intensificado
  - Motivações variadas
  - *Anonymous*
  - Ciber terrorismo

Ataques de Negação de Serviços (DoS)

- Objetivo: interromper ou prejudicar o fornecimento de um serviço;
- Explora vulnerabilidades dos protocolos de rede e dos sistemas operacionais;
- IP do Atacante:
  - Ataque de forma direta: sem disfarce;
  - IP *Spoofing*: IP mascarado;

Ataques de Negação de Serviços (DoS)

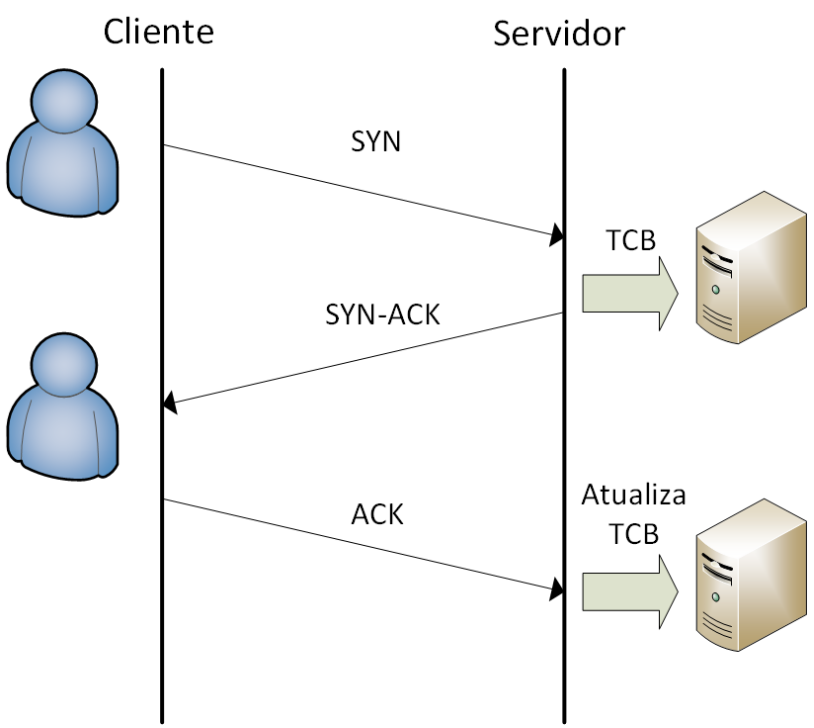
- Formas de Ataque:
  - Força Bruta
  - Protocolo

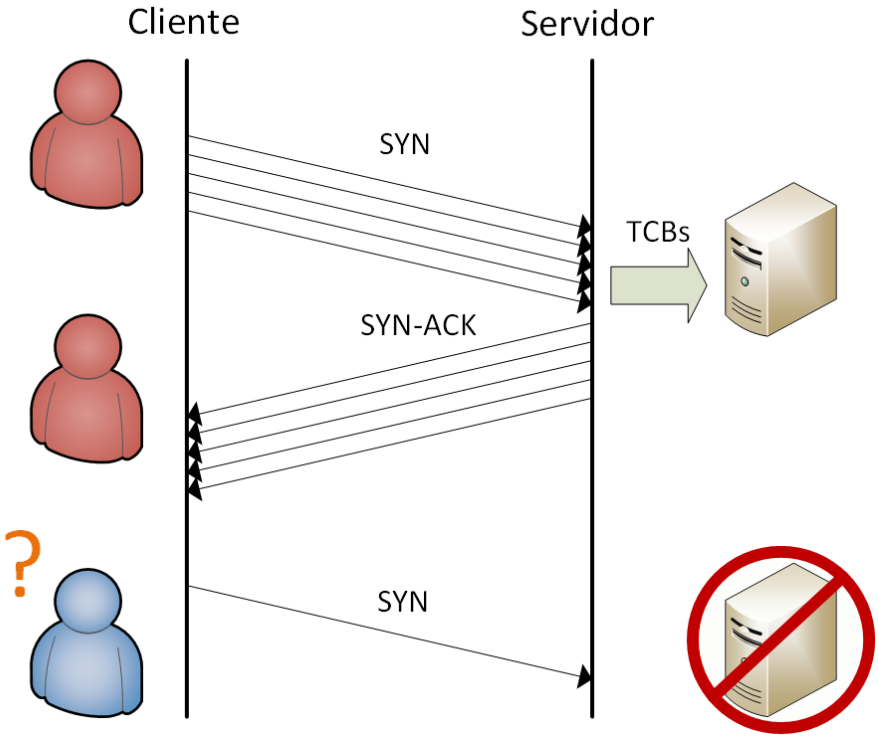
- Alguns ataques têm características das duas formas

SYN *Flood*

- Alvos: Máquinas que usam TCP;
- Explora o processo de apresentação (*handshake*);
- Usa os dados de conexão armazenados no servidor: TCB (*Transmission Control Block*).

