DoS e DDoS: Ataques de Negação de Serviço

Segurança da Informação

Charles Tim Batista Garrocho

Instituto Federal de São Paulo – IFSP
Campus Campos do Jordão

garrocho.ifspcjo.edu.br/SEGA6

charles.garrocho@ifsp.edu.br

Curso Superior de TADS

DoS - Defenal of Service

Um **ataque de negação de serviço** (DoS - Defenal of Service), é uma tentativa de tornar os recursos de um sistema indisponíveis para seus utilizadores.

Não visa invadir um computador para extrair informações.

Não modifica o conteúdo armazenado no computador.

Tornar inacessíveis os serviços providos pela vítima a usuários legítimos.

A vítima simplesmente **para de ofecer o seu serviço** aos clientes legítimos, enquanto tenta lidar com o **tráfego** gerado pelo atacante.

DoS - Defenial of Service

A vítima (servidor) recebe um número significativo de **requisições HTTP**.

Isso faz com que o servidor fique sobrecarregado de solicitações do cliente e **demore** a responder a novas requisições.

(DDoS) Distributed Denial of Service

Num **ataque distribuído de negação de serviço** (DDoS - Distributed Denial of Service), um computador **mestre** denominado Master pode ter sob seu comando até milhares de computadores **Zombies**.

Nesse caso, as tarefas de ataque de negação de serviço são **distribuídas** a um *exército* de máquinas escravizadas.

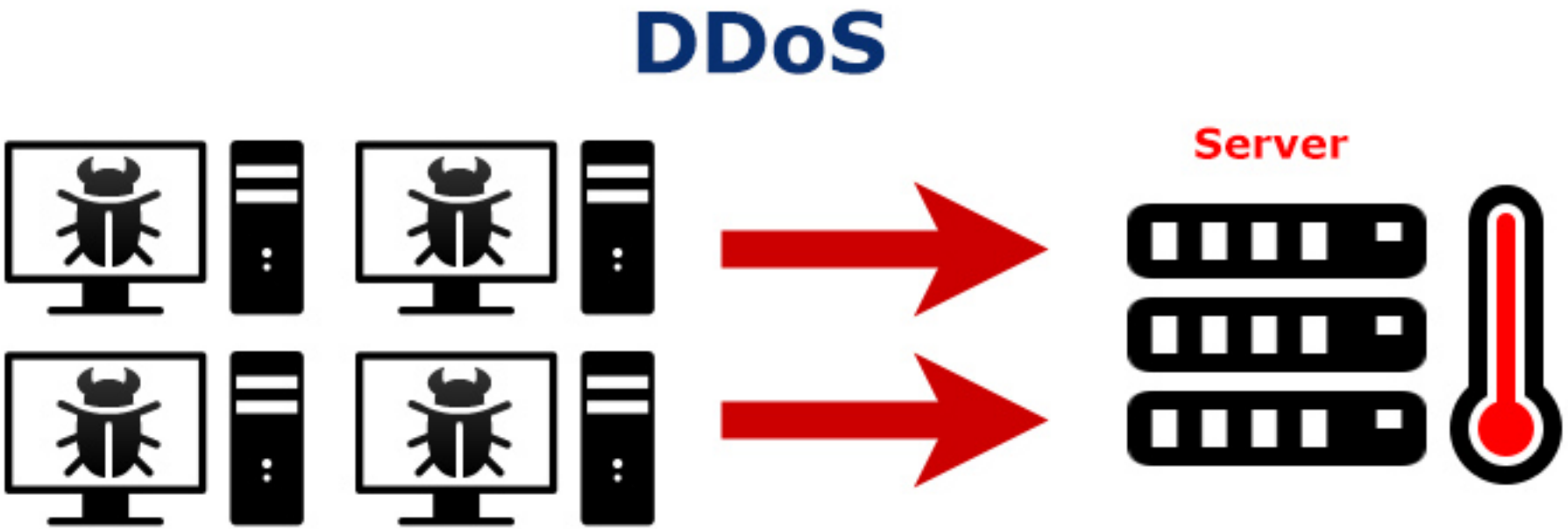
O ataque consiste em fazer com que os Zombies se preparem para executar uma determinada requisição a um recurso num determinado servidor **numa mesma hora de uma mesma data**.

O grande e repentino número de requisições de acesso **sobrecarrega o servidor**, fazendo com que o servidor não seja capaz de atender a mais nenhum pedido.

INSTITUTO FEDERAL

(DDoS) Distributed Denial of Service

Parecido com um ataque DoS. Entretanto o ataque DDoS ocorre de forma distribuída.



Tipos de Ataques DDoS

Ataques por Inundação: Se caracterizam por enviarem um grande volume de tráfego ao sistema da vítima de modo a congestionar sua banda.

Ataques por Amplificação: Se caracterizam por enviarem requisições forjando o endereço IP de origem das requisições para o endereço IP da vítima, de forma com que todas as respostas sejam direcionadas para o alvo do ataque.

Ataques por Exploração de Protocolos: Se caracterizam por consumir excessivamente os recursos da vítima explorando alguma característica específica ou faha de implementação de algum protocolo instalado no sistema da vítima.

Como se proteger?

Como servidores podem ter estrutura e recursos diferentes, **não há fórmula mágica** que funcione em todas as implementações que consiga evitar ou combater ataues DoS ou DDoS.

Dentre as estratégias recomendadas pode-se considerar as seguintes:

- Incrementar a segurança do host;
- Aplicar filtros anti-spoofing;
- Limitar a banda por tipo de tráfego;
- Manter as atualizações dos sistemas em dia.