Avaliando o impacto de ataques simultâneos ao sistema de gerenciamento de *Cloud Computing* com árvore de ataque

Ronierison de Souza Maciel
Orientador: Prof. Dr. Paulo Romero Martins Maciel

rsm4@cin.ufpe.br
http://cin.ufpe.br/~rsm4/

Universidade Federal de Pernambuco - UFPE
Centro de Informática - CIn

Agenda

1. Introdução
   - Introdução
   - Objetivos
2. Metodologia
   - Metodologia: Visão Geral
3. (Alguns) Modelos propostos
   - Avaliação dos cenários
   - Avaliação dos cenários
   - Avaliação dos cenários
   - Avaliação dos cenários

MoDCS Group

Centro de Informática UFPE

Motivação

- Um **número crescente de ataques de negação de serviço (DDoS)** em infraestruturas de nuvem com intuito ilícitos.
- Este crescimento é demonstrado pela **fragilidade das infraestruturas** de *cloud Computing*:
  - Estima-se um **crescimento de anual de 44% na taxa de ataque DDoS** (Arbor Networks, 2017).
- Com o avanço da **internet das coisas (IoT)**, há uma tendência na utilização indevida desses dispositivos conectados a rede a virem se tornar botnets.

Objetivo geral

- O propósito desta pesquisa é apresentar um **conjunto de cenários** para avaliar impactos de ações maliciosas em uma infraestrutura de **cloud computing**.

Objetivos específicos

- Propor modelos de **attack tree** para infraestrutura de **cloud computing**, considerando as **principais vulnerabilidades** que possam ocorrer em um ambiente de nuvem;
- Identificar o **impacto de diferentes tipos de ataques** que possam ocorrer em um ambiente de **cloud computing**;
- Propor **contramedidas** para mitigar ações maliciosas em uma infraestrutura de **cloud computing**.

