Università degli Studi di Padova

Decoding GAN-Generated Malware using Explainable AI Techniques

Corso di Laurea in Informatica

Tiozzo Matteo

Padova - 10/12/2024

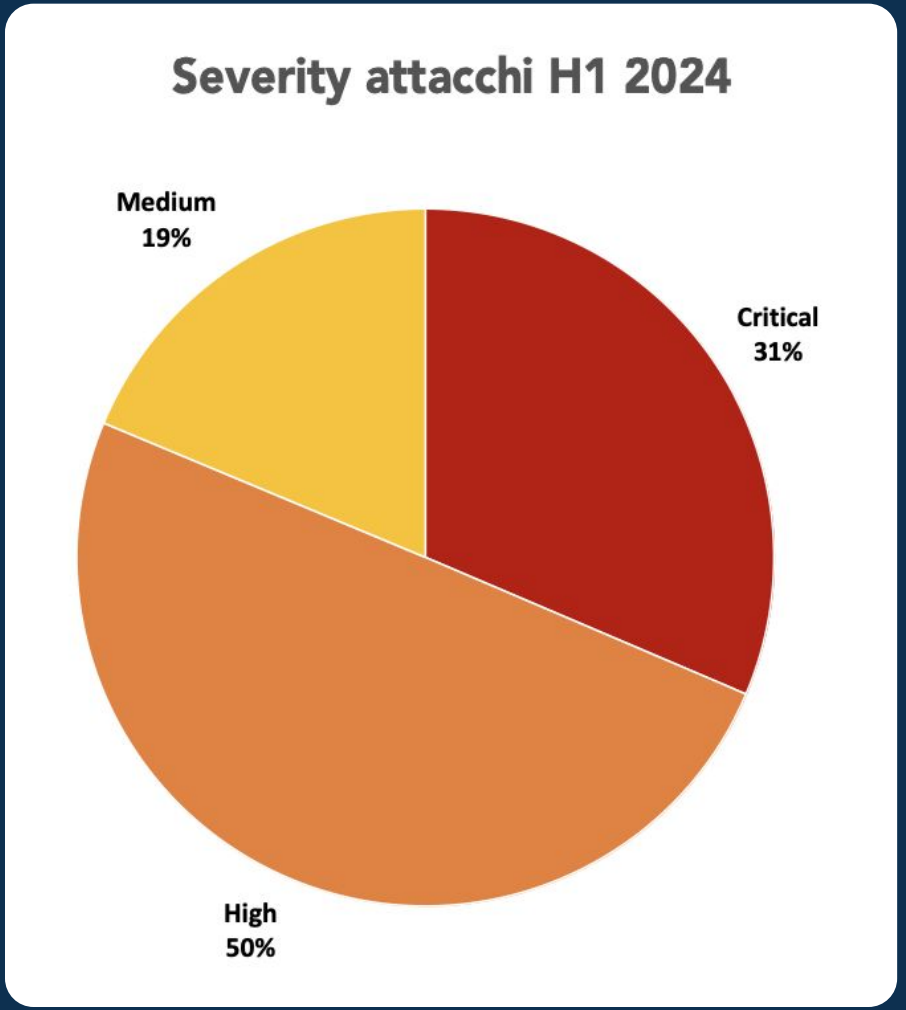
INDICE

MOTIVAZIONE

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

ANALISI DEI DATI

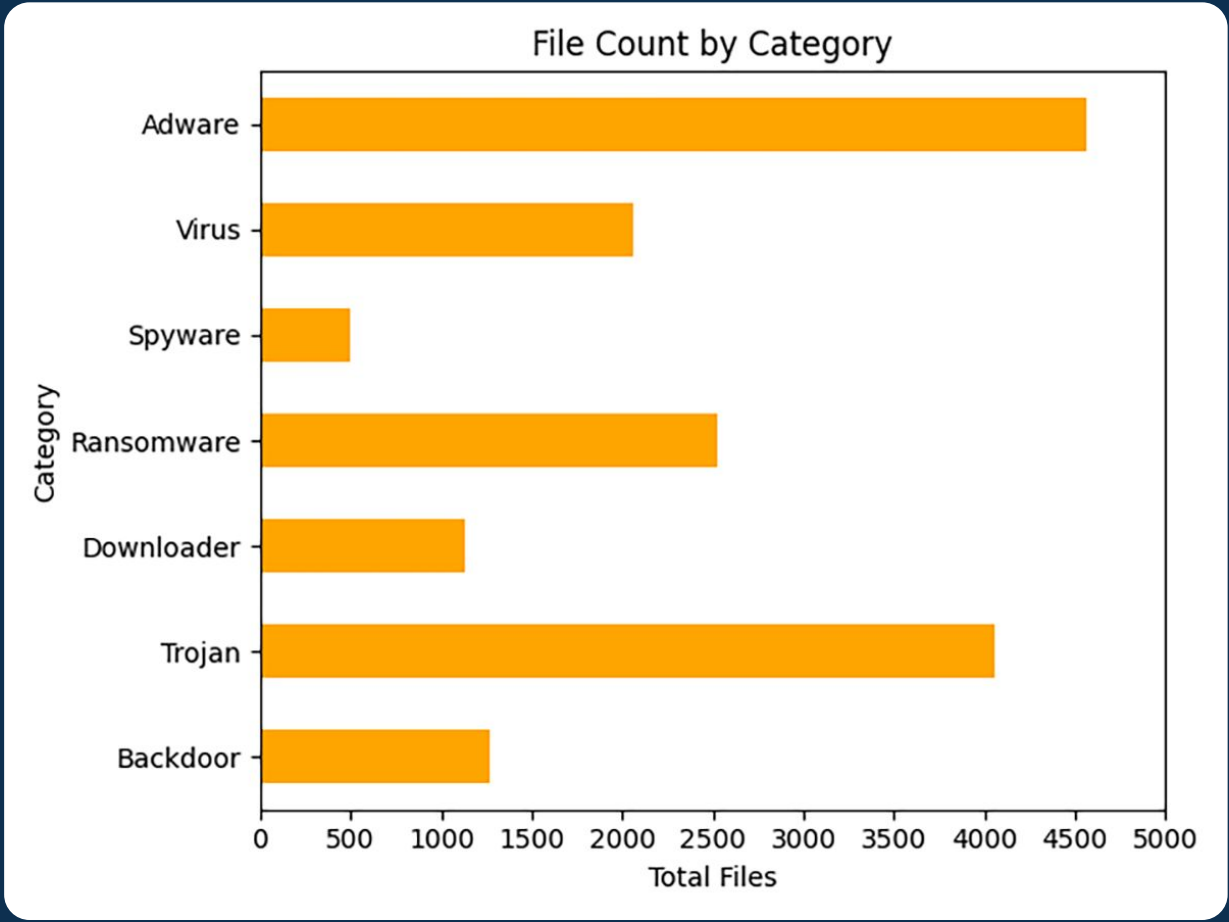
- **+23%** è la crescita degli incidenti dal *II* semestre 2023 al *I* semestre 2024
