How to Use ML to Detect Bad 🍎?

Martina Tivadar
Objective by the sea v7.0
December 2024

whoami

- Master's student
- Interested in cybersecurity and machine learning
- OBTS v6.0 student scholar
- Dog person

@xmartinaxo TivadarMartina

Overview

1. Problem and solution
2. Collection of the training data
3. Automatization
4. Data fetching
5. Preprocessing
6. Training of the models
7. Creating the web solution
8. Demo

Problem

- manual analysis is time consuming
- lots of steps
- high number of files
- complexity
- delay in response

Solution

- a web solution using machine lerarning that gives us a prediction if a file is malicious or not
- the user only need to run the file and collect the logs
- fast and efficient
- scalability
- easy to use

objective-see / **Malware**

Type / to search

Code | Issues | Pull requests | Actions | Projects | Security | Insights

Malware

Public

Watch 28 | Fork 37 | Star 316

main | 1 Branch | 0 Tags | Go to file t | Add file | Code

objective-see Update README.md — e94d300 · last week — 76 Commits

AMCleaner.zip	Update AMCleaner.zip	3 months ago
Activator.zip	uploading stage 1 and 2 of Activator stealer	3 months ago
Adwind.zip	Remaining samples	last year
AoboKeylogger (Baoba).zip	Remaining samples	last year
AppleJeus.zip	Remaining samples	last year
AtomicStealer.zip	Update AtomicStealer.zip	4 months ago
BackTrack.zip	Remaining samples	last year
BadBunny.zip	Remaining samples	last year
BeaverTail.zip	Update BeaverTail.zip	3 months ago
BirdMiner.zip	Remaining samples	last year
	Remaining samples	last year
	Update Bundlore.zip	3 months ago

About

macOS Malware Collection

- Readme
- GPL-3.0 license
- Activity
- 316 stars
- 28 watching
- 37 forks

Report repository

Releases

No releases published

Packages

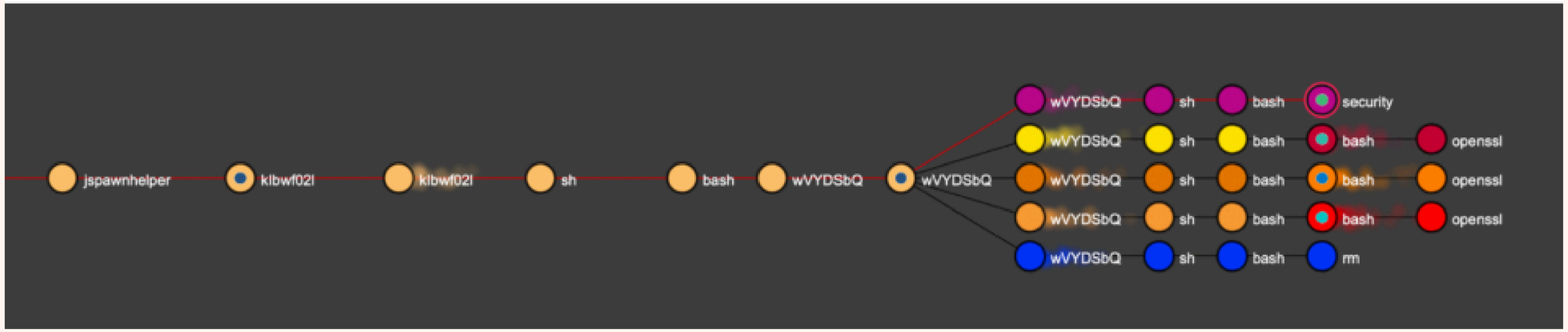
No packages published

github.com/objective-see/Malware

Data collected by Daisy Kopycienski

Atomic Stealer

XLoader



themittenmac.com/tools/

Automatization

1

fetch_data 1m 13s → preprocess_data 1m 9s → validate_data → test_data 1m 13s → split_data 1m 10s

2

train_model 2m 0s

3

deploy_to_dockerhub 2m 19s

GitHub

Data fetching

Preprocessing

encoding categorical data

removing unnecessary columns

feature engineering

handling missing values

scaling data

balancing the dataset

DagsHub

DVC

Models and experiments

TivadarMartina / ml-malware-detection

Connected to https://github.com/TivadarMartina/ml-malware-detection.git - 5 hours ago