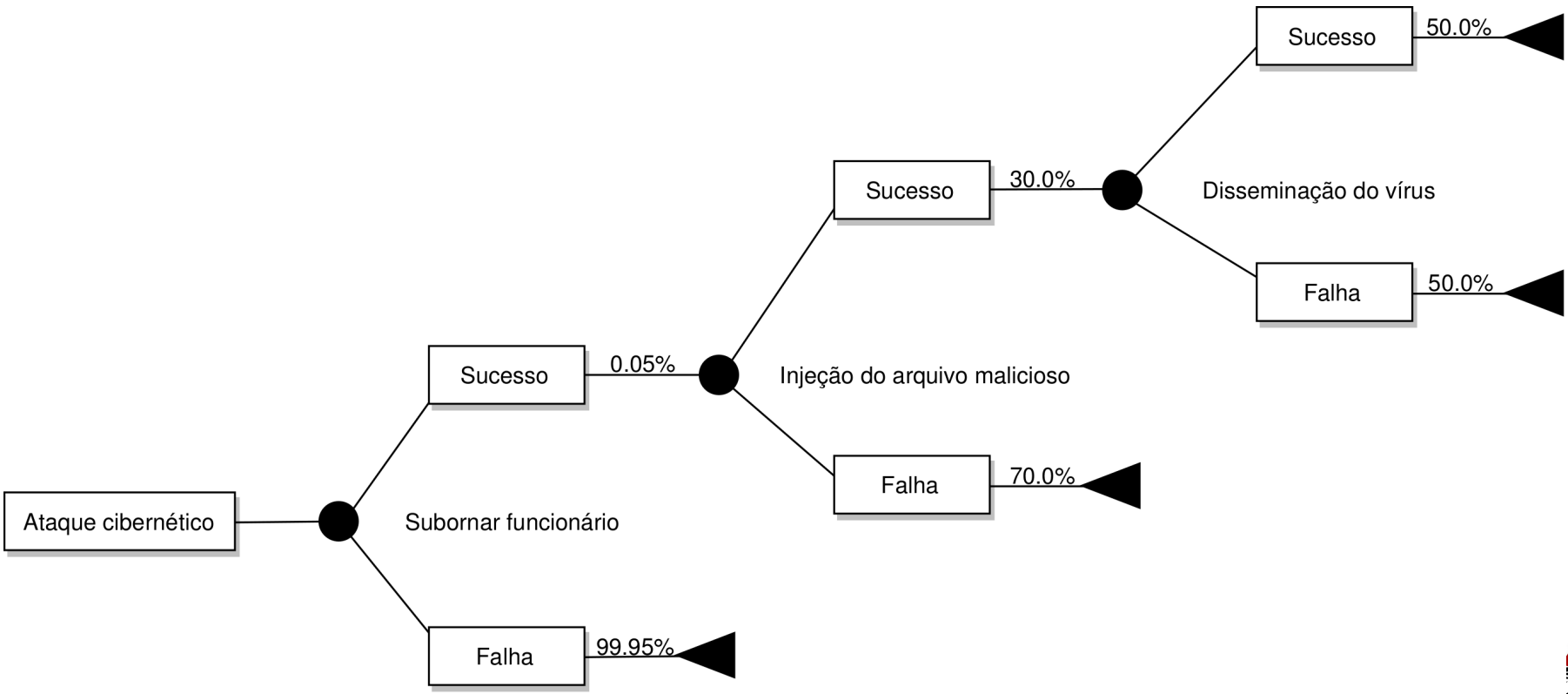
Objetivos específicos

- Propor modelos de **attack tree** para infraestrutura de **cloud computing**, considerando as **principais vulnerabilidades** que possam ocorrer em um ambiente de nuvem;
- Identificar o **impacto de diferentes tipos de ataques** que possam ocorrer em um ambiente de **cloud computing**;
- Propor **contramedidas** para mitigar ações maliciosas em uma infraestrutura de **cloud computing**.

