Università degli Studi di Padova

Decoding GAN-Generated Malware using Explainable AI Techniques

Corso di Laurea in Informatica

Tiozzo Matteo

Padova - 10/12/2024

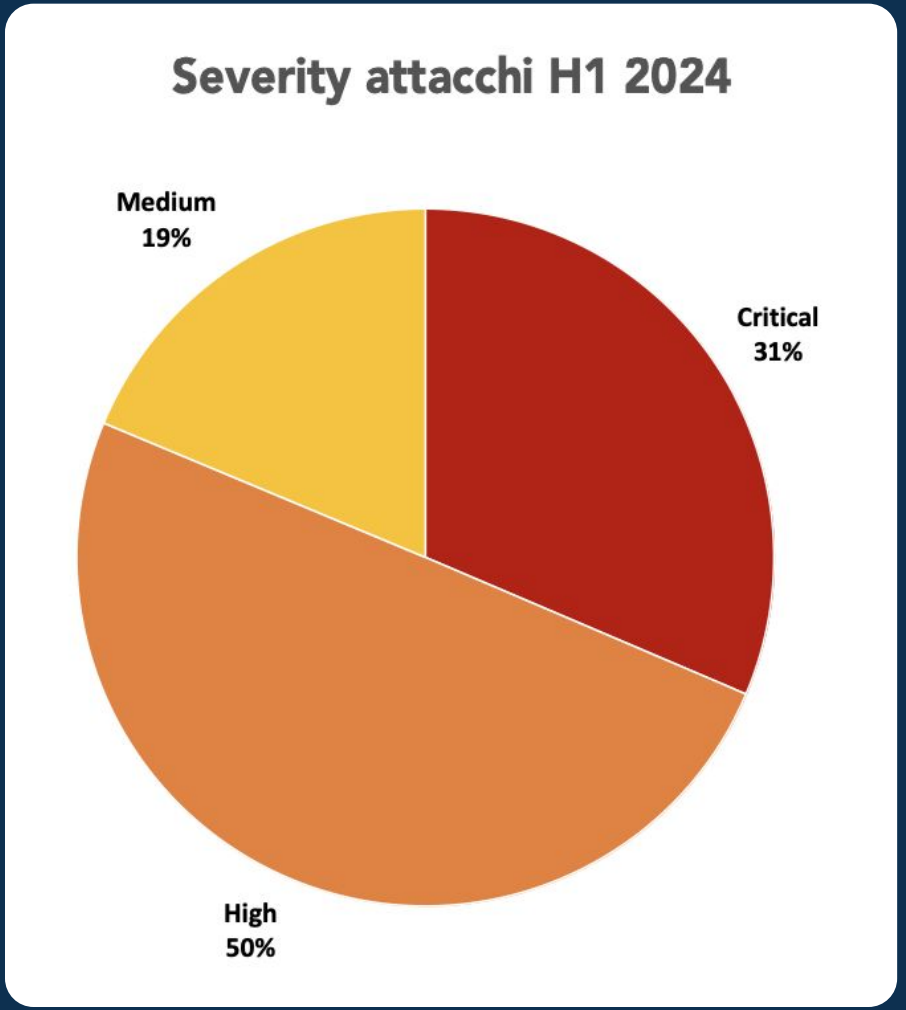
INDICE

MOTIVAZIONE

- Passione per la sicurezza informatica e l’intelligenza artificiale
- Crescente numero di attacchi negli ultimi anni
- Migliorare la difesa informatica con nuove tecnologie