SYN *Flood*


Cliente
Servidor
SYN
TCB
SYN-ACK
ACK
Atualiza
TCB


Cliente
Servidor
SYN
TCBs
SYN-ACK
?
SYN

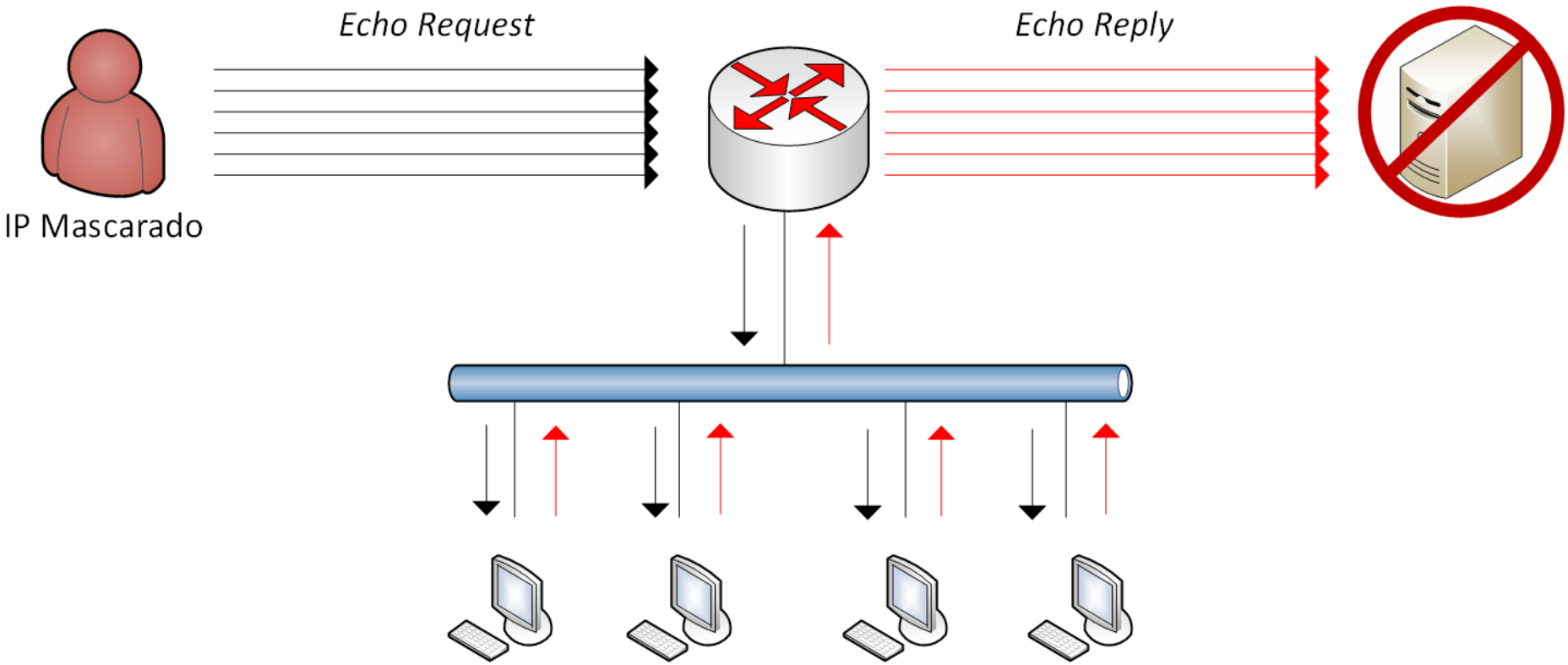
Ataque *Smurf*

- Usa o ICMP (*Internet Control Message Protocol*)
  - *Echo Request*
- Pacotes enviados para endereço de *broadcast* da rede
- IP do remetente mascarado com o IP da vítima

