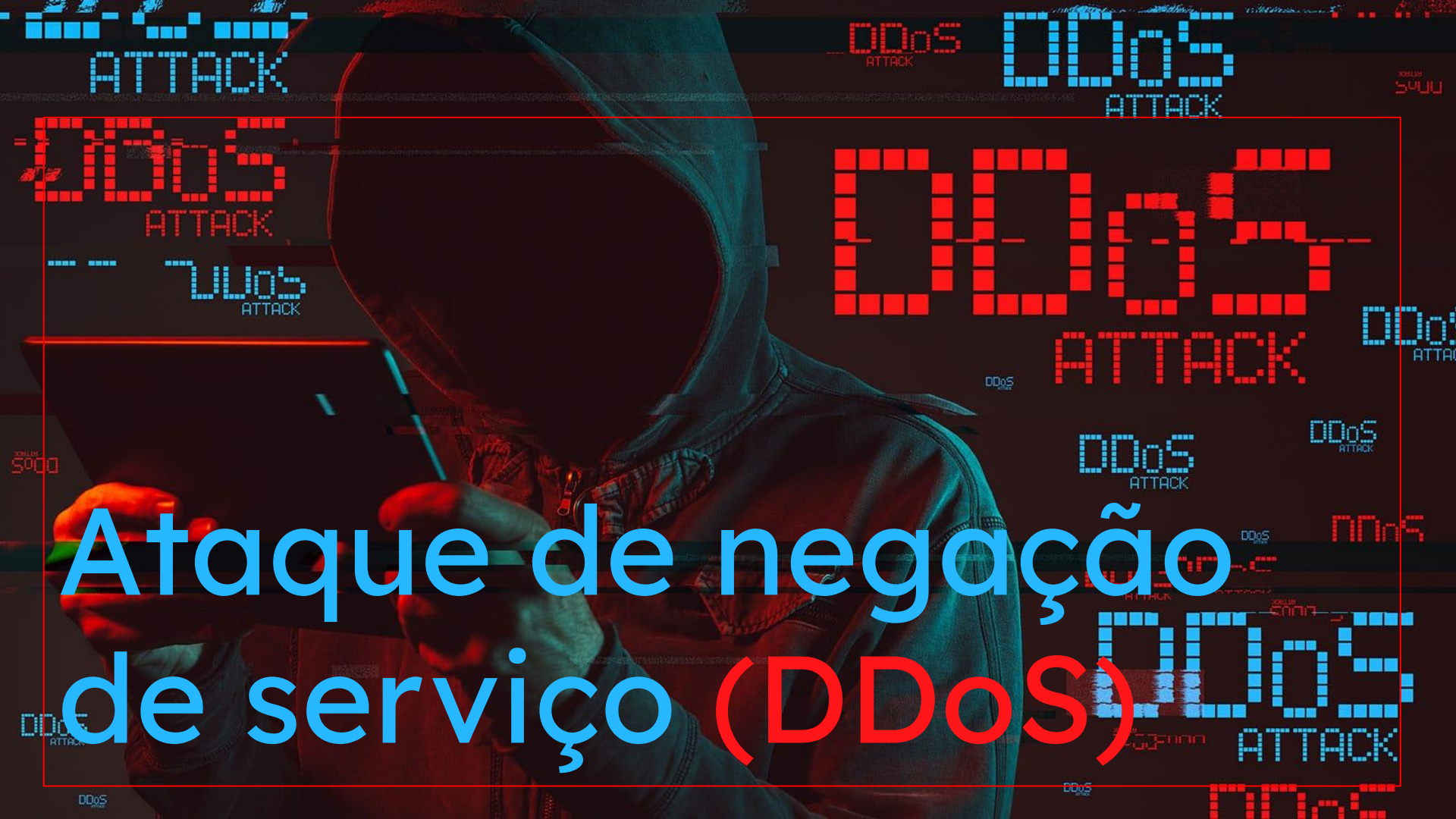
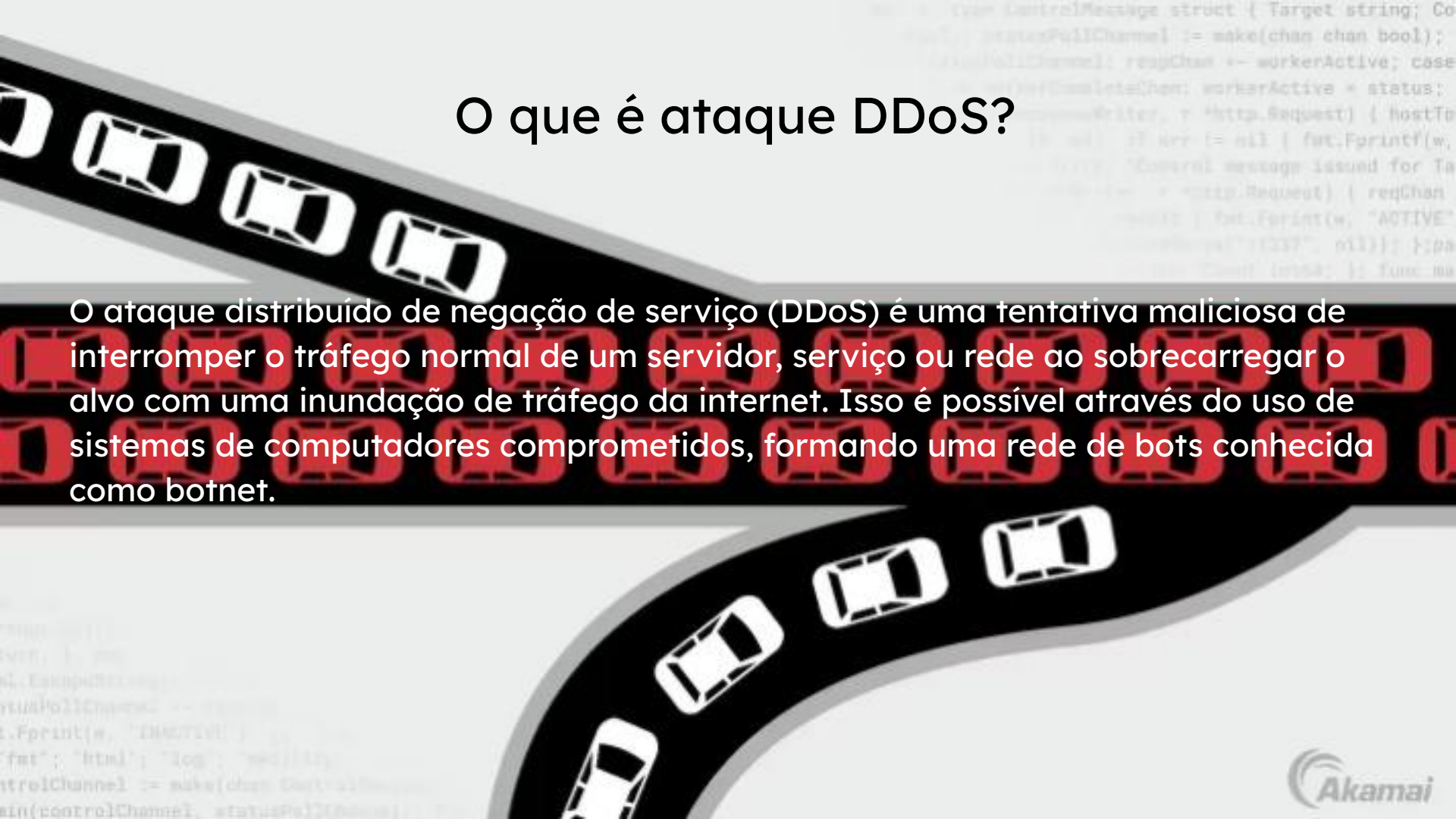