ANALISI DEI DATI

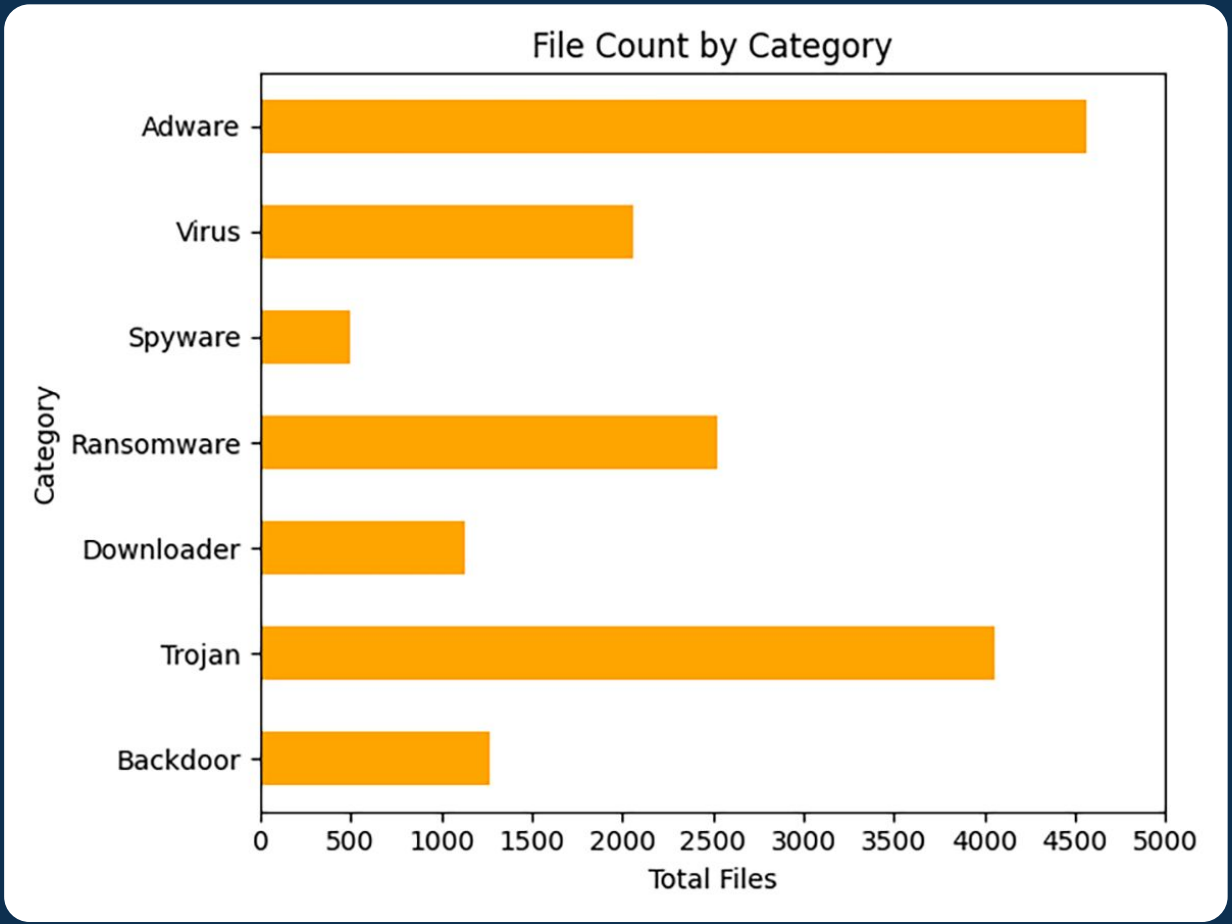
- **+23%** è la crescita degli incidenti dal *II* semestre 2023 al *I* semestre 2024
- **2x** è l'aumento della media mensile degli incidenti a livello mondiale rispetto al *I* semestre 2019
- **81%** è la percentuale di severità degli attacchi compresa tra "critica" e "alta"



Fonte: report Clusit giugno 2024

MALWARE

Cos’è, tipologie trattate e raccolta dati



Malware:

software dannoso che infiltra, danneggia o accede illegalmente a sistemi informatici.