Ataque *Smurf*

- Vítima sobrecarregada com o volume de respostas

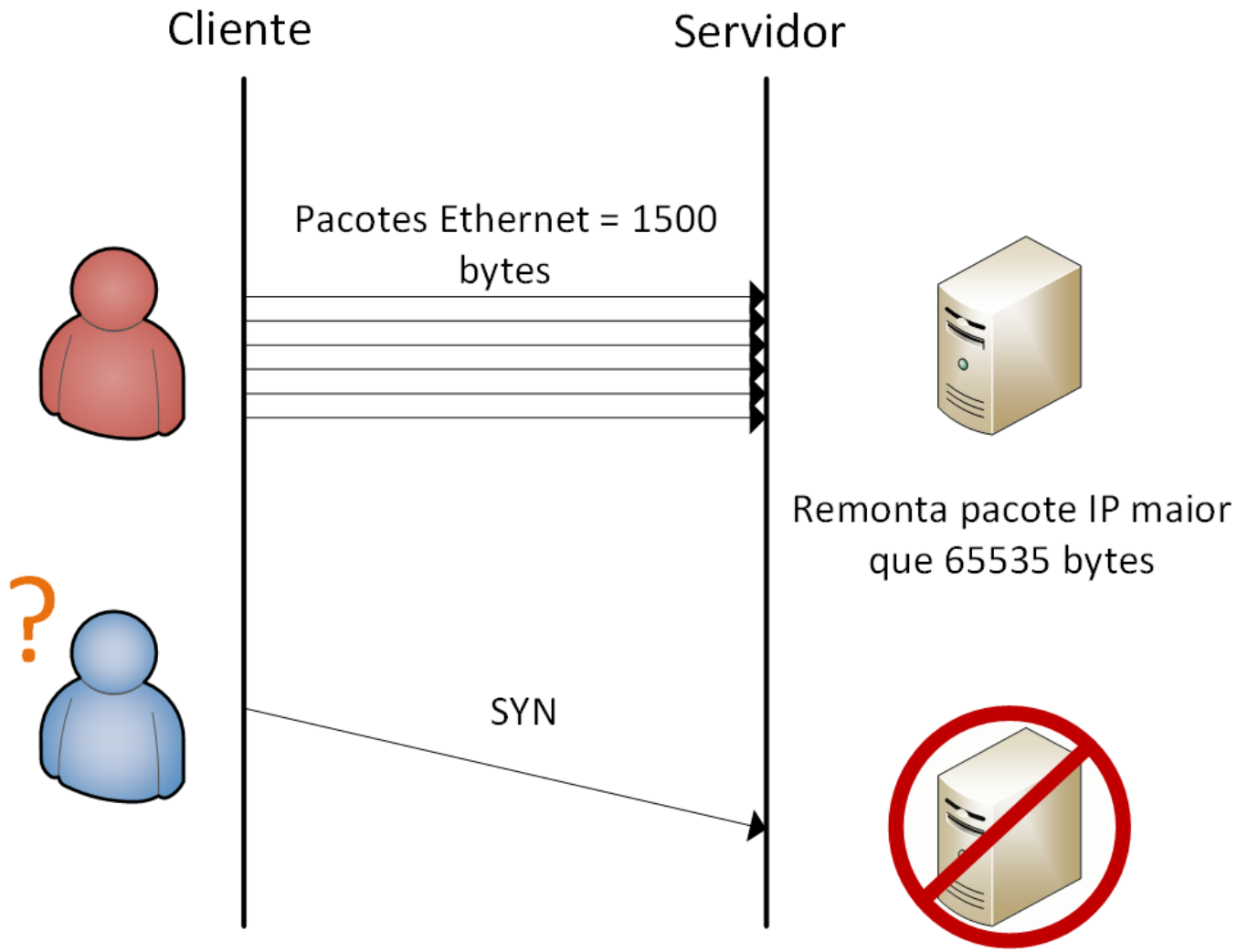
Ataque *Smurf*



Ping da morte

- Explora a divisão e remontagem de pacotes;
- Pacote IP < 65535 bytes;
- Pacote Ethernet < 1500 bytes;
- Envio de fragmentos de um pacote IP maior que o limite;

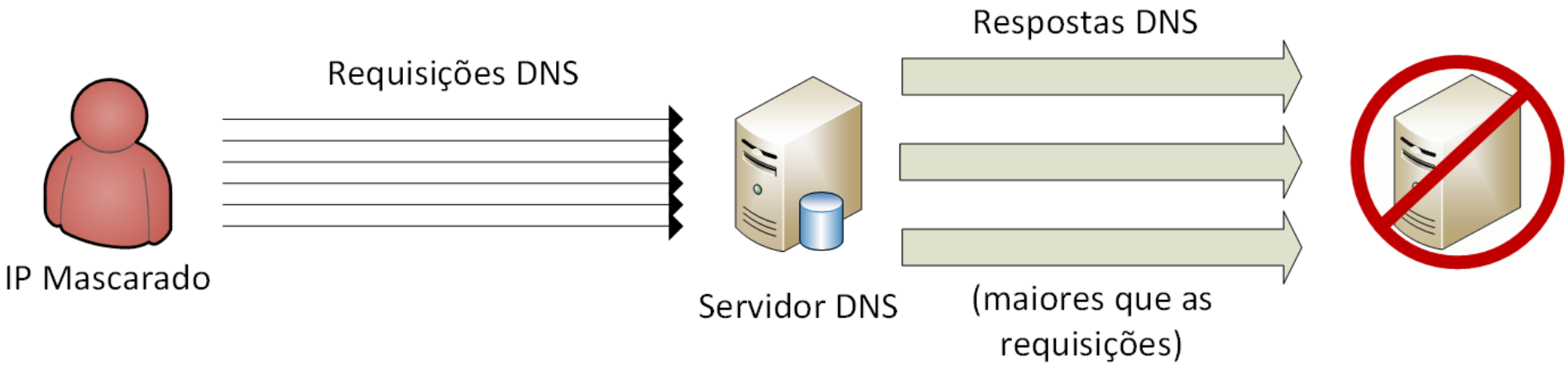
Ping da morte



Ataques de Amplificação DNS

- Explora a razão entre o tamanho da requisição e o tamanho da resposta DNS;
- Resposta > Requisição;
- IP do atacante mascarado com o IP da vítima;