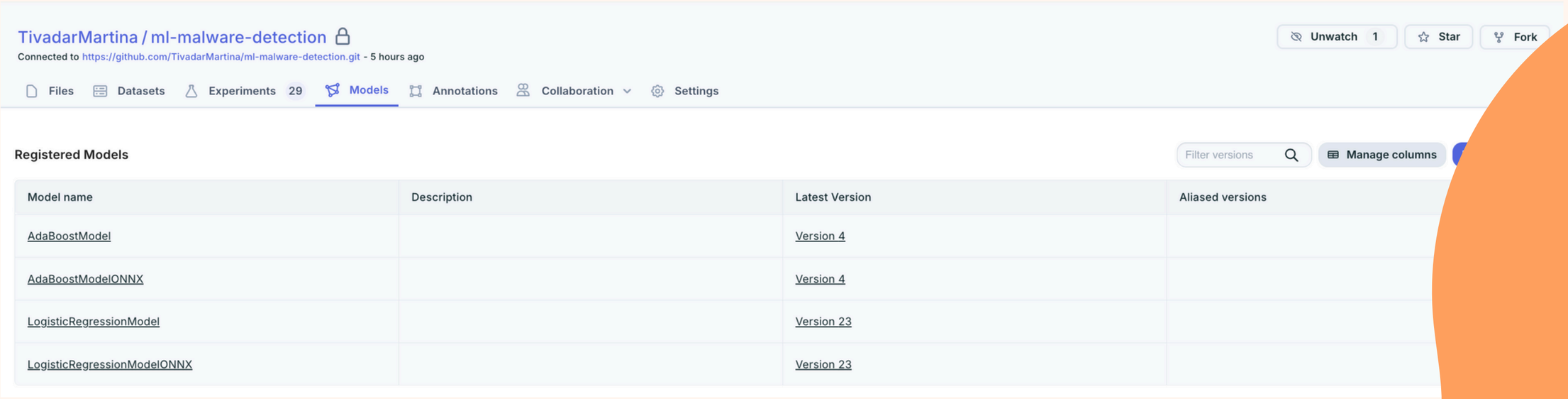
Files | Datasets | Experiments 29 | Models | Annotations | Collaboration | Settings

Compare | Reset filters | Delete | Archive | Labels | Columns | 29/100 EXPERIMENTS | + Log experiment