Numero totale di malware Windows:

- 16114

MALWARE VISUALIZATION

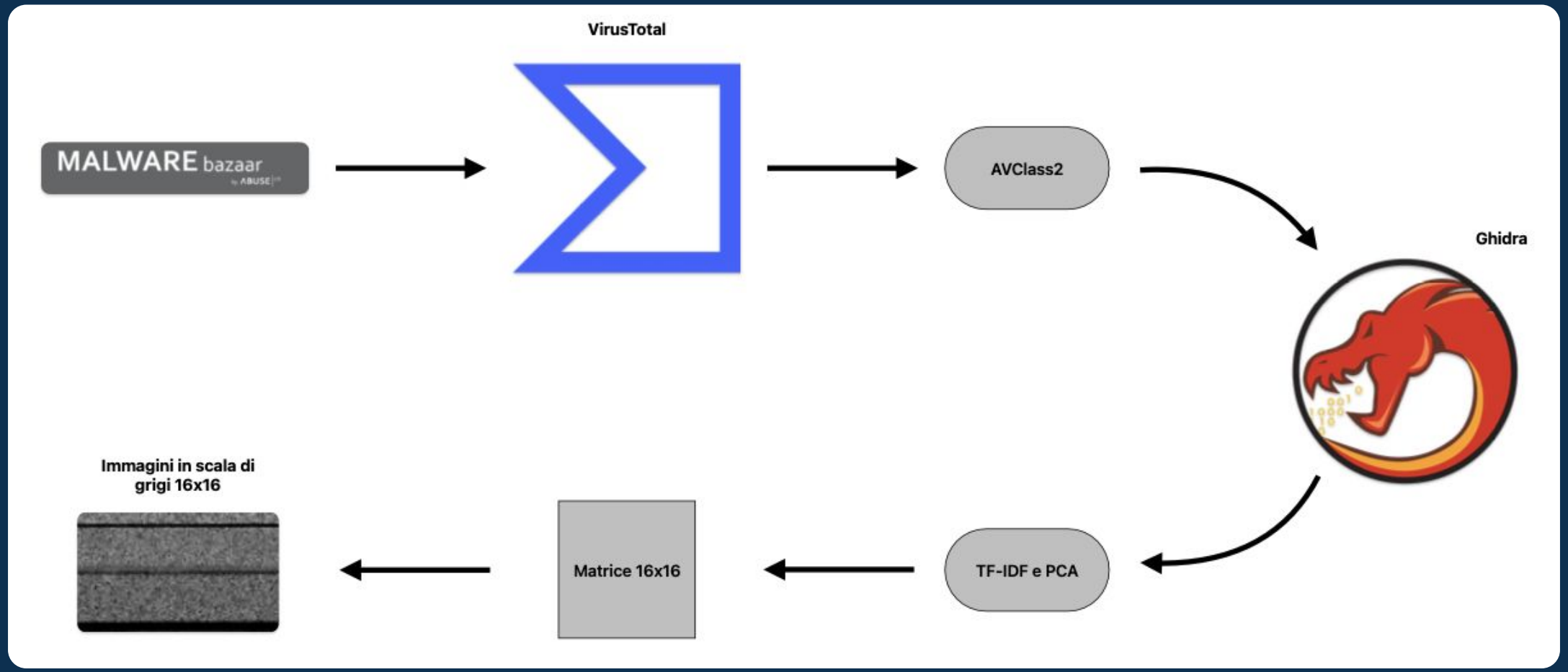
Perché?

