MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA
INSTITUTO MILITAR DE ENGENHARIA
ENGENHARIA DE COMPUTAÇÃO - SE/8

Jonas Rocha Lima Amaro, Yago Guimarães Coimbra

Ferramenta para detecção de padrões de botnet baseado em algoritmos de agrupamento de aprendizagem de máquina

Rio de Janeiro
1 de maio de 2016

Jonas Rocha Lima Amaro, Yago Guimarães Coimbra

Ferramenta para detecção de padrões de botnet baseado em algoritmos de agrupamento de aprendizagem de máquina

Trabalho Apresentado ao Curso de Engenharia de Computação do Instituto Militar de Engenharia como Verificação Especial do Projeto de Fim de Curso.

Instituto Militar de Engenharia

Orientador: Sergio dos Santos Cardoso Silva

Rio de Janeiro

1 de maio de 2016

Instituto Militar de Engenharia
Praça General Tibúrcio, 80 - Praia Vermelha
Rio de Janeiro - RJ CEP: 22290-270

Amaro, Jonas e Guimarães, Yago
S586d Ferramenta para detecção de padrões de botnet baseado em algoritmos de agrupamento de aprendizagem de máquina / Jonas Rocha Lima Amaro, Yago Guimarães Coimbra. - Rio de Janeiro: Instituto Militar de Engenharia, 2016.

??f. : il., graf., tab. : -cm.

Projeto de Fim de Curso - Instituto Militar de Engenharia
Orientador: Sergio dos Santos Cardoso Silva.

1 - Botnets 2 - Clustering

CDU 631.317.35

Jonas Rocha Lima Amaro, Yago Guimarães Coimbra

Ferramenta para detecção de padrões de botnet baseado em algoritmos de agrupamento de aprendizagem de máquina

Trabalho Apresentado ao Curso de Engenharia de Computação do Instituto Militar de Engenharia como Verificação Especial do Projeto de Fim de Curso.

Trabalho aprovado. Rio de Janeiro, 1 de maio de 2016:

Prof. Sergio dos Santos Cardoso Silva
Orientador, D. Sc., do IME

Profa. Raquel Coelho Gomes Pinto
Convidada, D. Sc., do IME

Prof. Julio Cesar Duarte
Convidado, D. Sc., do IME

Rio de Janeiro

1 de maio de 2016

Resumo

Resumo em pt

Palavras-chave: botnets, clustering.

Abstract

Abstract in English

Keywords: botnets, clustering.

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

Fig.	Figura

Lista de símbolos

Γ	Letra grega Gamas

Sumário

1 Introdução

1.1 Objetivo

1.2 Motivação

1.3 Justificativa

1.4 Metodologia

1.5 Estrutura

2 Botnets

As botnets ....

3 Cronograma

Embora o objetivo do trabalho seja o desenvolvimento de um projeto e não pesquisa, foi preciso começar por um intenso estudo do problema que queríamos resolver, ou seja das botnets. Isso é uma etapa importante de um projeto de aprendizagem de máquina, pois permite uma melhor identificação de quais features serão mais relevantes.

Em seguida, foi feito um estudo dos algoritmos de clustering existentes e os objetivos de cada técnica.

Após esses estudos, começa a implementação do sistema detector de botnets. A primeira etapa é desenvolver um tratamento automatizado dos dados obtidos pela coleta dos logs DNS, já que o objetivo final é de que esse tratamento seja feito diariamente. Depois serão implementados algoritmos de agrupamento que usarão os dados tratados para identificar padrões de botnets no log DNS coletado. Por fim, os resultados dessas técnicas serão testados e analisados e servirão de motivação para possíveis refinamentos nos algoritmos.

Durante essas tarefas, desenvolveremos também os relatórios e apresentações para as seguintes avaliações:

- Verificação Especial em Maio,
- Verificação Corrente em Julho,
- Verificação Final em Setembro.