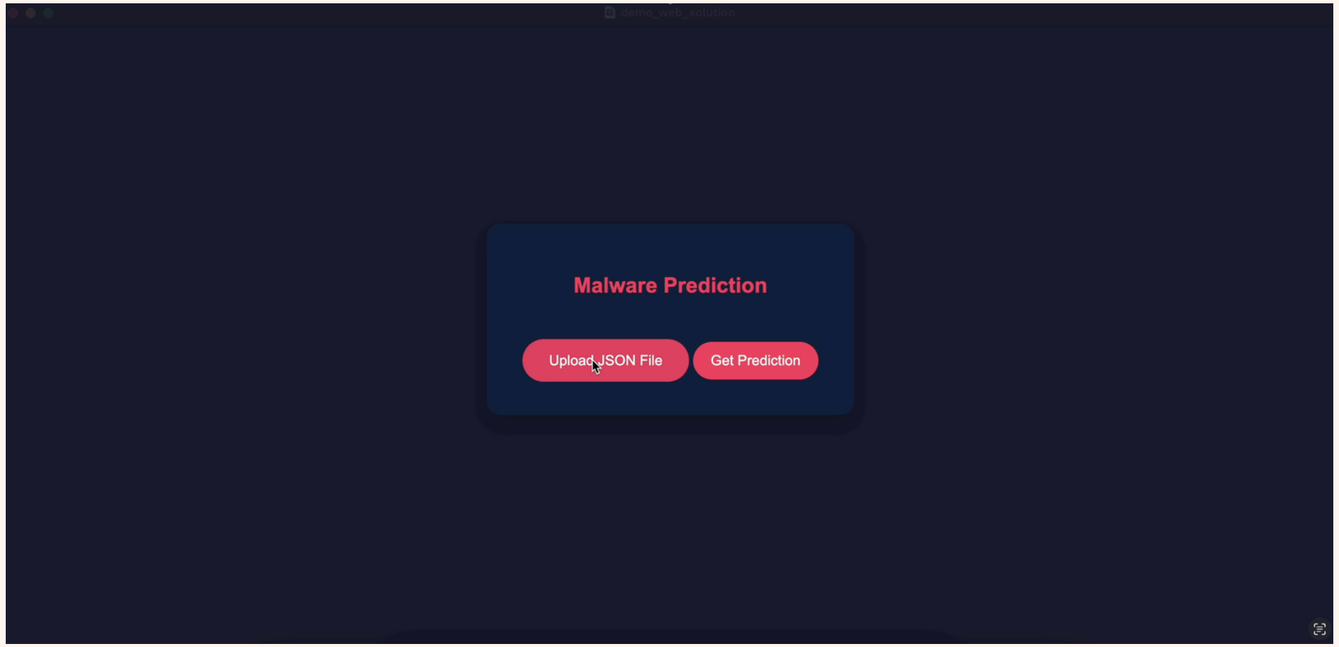
Code	Name	Commit	Created ↓	Labels	Sou...	test_accuracy	test_f1	test_precision	test_recall	train_accura...
	Multiclass Clas...	2e92	3 months ago		mlflow	0.9905660377...	0.9906092528...	0.9908608490...	0.9905660377...	1
	Binary Classifi...	2e92	3 months ago		mlflow	0.9811320754...	0.9810842220...	0.9817506959...	0.9811320754...	0.9727463312...
	nimble-mink-6...	2e92	3 months ago		mlflow					
	Multiclass Clas...	656b	3 months ago		mlflow	0.9905660377...	0.9906092528...	0.9908608490...	0.9905660377...	1
	Binary Classifi...	656b	3 months ago		mlflow	0.9811320754...	0.9810842220...	0.9817506959...	0.9811320754...	0.9727463312...
	peaceful-fox-7...	656b	3 months ago		mlflow					
	Multiclass Clas...	6954	3 months ago		mlflow	0.9905660377...	0.9906092528...	0.9908608490...	0.9905660377...	1
	Binary Classifi...	6954	3 months ago		mlflow	0.9811320754...	0.9810842220...	0.9817506959...	0.9811320754...	0.9727463312...
	Binary Classifi...	089d	3 months ago		mlflow	0.9811320754...	0.9810842220...	0.9817506959...	0.9811320754...	0.9727463312...
	Binary Classifi...	152a	3 months ago		mlflow	0.9811320754...	0.9810842220...	0.9817506959...	0.9811320754...	0.9727463312...
	Multiclass Clas...	60b2	3 months ago		mlflow	1	1	1	1	1
	Binary Classifi...	60b2	3 months ago		mlflow	0.9811320754...	0.9810842220...	0.9817506959...	0.9811320754...	0.9727463312...
	Binary Classifi...	e603	3 months ago		mlflow	0.9811320754...	0.9782608695...	1	0.9574468085...	0.9727463312...
	Binary Classifi...	c2b7	3 months ago		mlflow	0.9056603773...	0.9122807017...	0.9285714285...	0.8965517241...	0.9716981132...
	Binary Classifi...	ff28	3 months ago		mlflow	0.9056603773...	0.9122807017...	0.9285714285...	0.8965517241...	0.9716981132...
	Binary Classifi...	d751	3 months ago		mlflow	0.9855072463...	0.9859154929...	1	0.9722222222...	0.9710144927...
	Binary Classifi...	ec58	3 months ago		mlflow	0.9855072463...	0.9859154929...	1	0.9722222222...	0.9710144927...
	Binary Classifi...	283d	3 months ago		mlflow	0.9855072463...	0.9859154929...	1	0.9722222222...	0.9710144927...
	Binary Classifi...	a676	3 months ago		mlflow	0.9871794871...	0.9756097560...	0.9756097560...	0.9756097560...	0.9822569198...
	Binary Classifi...	a3ee	3 months ago		mlflow	0.9871794871...	0.9756097560...	0.9756097560...	0.9756097560...	0.9822569198...