- Performance **ottimali**
- Aperto a tecniche di ***explainability***
- **Indipendente** dal tipo di malware analizzato

Trojan

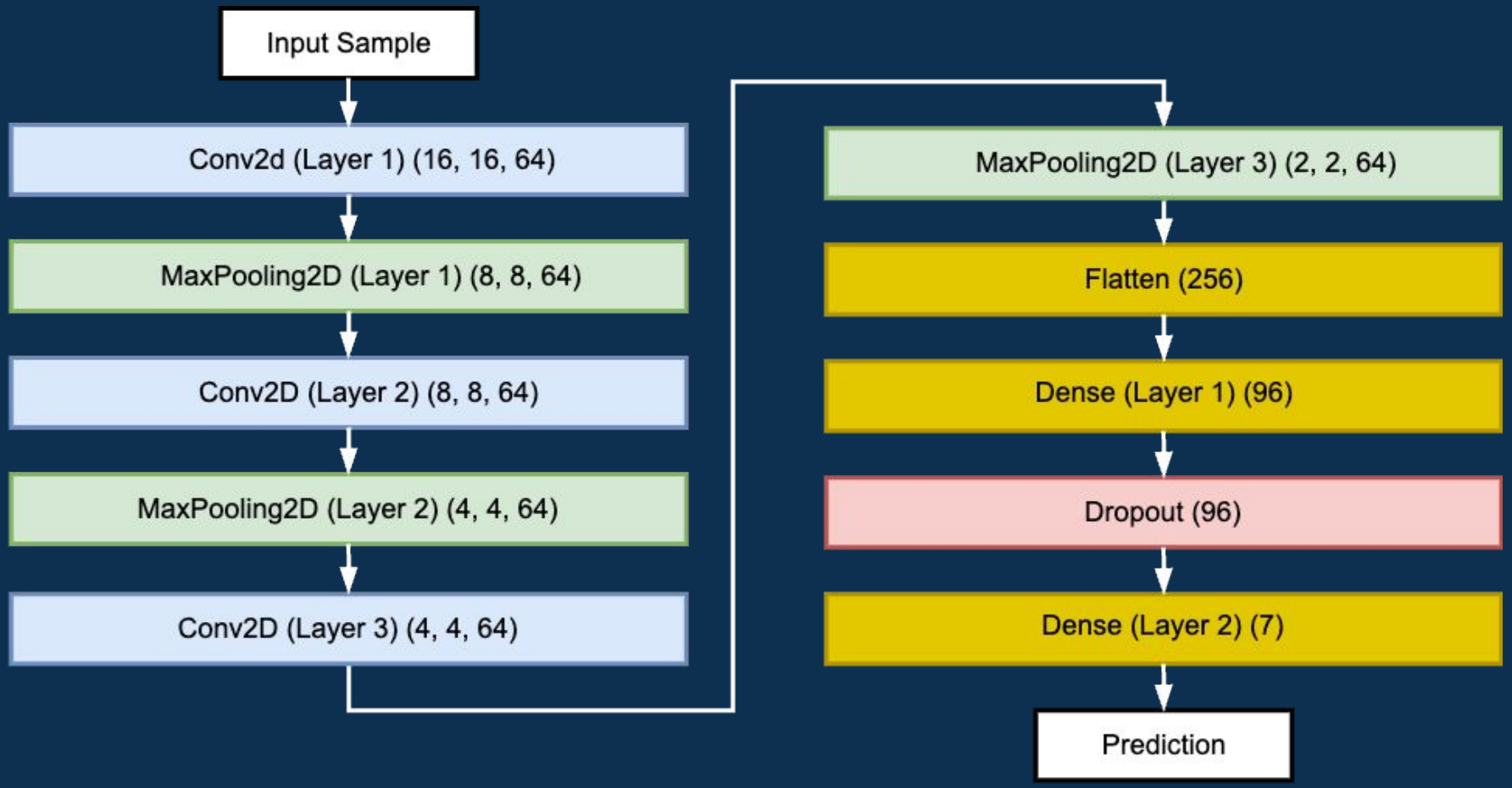
