



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

Camilla Alves, André Monteiro  
CEFET/RJ – Campus Petrópolis

# Motivação

- Análise baseada em logs de ataques de DDoS

```
samplelog.log
1 #Software: Microsoft Internet Information Services X.X-
2 #Version: X-
3 #Date: 2010-03-24 07:00:01-
4 #Fields: date time s-sitename s-computername s-ip cs-method cs-uri-stem cs-uri-query s-port cs
5 2010-03-24 07:00:01 ZZZZC941948879 RUFFLES 222.222.222.222 GET / - 80 - 220.181.7.113 HTTP/1.1
6 2010-03-24 07:00:23 ZZZZC941948879 RUFFLES 222.222.222.222 GET /2009/12/in_not_mean_im_just_ar
7 2010-03-24 07:00:32 ZZZZC941948879 RUFFLES 222.222.222.222 GET /terminal-blank.gif - 80 - 217.
8 2010-03-24 07:00:32 ZZZZC941948879 RUFFLES 222.222.222.222 GET /grep-options.gif - 80 - 217.2
9 2010-03-24 07:00:32 ZZZZC941948879 RUFFLES 222.222.222.222 GET /terminal-cat.gif - 80 - 217.2
10 2010-03-24 07:00:32 ZZZZC941948879 RUFFLES 222.222.222.222 GET /terminal-pwd-cd.gif - 80 - 217
11 2010-03-24 07:00:39 ZZZZC941948879 RUFFLES 222.222.222.222 GET /robots.txt - 80 - 95.55.207.95
12 2010-03-24 07:00:39 ZZZZC941948879 RUFFLES 222.222.222.222 GET /rss-short.xml - 80 - 173.45.2
13 2010-03-24 07:00:43 ZZZZC941948879 RUFFLES 222.222.222.222 GET /2009/08/22-things-you-dont-knc
14 2010-03-24 07:00:44 ZZZZC941948879 RUFFLES 222.222.222.222 GET /screen.css - 80 - 98.88.35.13
15 2010-03-24 07:00:44 ZZZZC941948879 RUFFLES 222.222.222.222 GET /img/rss-header-red.gif - 80 -
16 2010-03-24 07:00:44 ZZZZC941948879 RUFFLES 222.222.222.222 GET /img/logo.jpg - 80 - 98.88.35.1
17 2010-03-24 07:00:44 ZZZZC941948879 RUFFLES 222.222.222.222 GET /img/input-emailsend.jpg - 80 -
18 2010-03-24 07:00:45 ZZZZC941948879 RUFFLES 222.222.222.222 GET /images/cm-ebook-banner.gif - 80 -
19 2010-03-24 07:00:45 ZZZZC941948879 RUFFLES 222.222.222.222 GET /img/bg.jpg - 80 - 98.88.35.13
20 2010-03-24 07:00:45 ZZZZC941948879 RUFFLES 222.222.222.222 GET /img/bg-top.jpg - 80 - 98.88.35
21 2010-03-24 07:00:45 ZZZZC941948879 RUFFLES 222.222.222.222 GET /21things/checkout-login.gif -
22 2010-03-24 07:00:45 ZZZZC941948879 RUFFLES 222.222.222.222 GET /img/topnav-contact.jpg - 80 -
23 2010-03-24 07:00:45 ZZZZC941948879 RUFFLES 222.222.222.222 GET /21things/portent-email-sub.gif -
24 2010-03-24 07:00:45 ZZZZC941948879 RUFFLES 222.222.222.222 GET /rss-header.jpg - 80 - 98.88.35
```

# Motivação

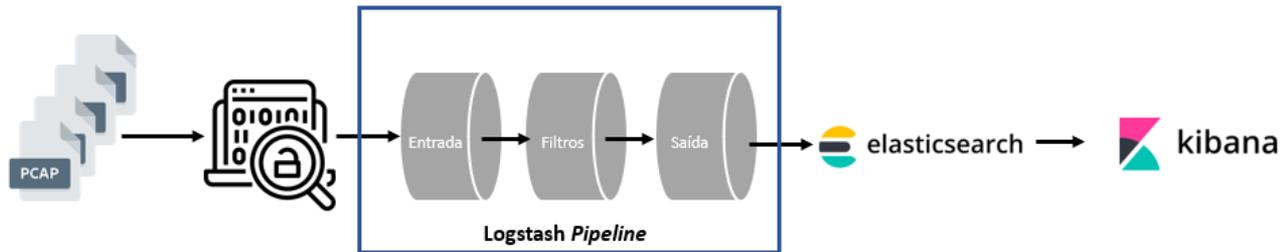
- Análise baseada em logs de ataques de DDoS