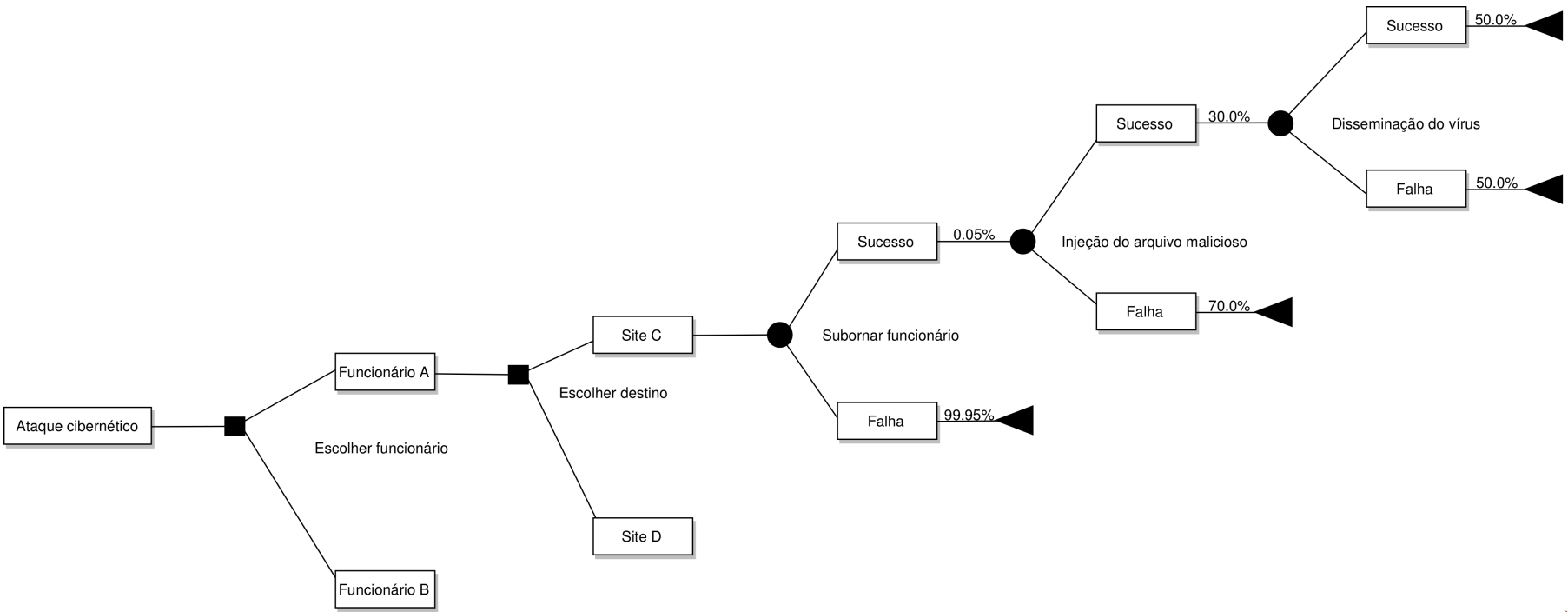
Objetivos específicos

- Propor modelos de **attack tree** para infraestrutura de **cloud computing**, considerando as **principais vulnerabilidades** que possam ocorrer em um ambiente de nuvem;
- Identificar o **impacto de diferentes tipos de ataques** que possam ocorrer em um ambiente de **cloud computing**;
- Propor **contramedidas** para mitigar ações maliciosas em uma infraestrutura de **cloud computing**.