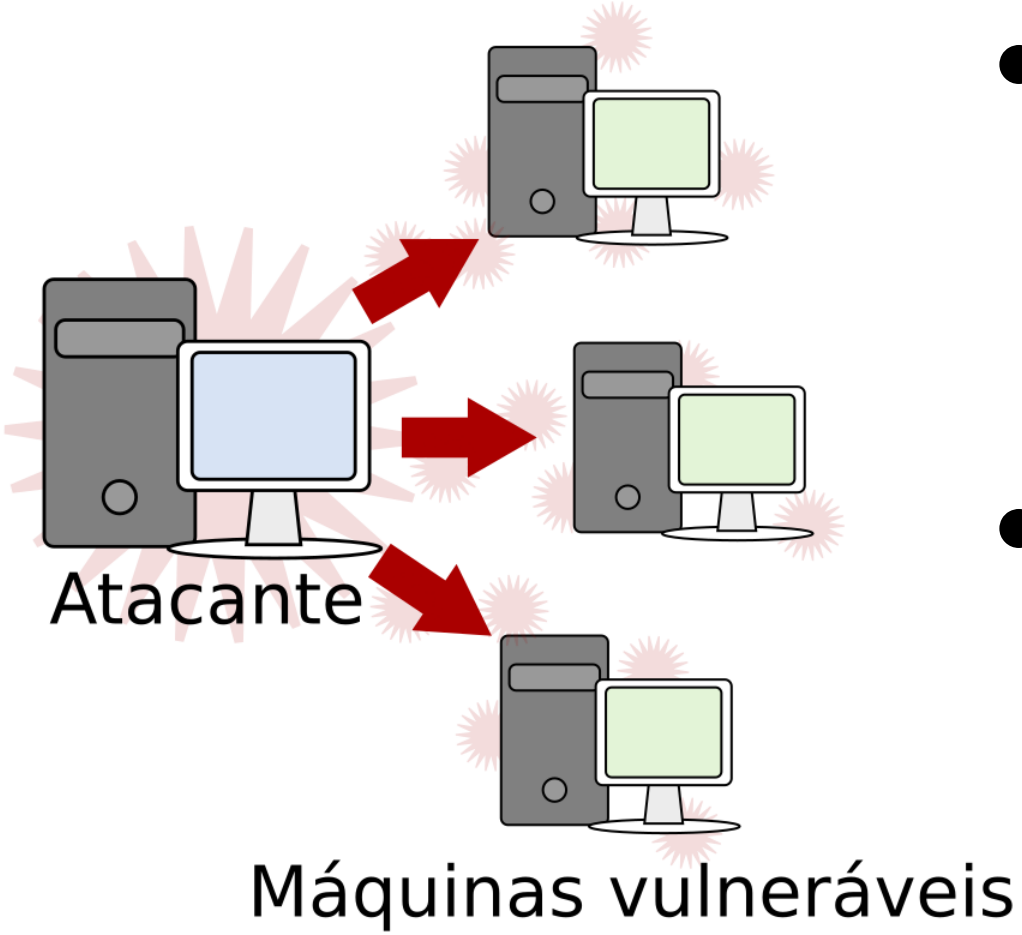
Ataques de Amplificação DNS



Ataques Distribuídos de Negação de Serviços (DDoS)

- Diversos ataques DoS conjuntos e coordenados;
- Realizado por uma rede de máquinas *zombie;*
- Duas etapas:
  - Recrutamento;
  - Comando de ataque;

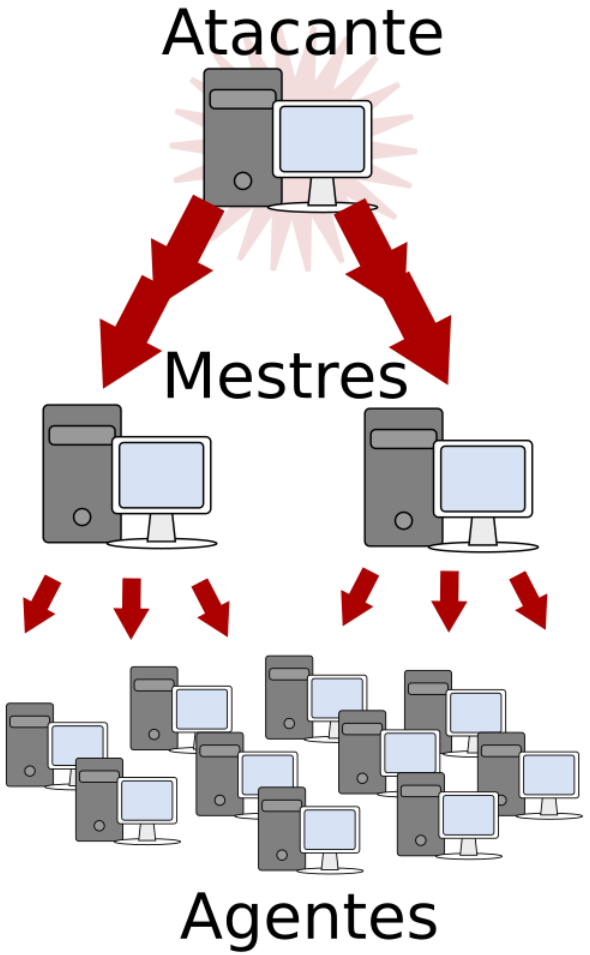
Ataques Distribuídos de Negação de Serviços (DDoS)