Spyware

PROCESSO DI CREAZIONE DEL DATASET



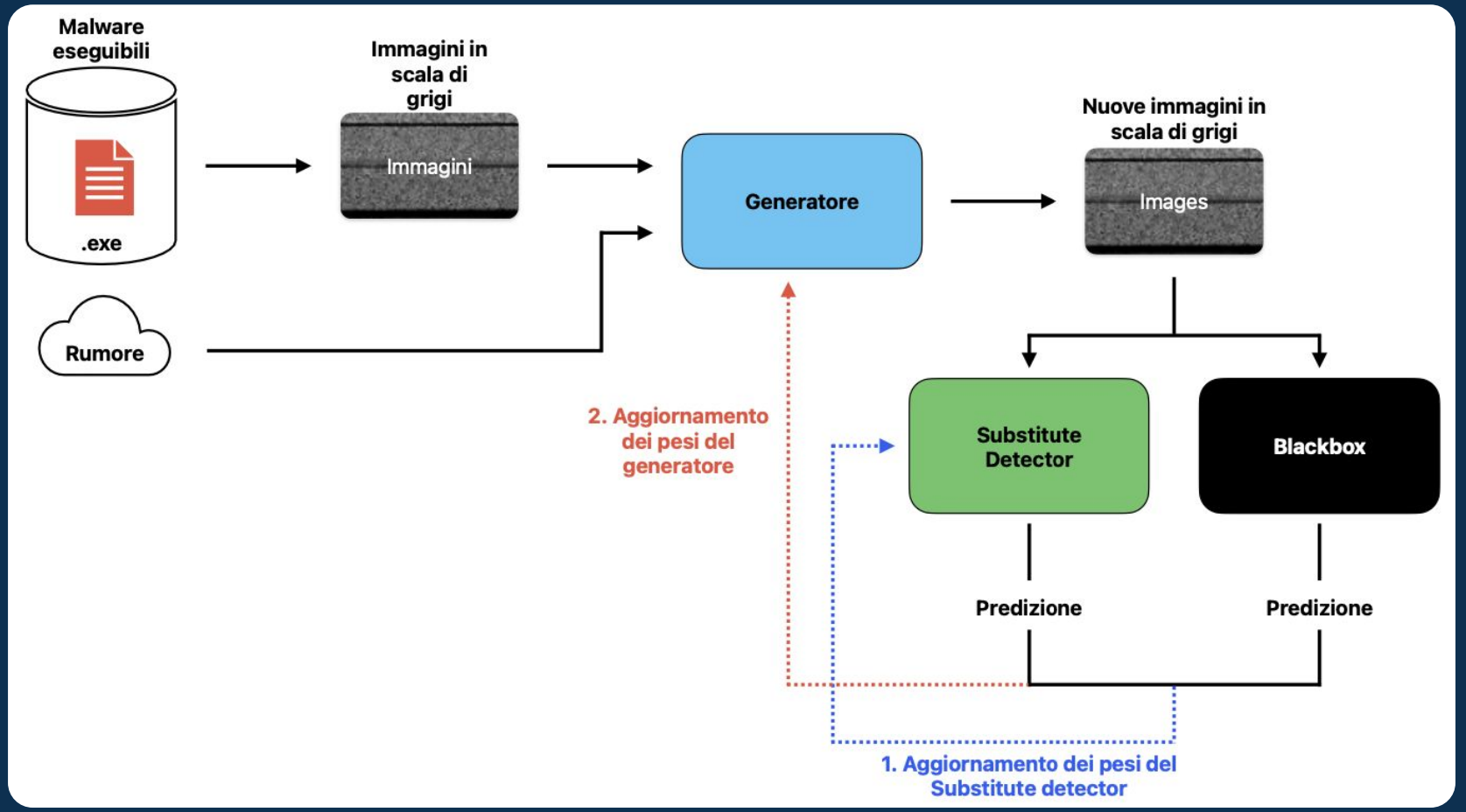
CONVOLUTIONAL NEURAL NETWORK