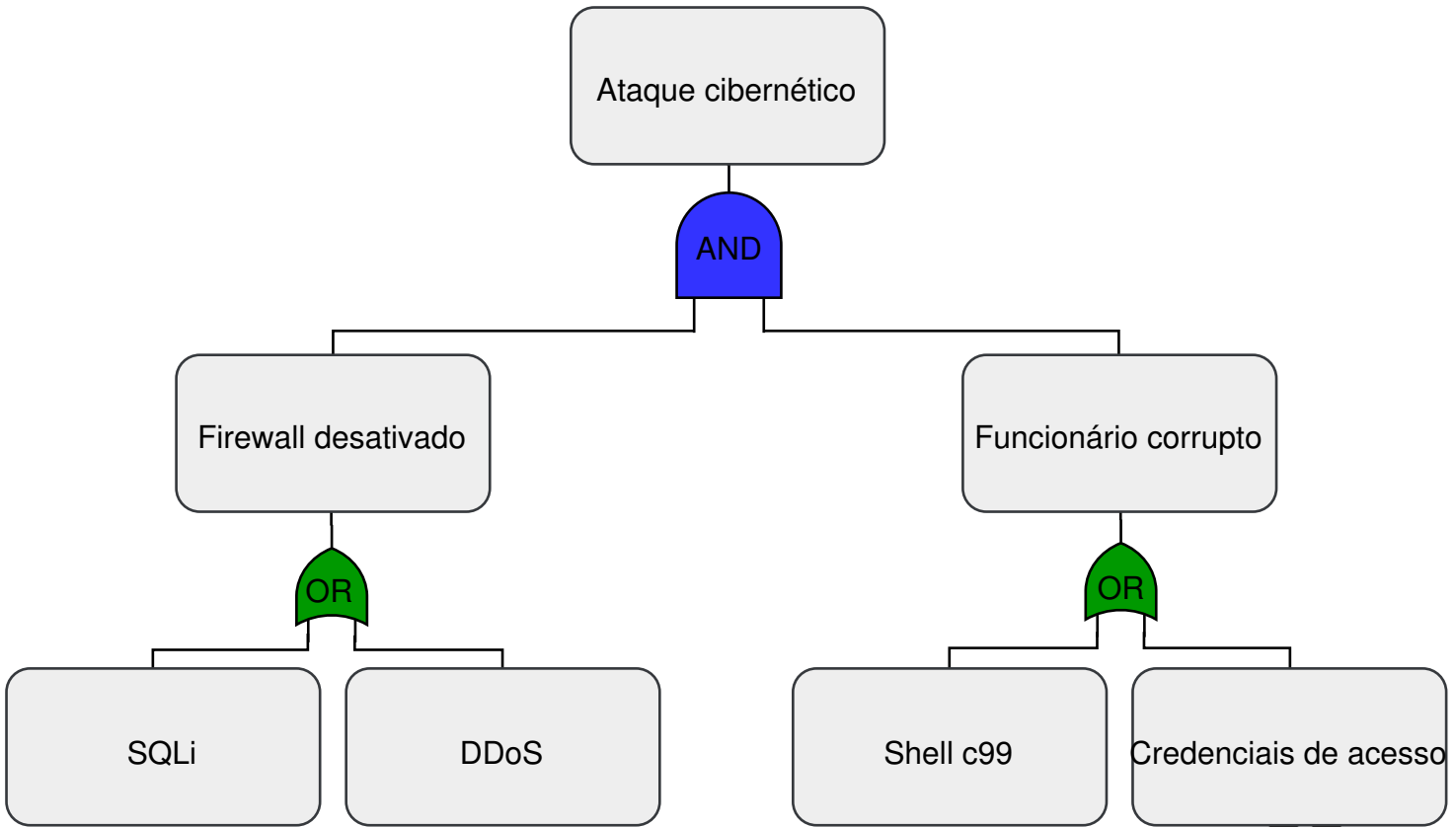
Árvore de probabilidade



Árvore de decisão

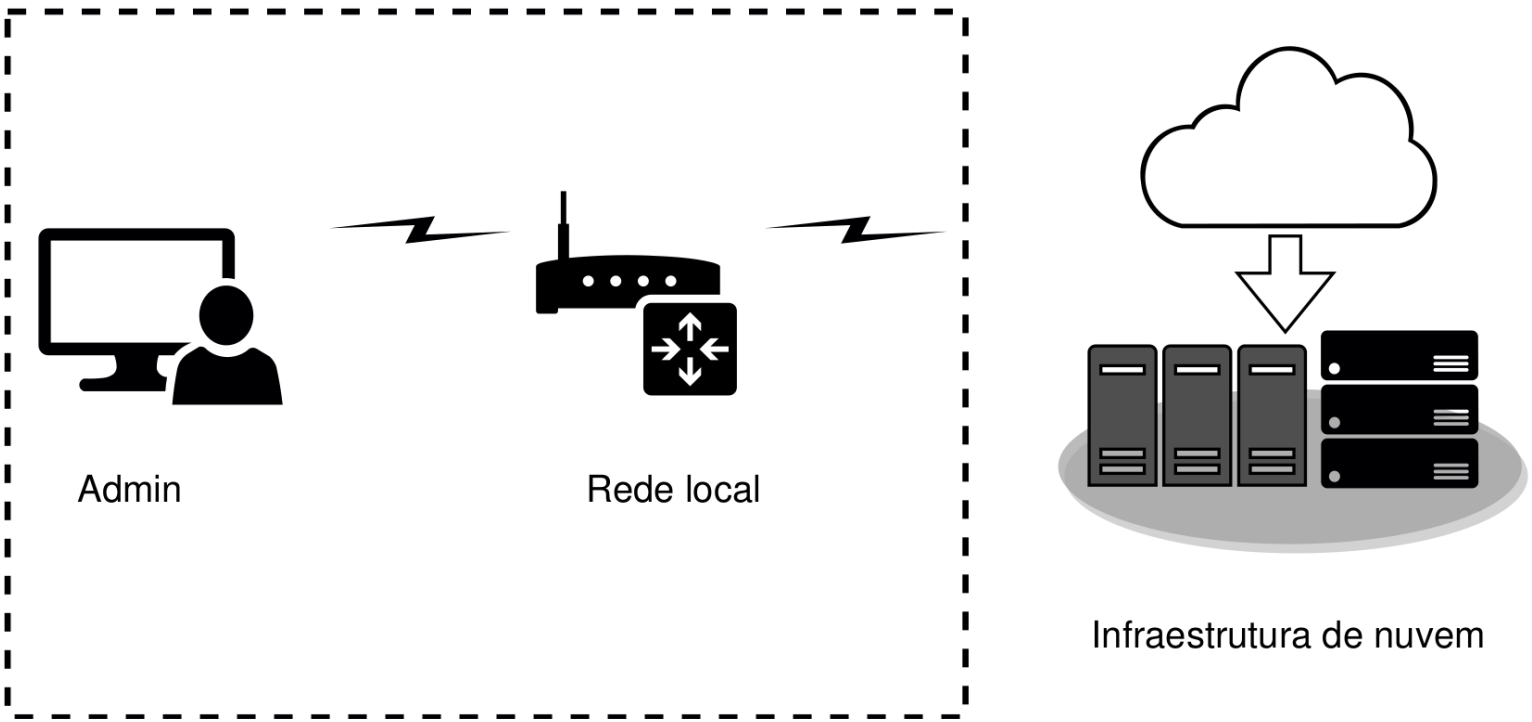


Metodologia: Visão Geral



MoDCS Group

Arquitetura de acesso



Cenários de conectividade

(a) Cenário #1

(b) Cenário #2

Métricas da árvore de ataque

$$\prod_{i=1}^{n} prob_i \tag{1}$$

$$1 - \prod_{i=1}^{n} (1 - prob_i) \tag{2}$$

onde, o produtório 1 é a probabilidade de ataque pela porta **and**. O produtório 2 representa a probabilidade de ataque pela porta **or** utilizando a árvore de ataque.

Métricas da árvore de ataque

$$\sum_{i=1}^{n} cost_i \tag{3}$$

$$\frac{\sum_{i=1}^{n} prob_i \times cost_i}{\sum_{i=1}^{n} prob_i} \tag{4}$$

onde, o somatório 3 é relativo ao custo do ataque pela porta **and**. O somatório 4 representa o custo do ataque pela porta **or** utilizando a árvore de ataque.

Métricas da árvore de ataque

$$\frac{10_n - \prod_{i=1}^{n}(10 - impact_i)}{10^{(n-1)}} \tag{5}$$

$$\mathbf{Max_{i=1}^{n} impact_i} \tag{6}$$

onde, o 5 refere-se ao impacto do ataque pela porta **and**. O 6 é relativo ao impacto do ataque pela porta **or** utilizando a árvore de ataque.