- **2x** è l'aumento della media mensile degli incidenti a livello mondiale rispetto al *I* semestre 2019
- **81%** è la percentuale di severità degli attacchi compresa tra "critica" e "alta"



Fonte: report Clusit giugno 2024

MALWARE

Cos’è, tipologie trattate e raccolta dati



Malware:

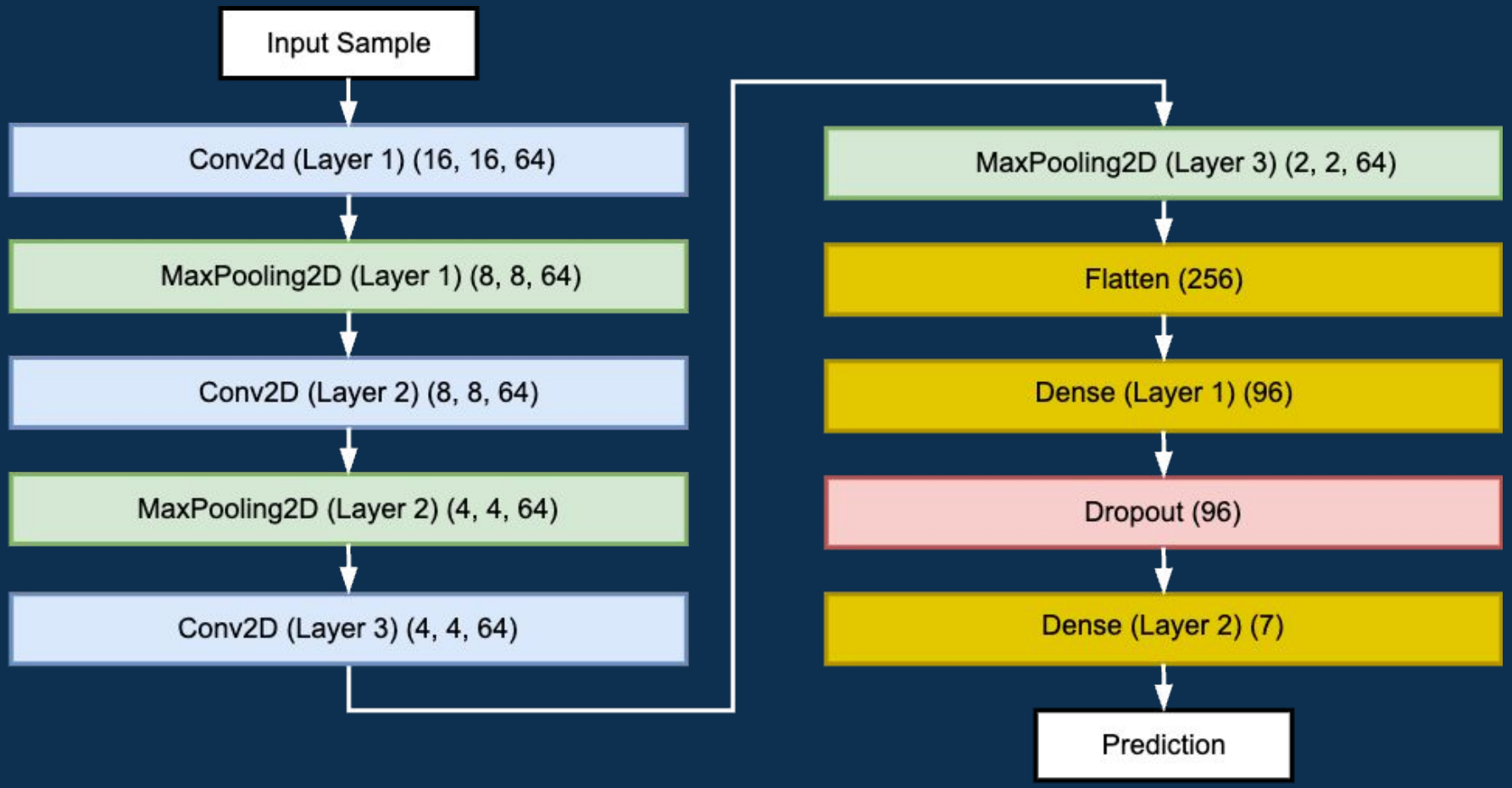
software dannoso che infiltra, danneggia o accede illegalmente a sistemi informatici.

