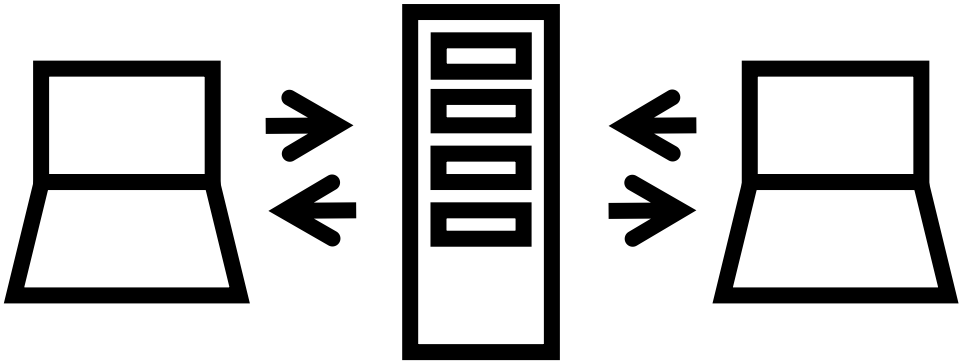
Análise de mensagens associadas à cibersegurança em redes IRC

Gabriel Gomes de Sousa

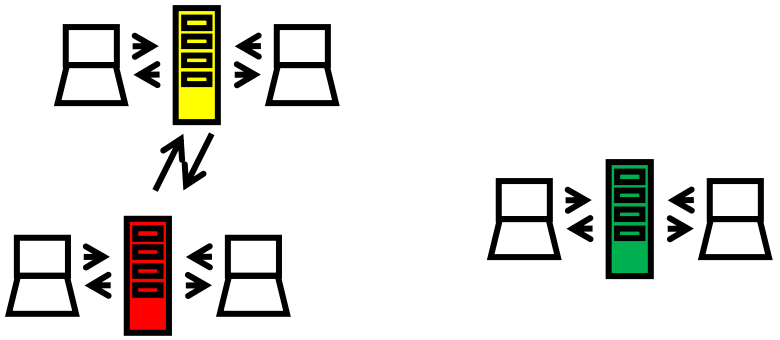
Sistema centralizado

- Todas as comunicações são intermediadas por servidores
- Todos os servidores utilizados pertencem, ou são controlados, por uma única entidade
- Exemplos:
  - Facebook
  - Google+
  - LinkedIn



Sistema descentralizado

- Os servidores que controlam a comunicação não pertencem a uma única entidade
- Cada servidor pode ter sua própria política
- Os servidores podem ou não se comunicar
- Exemplos:
  - BitTorrent
  - Jogos em LAN
  - Bitcoin



Segurança dos dados

Centralizado

- Os dados dos usuários estão concentrados em um local conhecido
- Monitoramento relativamente fácil

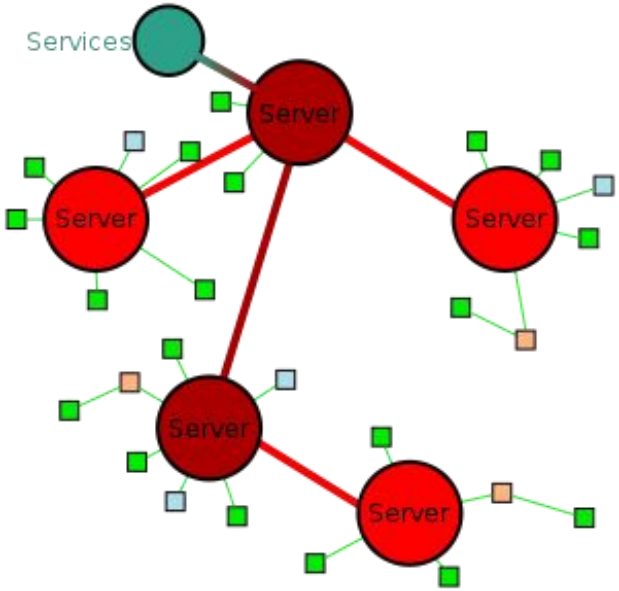
Descentralizado

- Não se sabe ao certo onde estão armazenados os dados dos usuários
- Monitoramento dificultado por causa da descentralização dos dados

IRC - Internet Relay Chat

- Protocolo de troca de mensagens de texto
- Utilizado principalmente como forma de comunicação em grupo
- Pode ser utilizado para transferência de arquivos
- Permite um certo nível de anonimato
- É um protocolo livre e qualquer um pode criar um servidor

