Avaliação de algoritmos de machine learning para detecção de malware IoT no dataset IoT-23

Cristian H. M. Souza

Carlos H. Arima

Agenda

- Introdução
- Metodologia
- Implementação e resultados
- Conclusão e trabalhos futuros

Introdução

Introdução

- Malwares continuam sendo um dos principais desafios à segurança dos sistemas computacionais.

- O advento do paradigma IoT foi acompanhado pelo aumento do número de programas maliciosos com foco nas arquiteturas ARM e MIPS.

- Soluções a nível de rede que utilizam machine learning têm se mostrado efetivas na detecção e mitigação de malwares.

Introdução

- Este trabalho propõe uma avaliação de algoritmos de machine learning para classificação de malware IoT com base no dataset IoT-23.

- O objetivo principal é auxiliar pesquisadores de segurança na escolha e implementação de modelos para detecção de artefatos maliciosos em tais ambientes.

- Foram implementados os algoritmos de Random Forest, SVM e uma árvore de decisão, além de uma rede neural convolucional.

- Os modelos são comparados com base nas métricas de acurácia, precisão, recall e F1-Score.

Metodologia

Metodologia

- O dataset utilizado para treinamento dos modelos propostos neste estudo é o IoT-23, criado pelo Avast AIC Laboratory.

- Esta base contém 20 capturas de malwares coletadas de diversos dispositivos IoT, além de 3 capturas de tráfego benigno.

- Seu objetivo é fornecer aos pesquisadores um grande conjunto de dados reais e rotulados de infecções e tráfego legítimo, visando auxiliar o desenvolvimento de algoritmos de machine learning.

Metodologia

- Em números totais, o dataset possui 325.307.990 registros, sendo 294.449.255 deles maliciosos.

Tipo de ameaça	**Descrição**
Attack	Anomalias que não puderam ser identificadas e classificadas.
Benign	Tráfego benigno.
C&C	Tráfego gerado pela comunicação entre um dispositivo infectado e uma estação de comando e controle.
DDoS	Tráfego gerado por ataques de negação de serviço distribuídos.
FileDownload	Tráfego gerado pela transferência de arquivos maliciosos.
HeartBeat	Tráfego gerado pela estação de C&C para verificar a conexão com o alvo.
Mirai	Tráfego que possui características da *botnet* Mirai.
Okiru	Tráfego que possui características da *botnet* Okiru.
PartOfAHorizontalPortScan	Tráfego gerado por *scanners* de rede para coleta de informações.
Torii	Tráfego que possui características da *botnet* Torii.

Metodologia

Pré-processamento:

1. Remoção de colunas não importantes.
2. Label encoding.
3. Substituição de valores ausentes.
4. Feature scaling.
5. Separação do conjunto de treinamento e de teste (7:3).

Implementação e resultados

Implementação e resultados

- **CNN:** Max pooling 1D, pool_size=2 e 500 neurônios.
  - Otimizador Adam.
- **RF:** 100 árvores e random_state=0.
- **SVM:** regularização = 1 e kernel cache = 700 MB.

Algoritmo	**Acurácia**	**Precisão**	***Recall***	**F1-Score**
CNN	92.83%	0.97	0.99	0.98
Decision Tree	97.33	0.93	0.99	0.96
Random Forest	99.33%	0.97	0.99	0.98
SVM	94%	0.91	0.93	0.92

Conclusão e trabalhos futuros

Conclusão e trabalhos futuros

- Este trabalho apresenta uma avaliação de diferentes algoritmos de machine learning para a detecção de malware em dispositivos IoT, utilizando o dataset IoT-23.

- Como trabalhos futuros, pretende-se avaliar o desempenho dos algoritmos contra artefatos maliciosos não presentes no dataset IoT-23, com o objetivo de mensurar a acurácia dos modelos em cenários reais.

- Avaliar o comportamento dos modelos considerando artefatos especializados na evasão de defesas pode fornecer dados importantes para aprimorar a capacidade de detecção dos algoritmos.

Avaliação de algoritmos de machine learning para detecção de malware IoT no dataset IoT-23

Cristian H. M. Souza

Carlos H. Arima