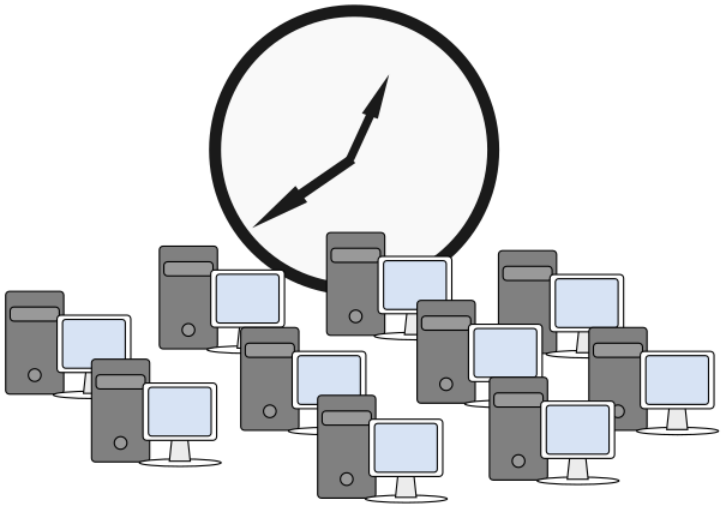
- Recrutamento:
  - Manual
  - Atumático
- Propagação

Ataques Distribuídos de Negação de Serviços (DDoS)

- Comando de ataque:
  - *Handlers* (mestres)
  - Pré-programado



Ataques Distribuídos de Negação de Serviços (DDoS)



- Dificulta desarme
- *Backdoors*

Ataques Distribuídos de Negação de Serviços (DDoS)

- Ataque:
  - Consumo de banda e recursos
    - *Smurf, Fraggle* e *packet-floods* em geral
  - Exploração de protocolos ou aplicações
    - *Syn flood, bugs, Zero-Day*

Como são e o que são essas redes de agentes?

Bot

- *T*ermo genérico para descrever um *script* que desempenha funções preestabelecidas de forma automatizada;

- Usos:
  - indexação de sites;
  - jogos;
  - ataques;

IRC

- Protocolo de comunicação;
- Jarkko Oikarinen, 1988;
- Interação:
  - Conversa por texto;
  - Canal;
- Arquitetura cliente servidor;

Botnet

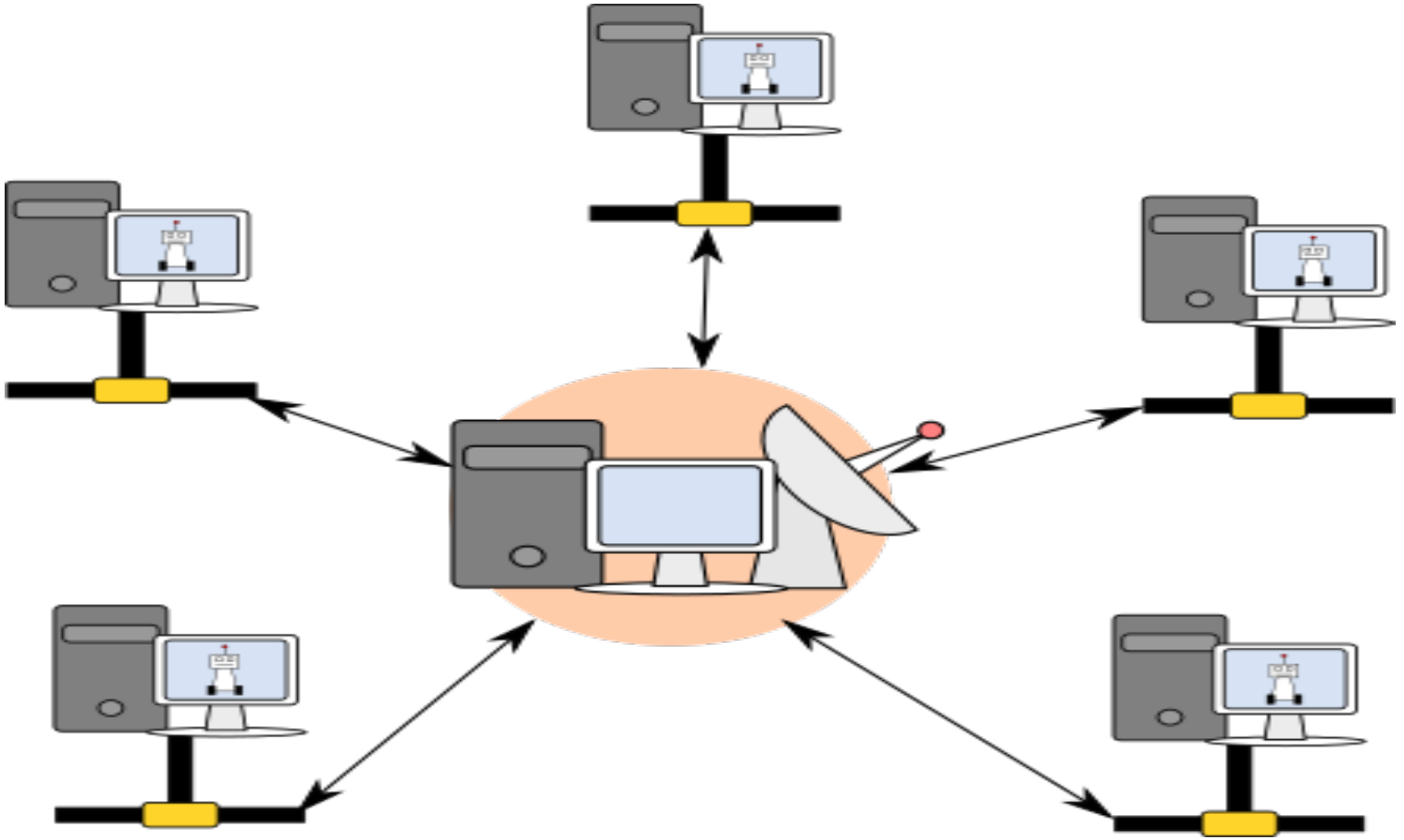
- Conjunto de *bots* servindo ao mesmo mestre;
- Troca de mensagens:
  - Recepção de comandos;
  - Envio de resultados;
- Servidor C&C;