Modelo

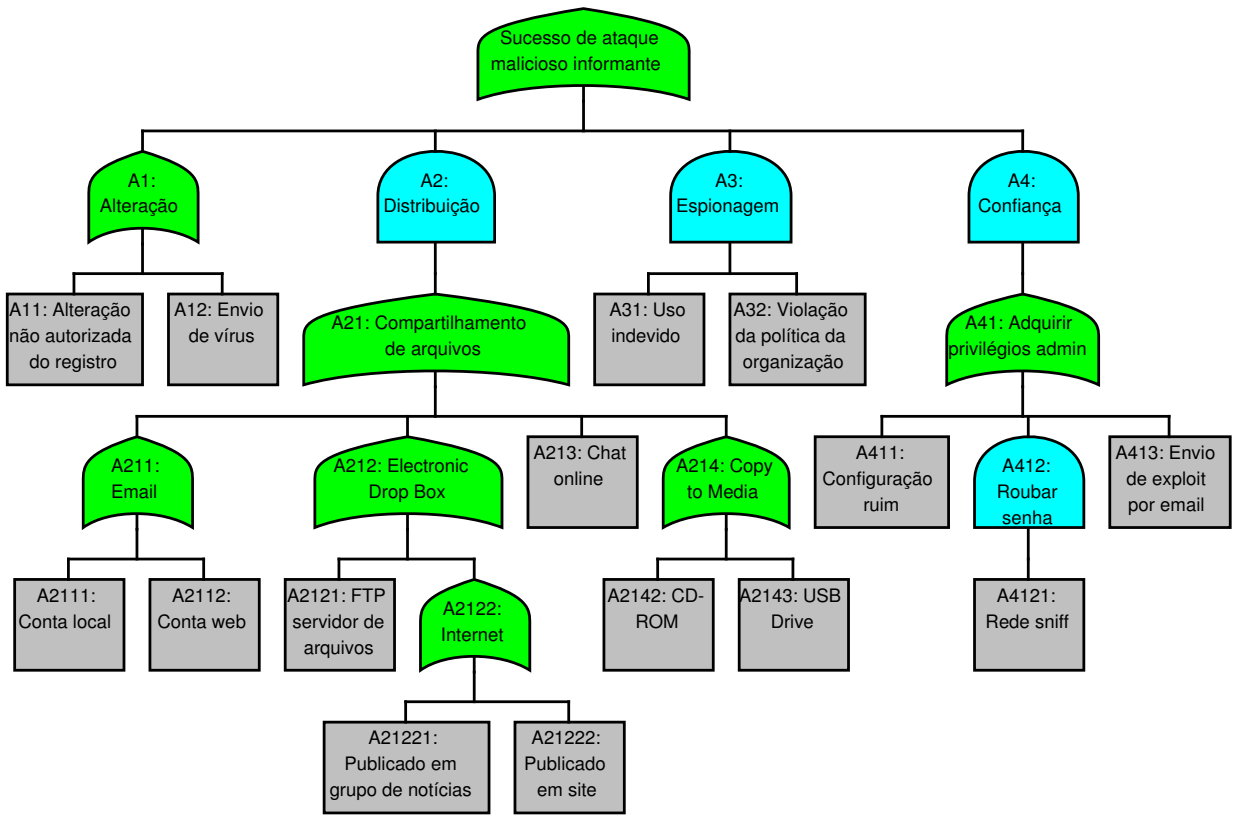


Figure: Attack Tree base

MoDCS Group
Centro de Informática UFPE

Modelo

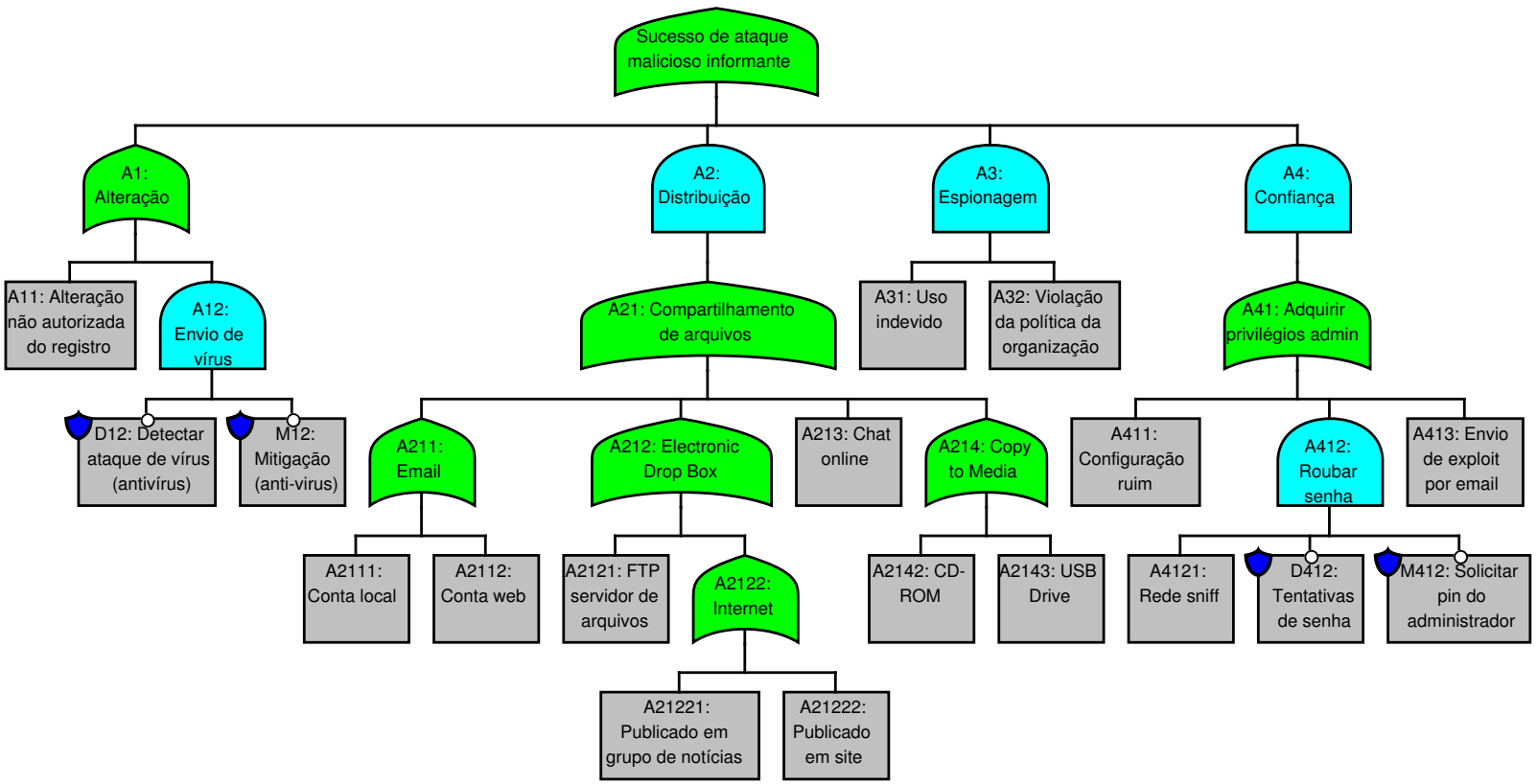


