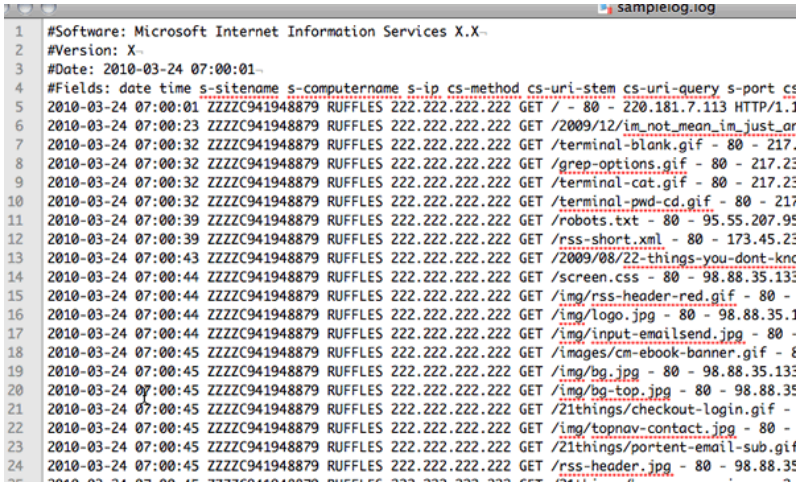
Um Framework Baseado na Pilha ELK Para Análise Pós-Intrusão de Ataques de DDoS

Camilla Alves, André Monteiro
CEFET/RJ – Campus Petrópolis

CEFET/RJ
campus Petrópolis

Motivação

- Análise baseada em logs de ataques de DDoS



Motivação

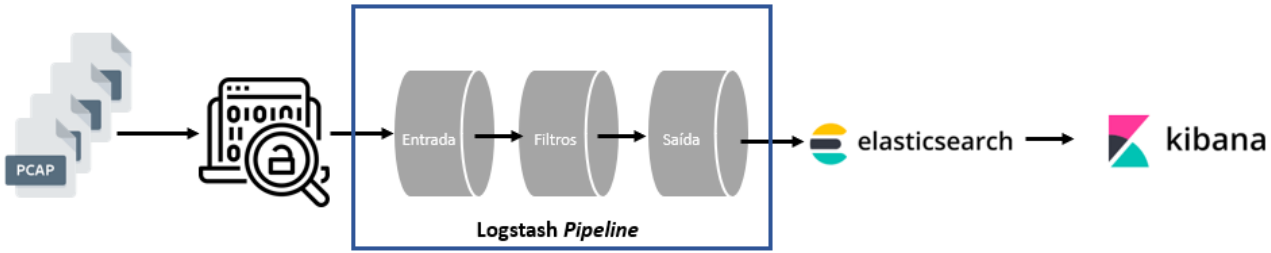
- Análise baseada em logs de ataques de DDoS

Problema

- Análise pós-intrusão de ataques de DDoS
  - Baseada em dados não estruturados (logs)
  - Complexa
  - Grande volume de dados

- Pilha ELK
  - Soluções com objetivo específico
  - Poucas ferramentas com abordagem ponta a ponta