# 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



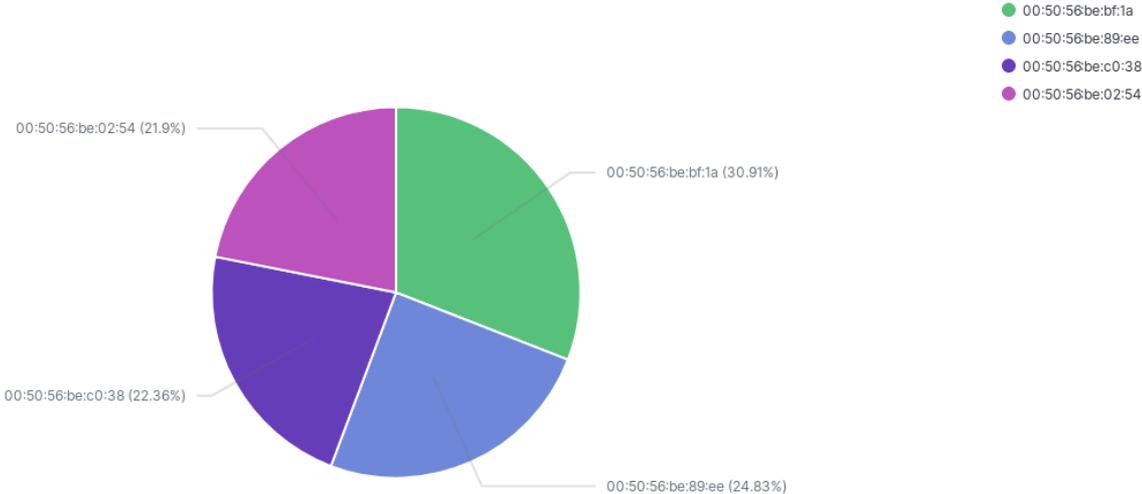
- Algoritmo para identificação de ataques
  - Características de ataques de DDoS
  - Arquivo JSON com os vetores de ataque
  - Indexação, armazenamento e visualização

# 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

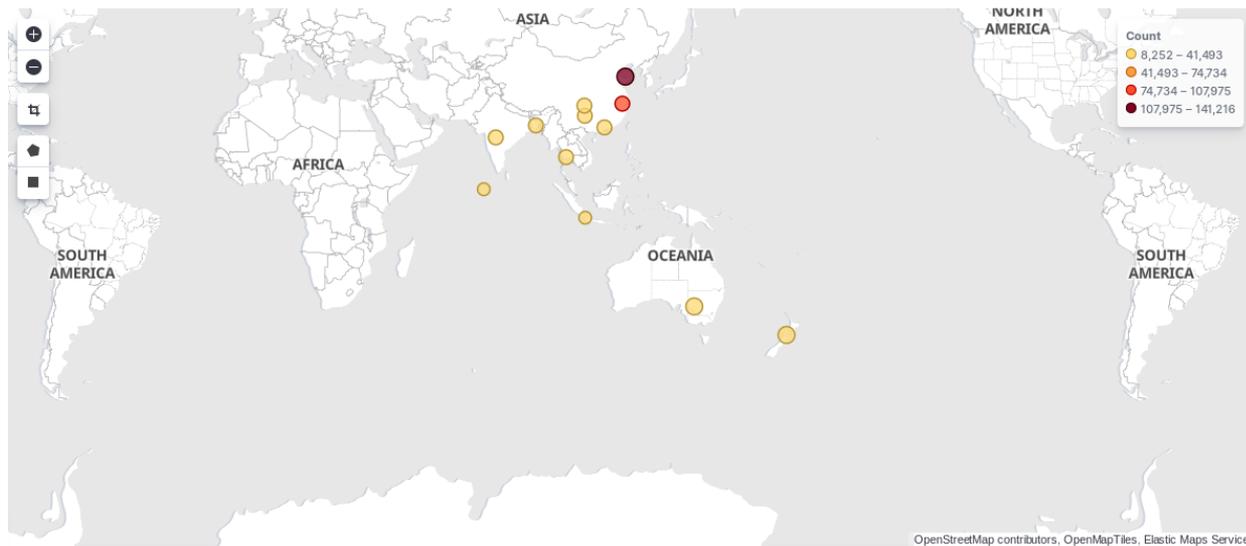
# Resultados

- 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



**CEFET/RJ**  
campus Petrópolis