Figure: Attack Tree de contramedida

Modelo

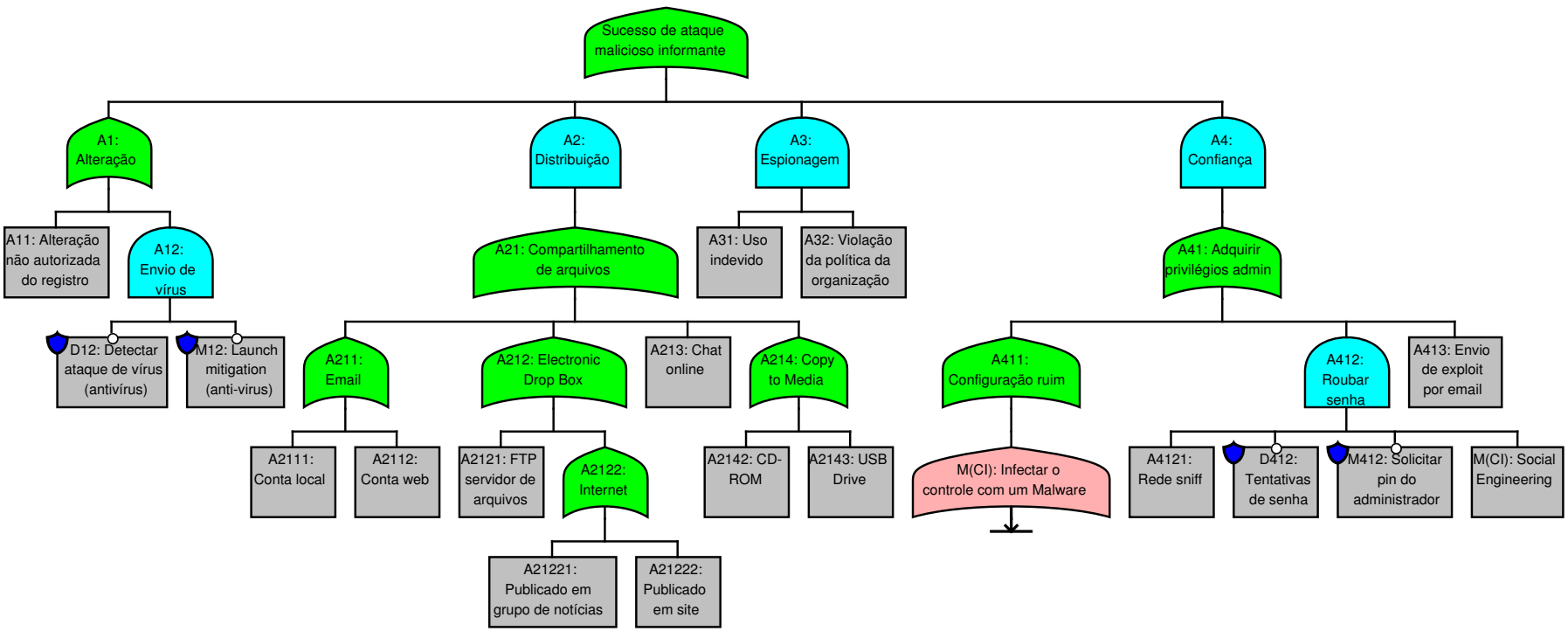


Figure: Attack Tree de adição

Dúvidas?