Botnet

- Propagação:
  - Vulnerabilidades;
  - Instalação não intencional;
- Sistema Operacional;
- Parâmetros:
  - Banda;
  - Poder de processamento;

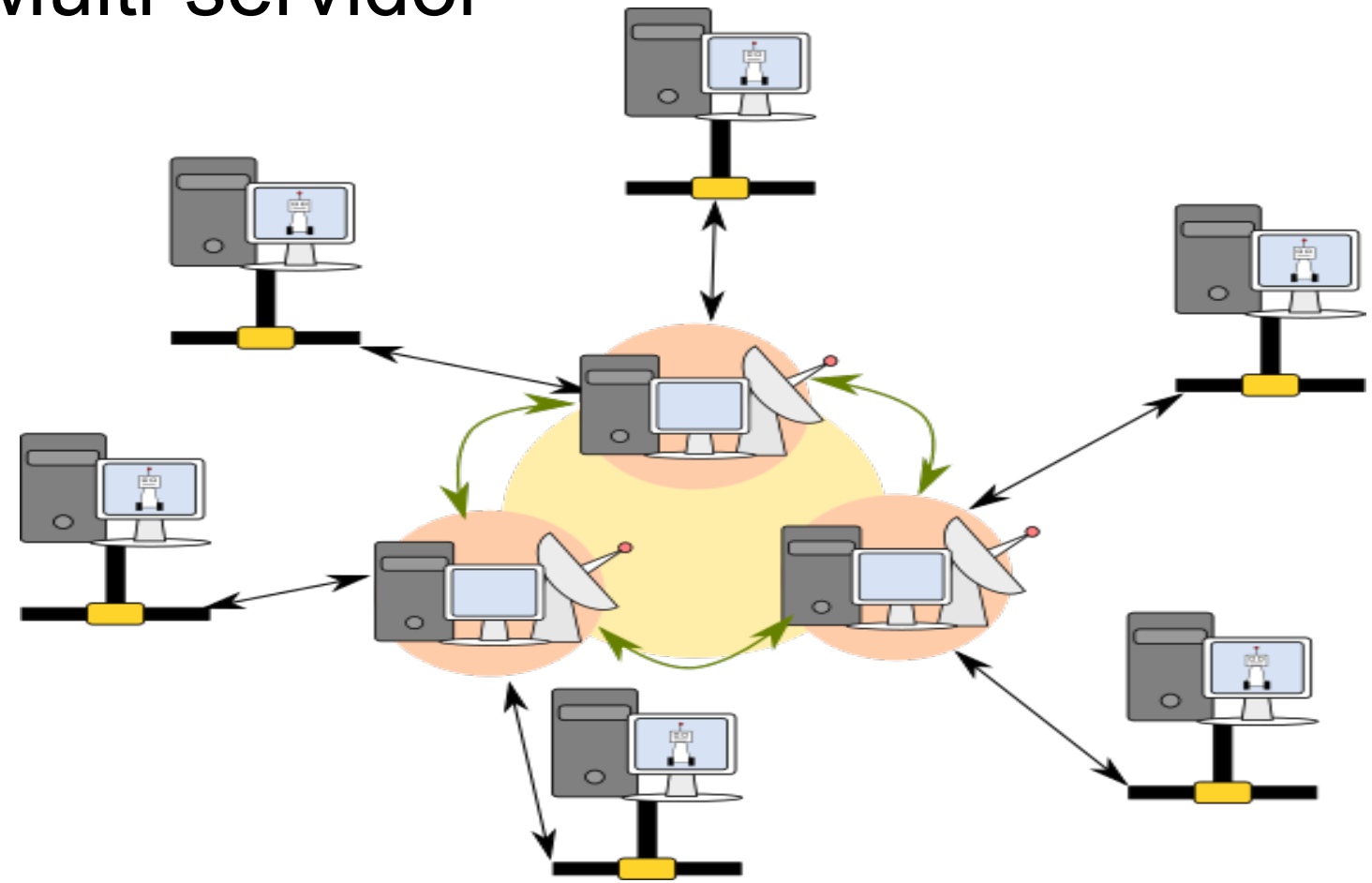
Topologias de comunicação da *botnet*

- Estrela



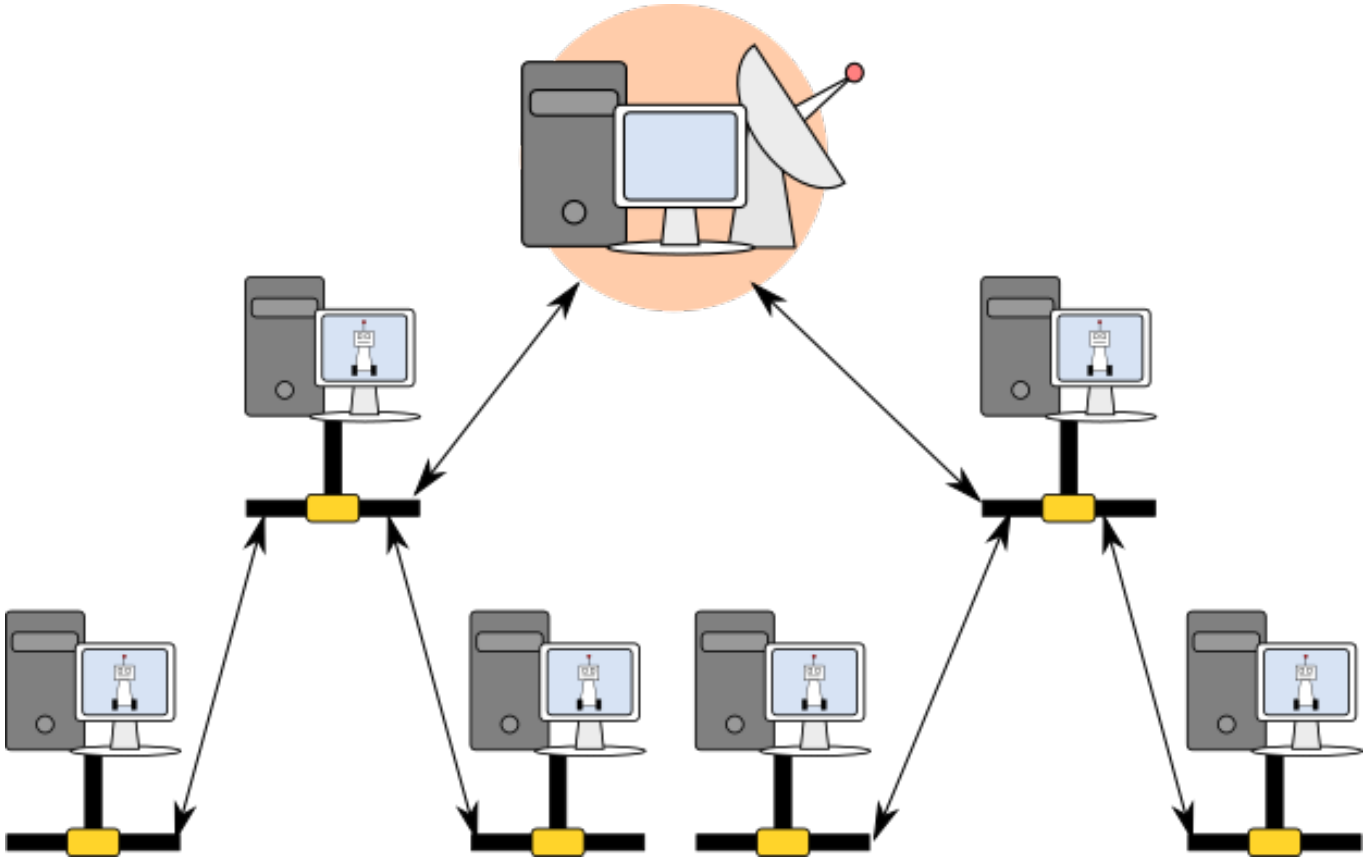
Topologias de comunicação *botnet*

- Multi-servidor



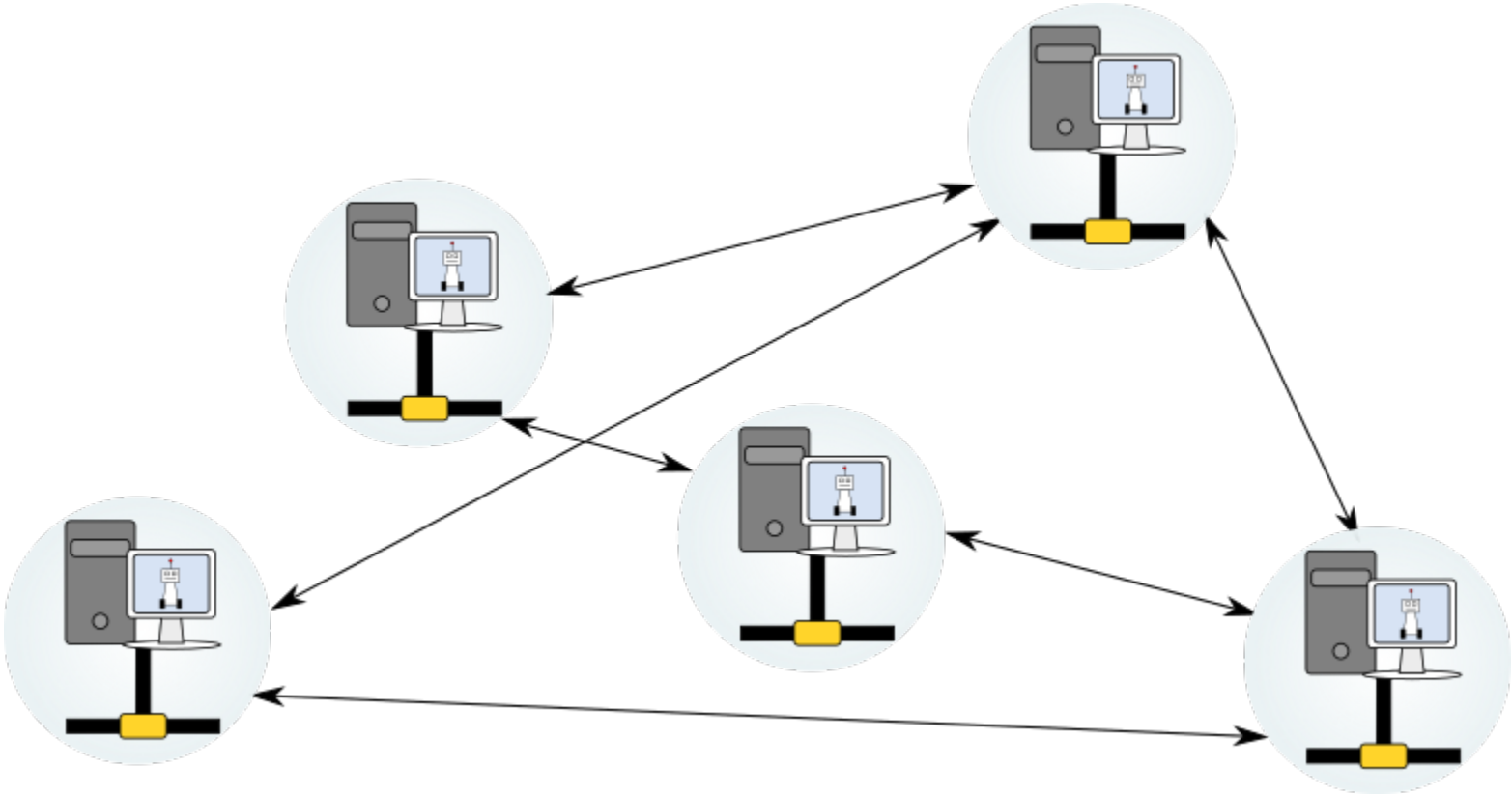
Topologias de comunicação de *botnet*

- Hierárquica



Topologias de comunicação de *botnet*

- Randômica



Atividades maliciosas

- DDoS;
- “Infecção local secundária”
  - Key logger;
- “Troca de banda”;
- *Backdoor;*

Proteção

- Prevenir
- Detectar
- Responder

Botnets legais

- *Charity Engine*:
  - Caridade;
  - Recompensa;

- *Folding @ Home (Stanford):*
  - Alzheimer's;
  - Huntington's;
  - Parkinson's;
  - Câncer;

Conclusão

- Ataques DoS existem desde o surgimento das redes de computadores;

- Não eram considerados de grande importância
  - Não afetavam serviços importantes;

Conclusão