Architettura del modello CNN sviluppato



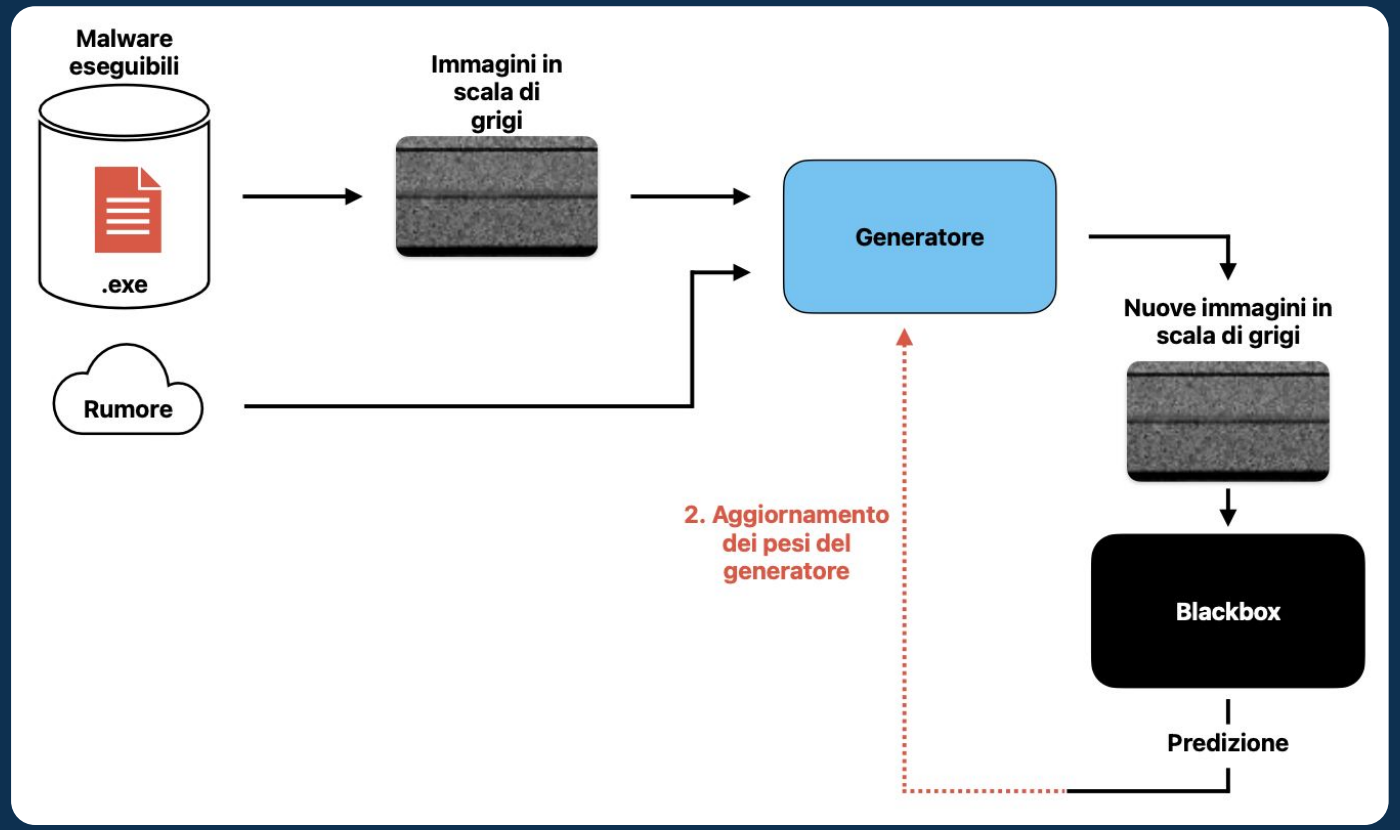
GENERATIVE ADVERSARIAL NETWORK

Architettura del modello GAN sviluppato