mlflow™

Registered models



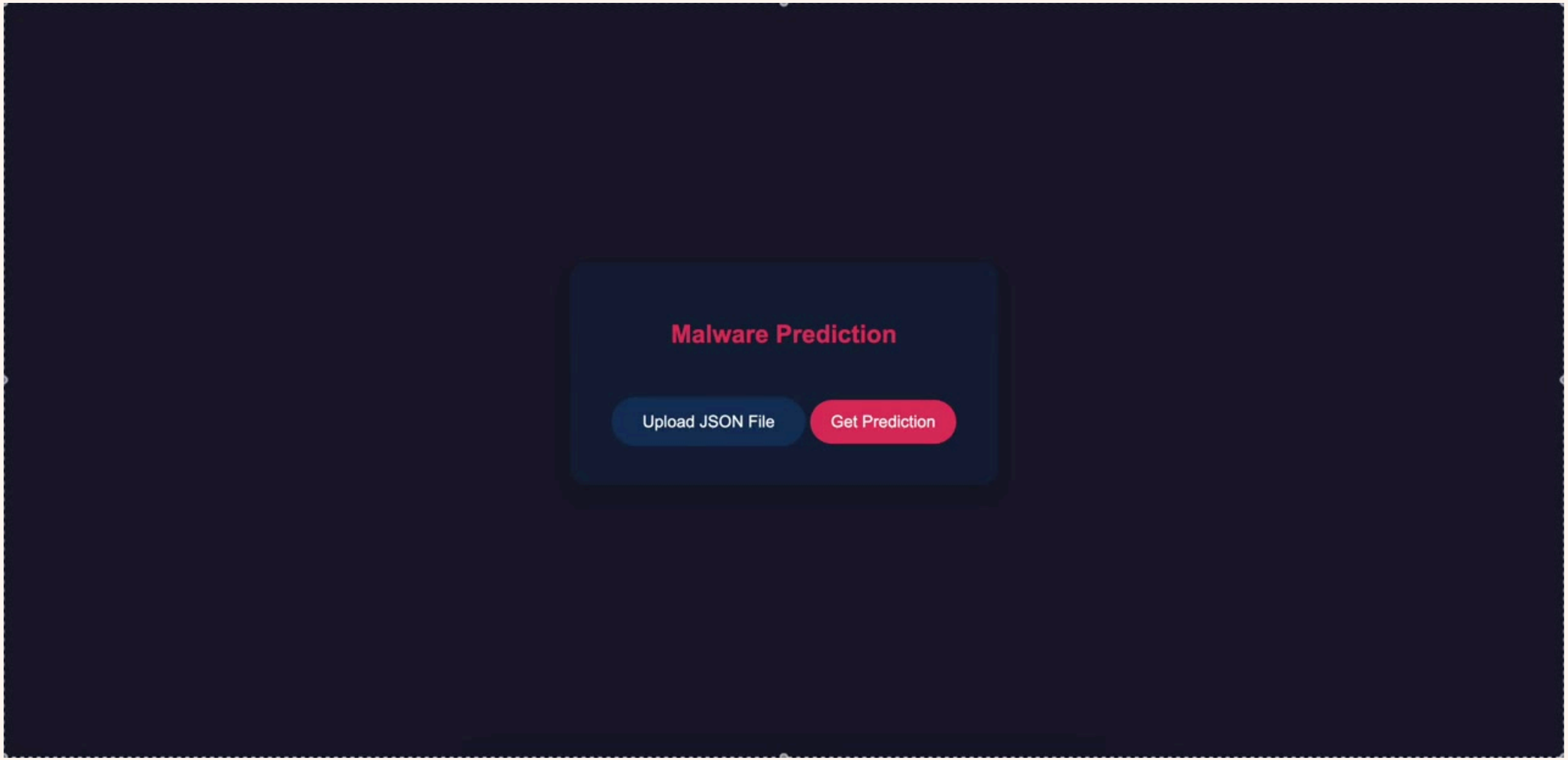
Web solution



Flask
web development,
one drop at a time

Render

Demo



Not!

Possible improvements

- automatization of log the collection
- the prediction process on Render is slow

TivadarMartina

Q&A

LinkedIn

@xmartinaxo

TivadarMartina