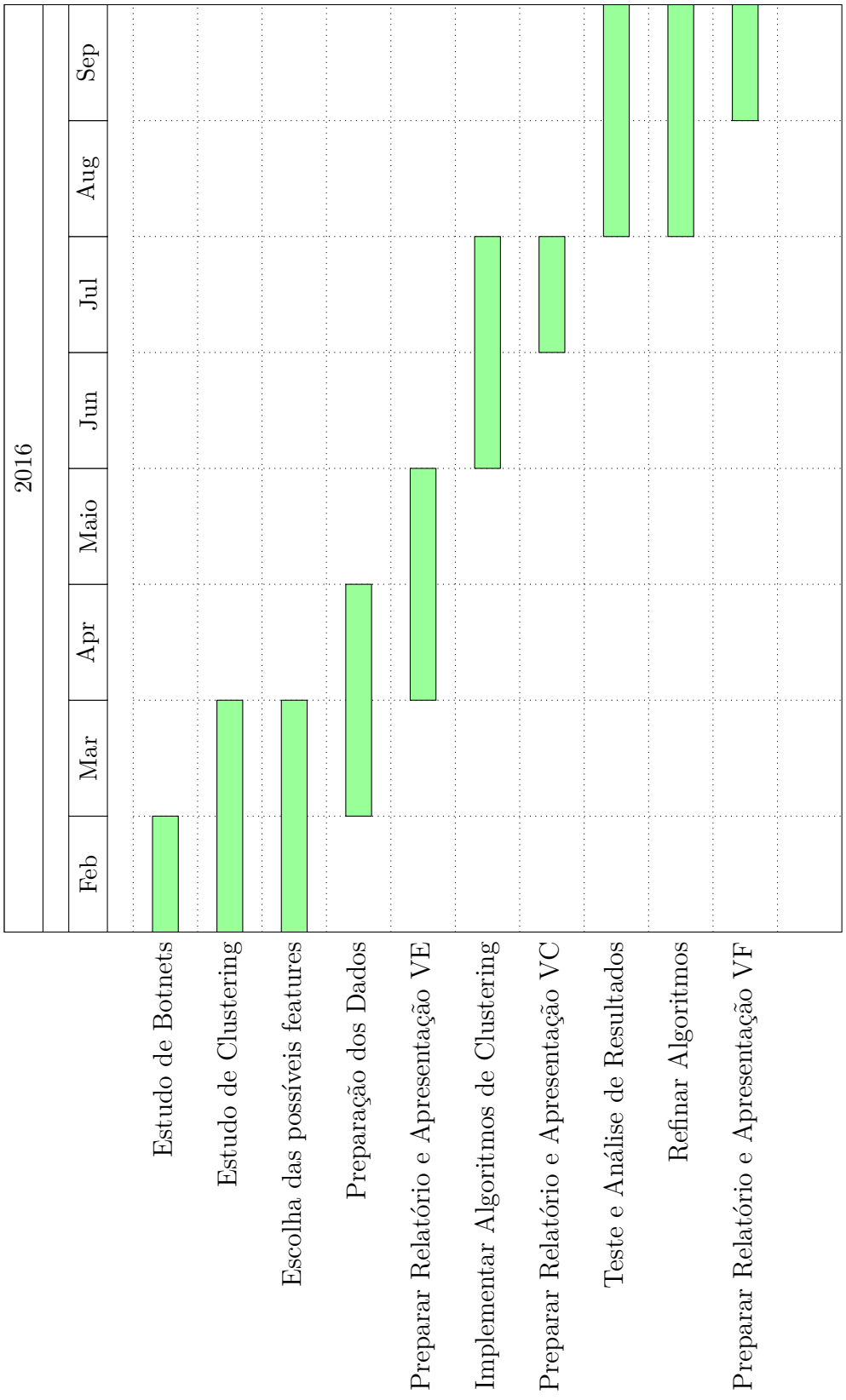

Figura 1 – Cronograma

4 Conclusão

Texto Conclusão

Referências

1 GU, G. et al. Botminer: Clustering analysis of network traffic for protocol-and structure-independent botnet detection. In: *USENIX Security Symposium*. [S.l.: s.n.], 2008. v. 5, n. 2, p. 139–154.