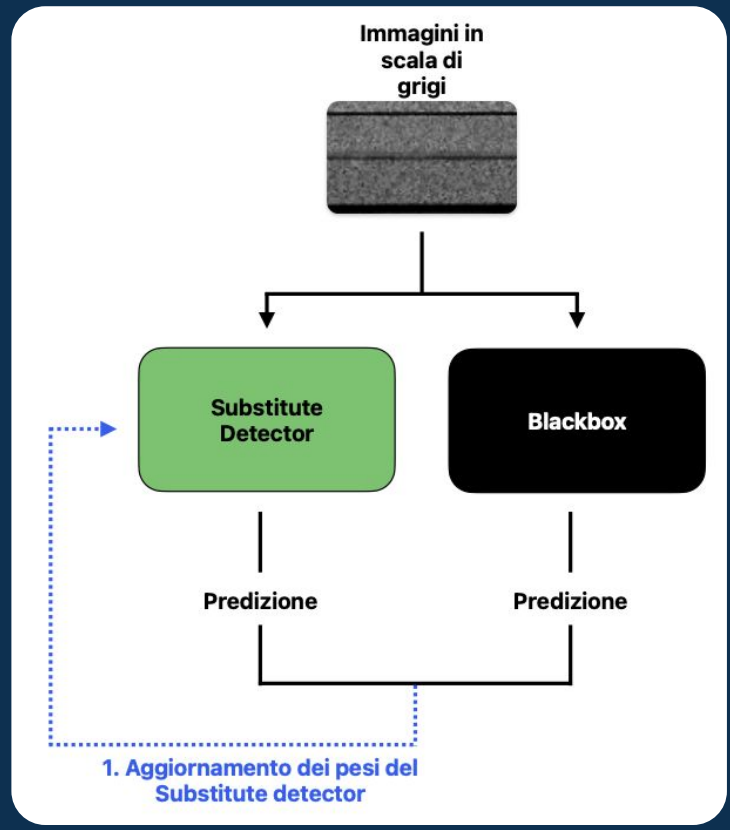


GENERATIVE ADVERSARIAL NETWORK

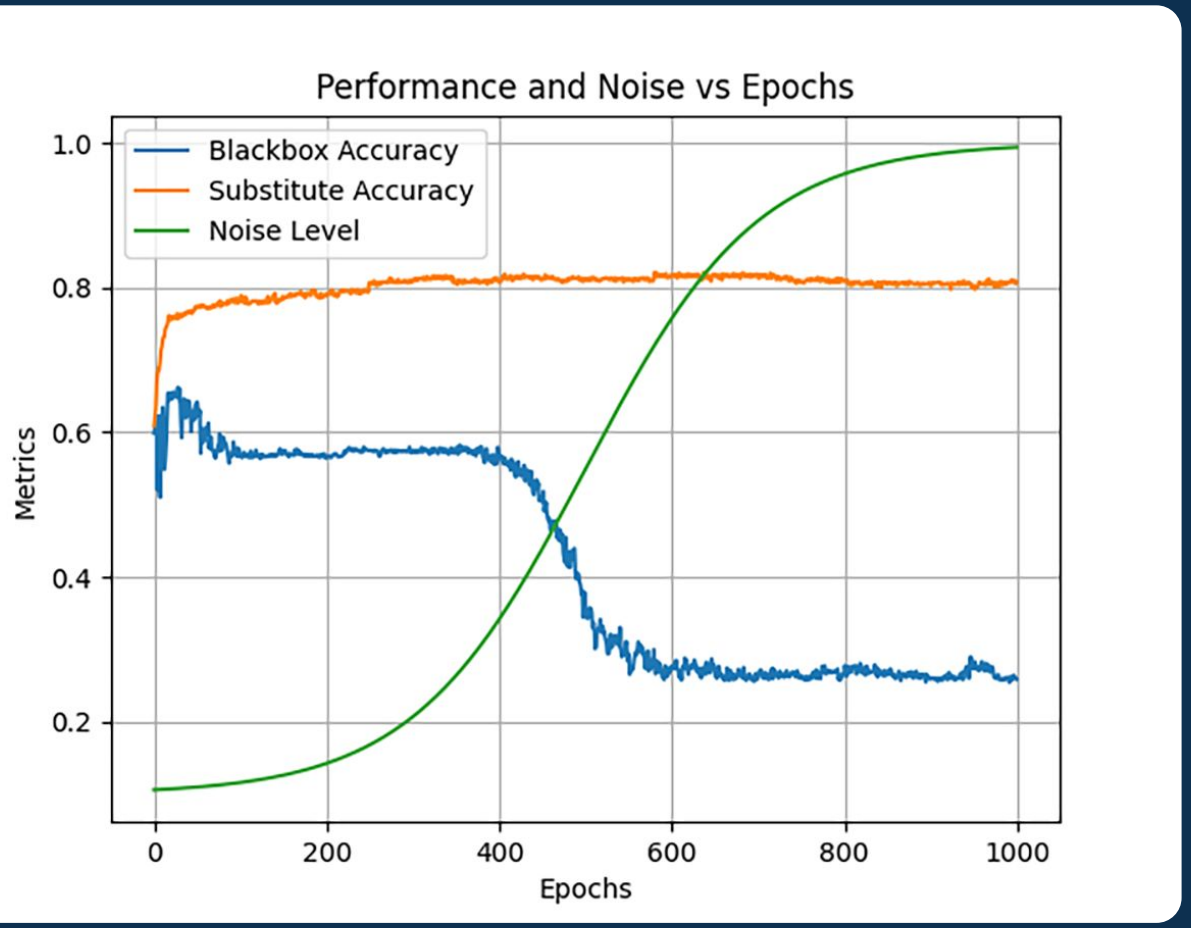
Processo di addestramento del generatore