IRC - Internet Relay Chat



IRC - Internet Relay Chat

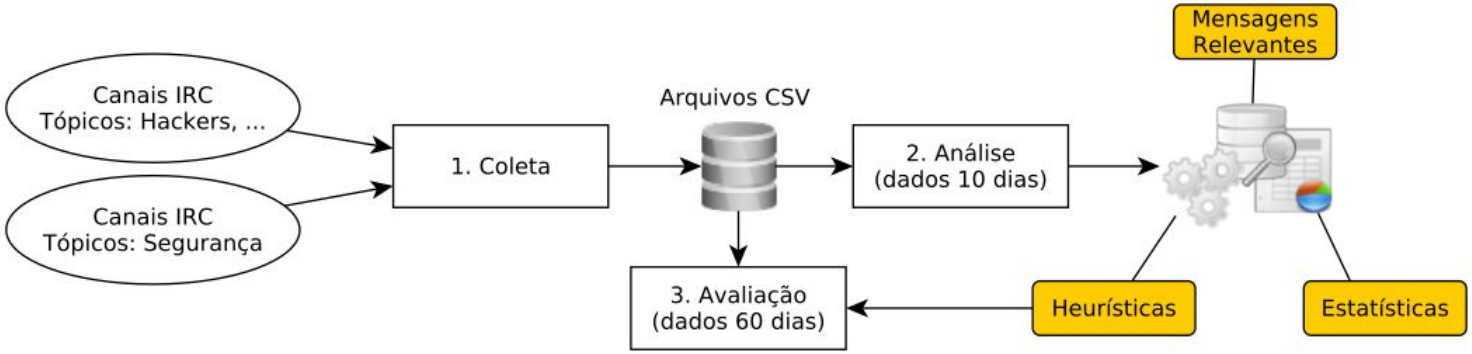
- Pode ser utilizada como meio de comunicação anônima, o que permite seu uso em atividades ilegais
- Pode ser utilizado como meio para enviar comandos à outras maquinas (bots)
- Trasferênferencia de arquivos maliciosos
- Orquestração de ataques e troca de informações sobre vulnerabilidades

Monitoramento

- Volume de mensagens
- Multiplos canais
- Mensagens irrelevantes
- Girias, erros de ortografia ...

Classificação de mensagens suspeitas

- Coleta de dados
- Analise dos dados
- Avaliação dos resultados



Coleta de dados

- Canais mais populares e tópicos mais relevantes
- O software de coleta não pode ser identificado
- Períodos longos

Análise dos dados

- A analize foi feita sobre os dados coletados em 10 dias
- Normalizar
- Estatisticas
- Identificação de mensagens relevantes

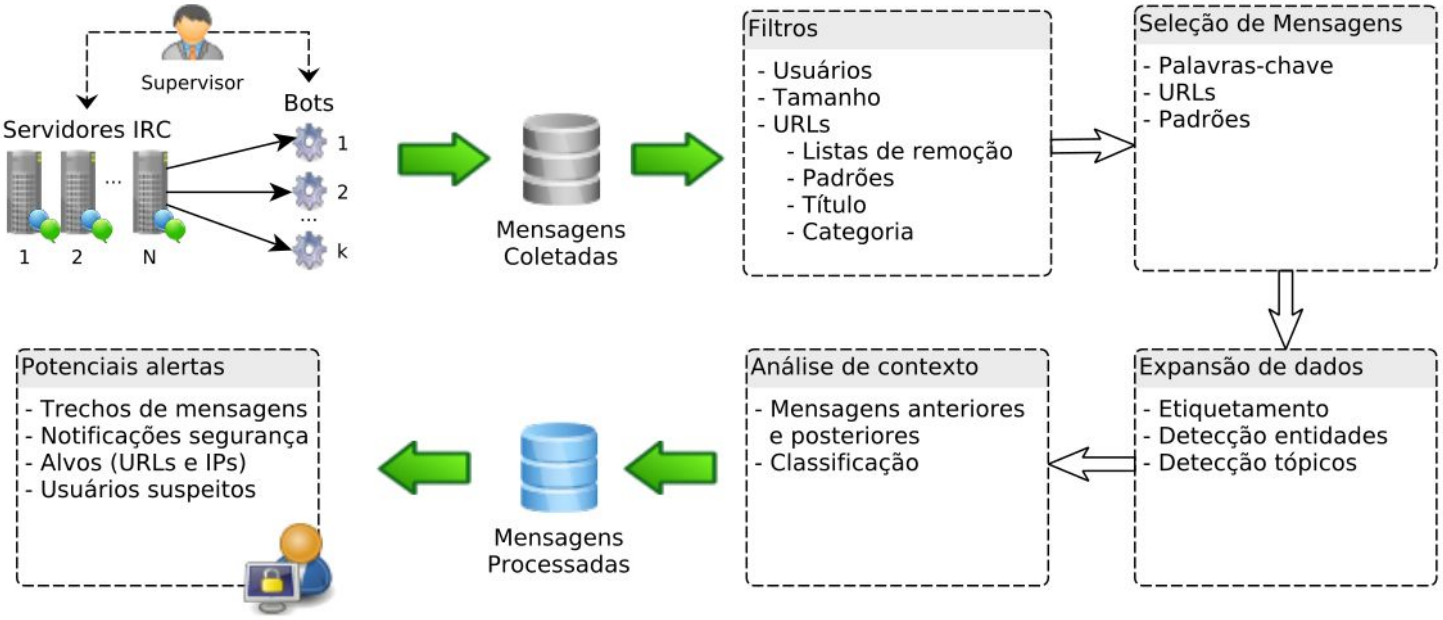
Análise dos dados

- Análise estatística
- Análise de frequência de palavras
- Mineração de associação de palavras
- Análise de URLs
- Análise de extração de tópicos e entidades
- Análise de correlação com outras fontes

Avaliação

- Aplicar os mecanismos de classificação sobre os dados coletados em 60 dias

Modelo de classificação



Coclusão

- É possível obter informações relevantes sobre ataques
- Os mecanismos de classificação apresentaram resultados variados e que depende do tópico avaliado