Solução Proposta



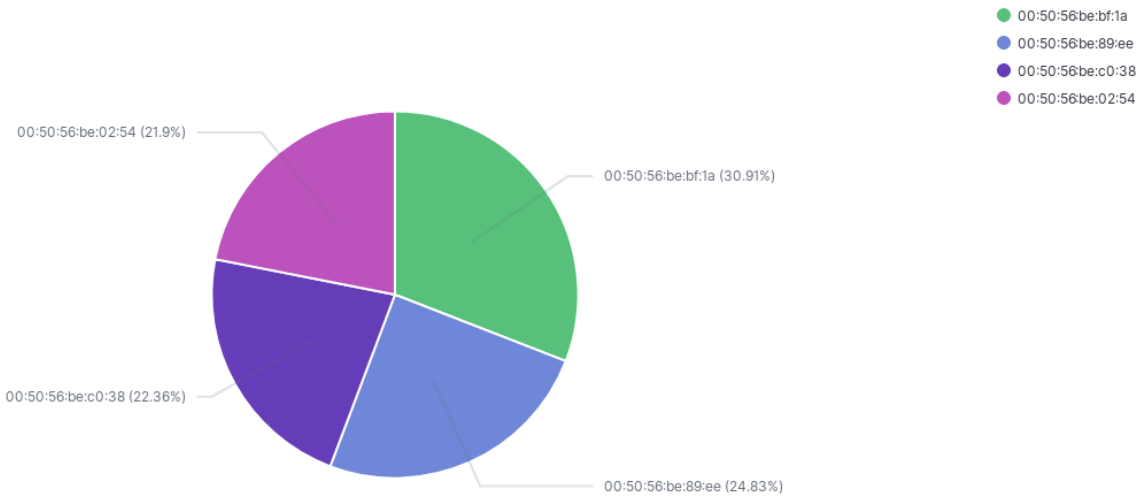
- Algoritmo para identificação de ataques
  - Características de ataques de DDoS
  - Arquivo JSON com os vetores de ataque
  - Indexação, armazenamento e visualização

Identificação de ataques de DDoS

- Definir o alvo dos ataques
  - IP destino com a maior quantidade de pacotes recebidos
- Evidenciar uma inundação de tráfego
  - Quantidade de SYN e SYN/ACK recebidos
- Definição dos vetores de ataque de DDoS
  - IP origem/destino, protocolos, portas e timestamp

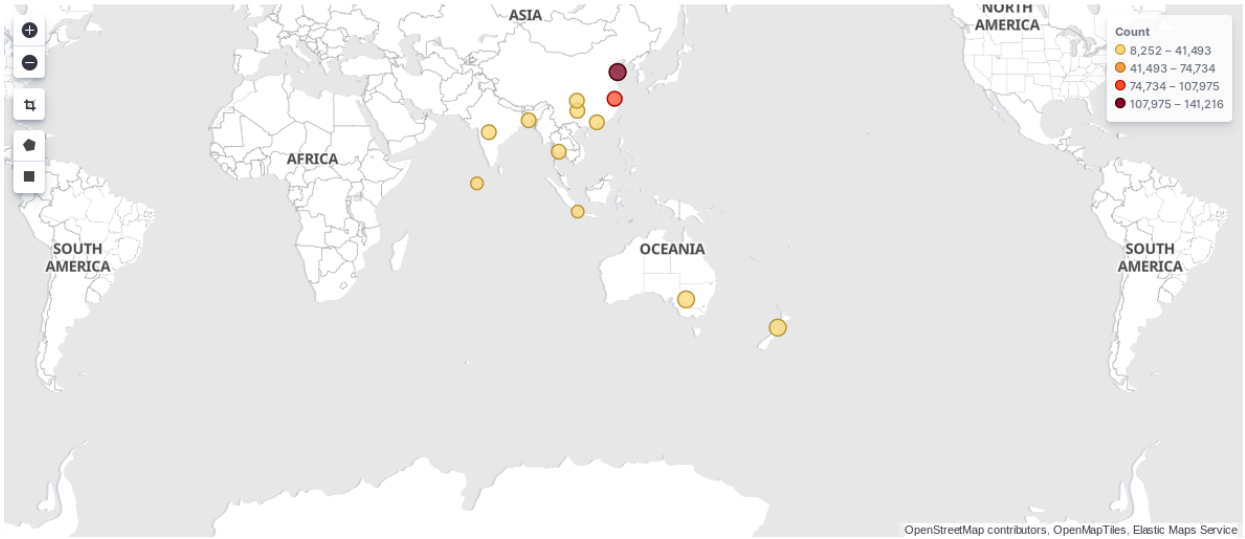
Resultados

- Ambiente de IoT



Resultados

- Booter (DDoS-as-a-Service)



Considerações Finais

- Algoritmo eficiente para identificação de ataques
- Abordagem ELK de ponta a ponta
- Trabalhos futuros
  - Análise de DDoS em tempo real
  - Restrições da plataforma computacional

Obrigado!

- Camilla Alves e André Monteiro

camilla.Alves@aluno.cefet-rj.br

andre.monteiro@cefet-rj.br