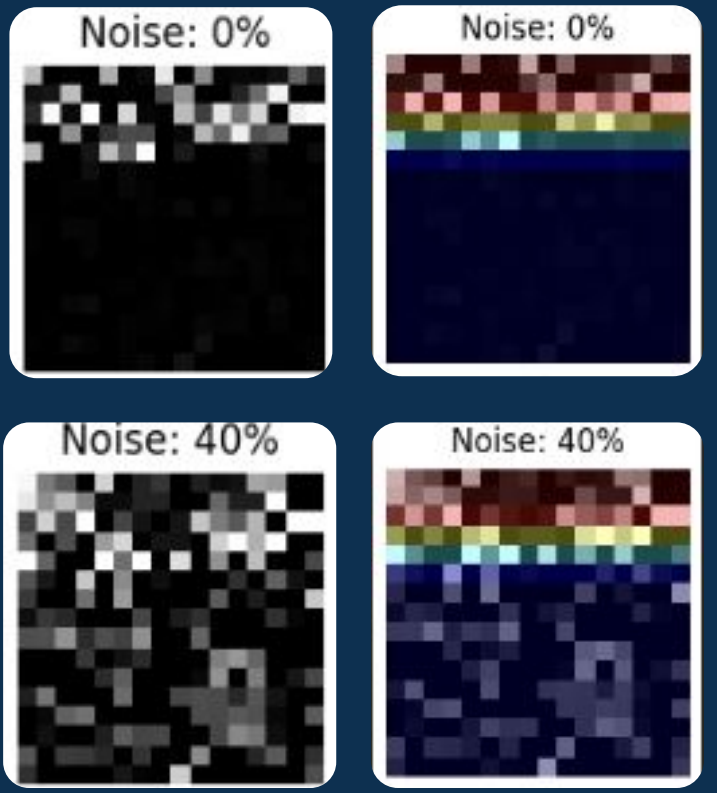
Processo di addestramento del Substitute detector



ESPERIMENTI CONDOTTI



Esempio applicazione grad-cam a malware di famiglia ***Spyware***



EVOLUZIONI FUTURE E POSSIBILI AMBITI DI APPLICAZIONE

- Ampliamento del dataset e miglioramento performance dei modelli
- Integrazione in scenari reali

Università
degli Studi
di Padova

Corso di Laurea in Informatica

Tiozzo Matteo