- Popularização da Internet
  - Aumento da comunidade *hacker*
  - Maior visibilidade

- Maior incentivo + comunidade hacker maior: sofisticação dos ataques;

Conclusão

- Atualmente, DoS é uma ameaça a grandes empresas e órgãos governamentais, e um desafio para companhias de segurança
  - Exploração de brechas difíceis de reparar;
  - Poder computacional maciço através das *botnets*

Conclusão

- Ataques DDoS são uma área de pesquisa de importância em centros de pesquisas e universidades;

- Princípios dos ataques são aplicados para fins benéficos -> *Botnets* legais

Questões

- Quais as vantagens e desvantagens de se utilizar o IP Spoofing?
- Quais as formas de se evitar um ataque Smurf?
- Do ponto de vista do atacante, qual a vantagem e qual a desvantagem de realizar um ataque de exploração de protocolo ao invés de um ataque de consumo de banda e recursos?

Questões

- Qual é a principal desvantagem da utilização de uma topologia multi-servidor?
- Qual seria uma possível maneira utilizada para detectar uma botnet?

Respostas:

Vantagens: Evita filtros de IP implementados em firewalls, dificulta o rastreamento e a máquina atacante não recebe pacotes de resposta.

Desvantagem: Requer maior processamento e torna a execução do ataque mais complexa.

Respostas:

Um ataque Smurf pode ser evitado bloqueando-se pacotes ICMP que tenham como destinatário o endereço de broadcast, por meio de um filtro adicionado a um firewall.

Respostas:

A vantagem é que é necessário gerar menos volume de ataque do que um ataque de consumo de banda, uma vez que ao invés de utilizar a força bruta, os ataques de protocolo acertam o sistema em pontos fracos. A desvantagem é que são mais facilmente prevenidos através da modificação dos protocolos utilizados.

Respostas:

Exige mais esforço e conhecimento para a construção da infraestrutura de um C&C multi-servidor.

Respostas:

Detectar a comunicação C&C ou detectar características secundárias de uma da máquina (bot).