Ataque de negação de serviço (DDoS)

O que é ataque DDoS?



O ataque distribuído de negação de serviço (DDoS) é uma tentativa maliciosa de interromper o tráfego normal de um servidor, serviço ou rede ao sobrecarregar o alvo com uma inundação de tráfego da internet. Isso é possível através do uso de sistemas de computadores comprometidos, formando uma rede de bots conhecida como botnet.

Tipos de ataques DDoS:

Existem três categorias principais de ataques DDoS:

Ataques à camada de aplicação (Camada 7): Visam exaurir os recursos do alvo, prejudicando a geração e distribuição de páginas da web.

Ataques de protocolo: Exploram vulnerabilidades nas camadas 3 e 4 da pilha de protocolos, consumindo recursos de servidores e equipamentos de rede.

Ataques volumétricos: Tentam criar congestionamento consumindo toda a largura de banda disponível entre o alvo e a internet, utilizando amplificação ou tráfego em massa, como o de uma botnet.

Áreas de ataque (Integridade, confiabilidade ou Vulnerabilidade):

Os ataques DDoS podem impactar a confiabilidade e a disponibilidade de um sistema ao sobrecarregar seus recursos. A integridade também pode ser comprometida, especialmente em ataques à camada de aplicação, onde a manipulação de dados pode ocorrer.

Por que esses ataques acontecem?

Os crackers realizam ataques DDoS com diversos objetivos, como prejudicar a reputação de uma empresa, extorquir dinheiro, ou mesmo por motivações ideológicas. Esses ataques são frequentemente executados por grupos de hackers para criar interrupções e causar danos.

Como se prevenir desses ataques?

Identificar sinais de ataque: Monitorar padrões de tráfego suspeitos, como picos incomuns.

Mitigação multivector: Implementar estratégias diversificadas para combater diferentes tipos de ataques.

Roteamento para black hole: Criar uma rota que direcione o tráfego para um black hole em casos extremos.

Rate Limiting: Limitar o número de solicitações aceitas por um servidor em um período de tempo.

Firewall de Aplicativos Web (WAF): Usar um WAF para filtrar solicitações maliciosas na camada 7.

Difusão de rede anycast: Dispersar o tráfego do ataque por uma rede de servidores distribuídos para absorção.

A proteção contra DDoS é uma abordagem multifacetada e depende da implementação de várias medidas preventivas e de mitigação para garantir a segurança e a continuidade dos serviços online.