Numero totale di malware Windows:

- 16114

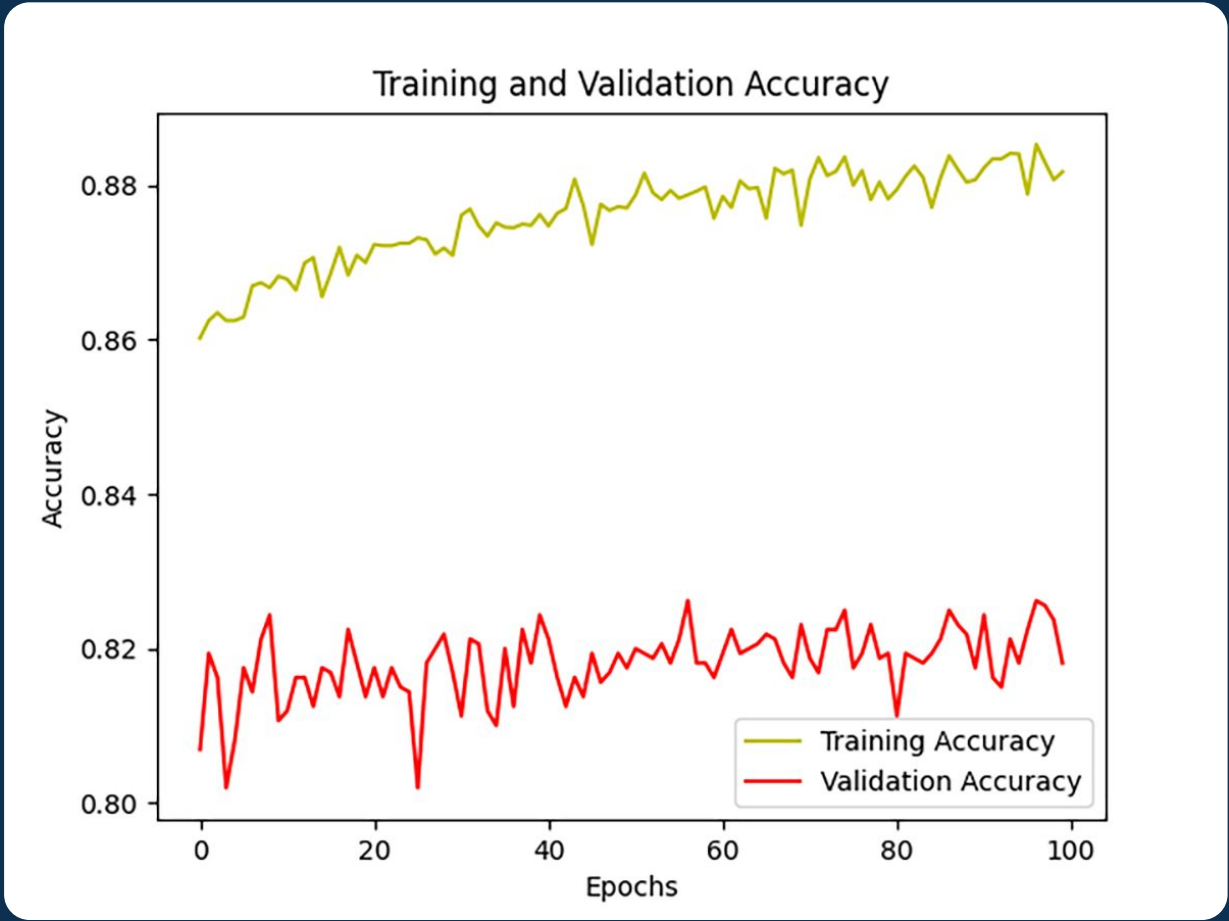
CONVOLUTIONAL NEURAL NETWORK

Architettura del modello CNN sviluppato



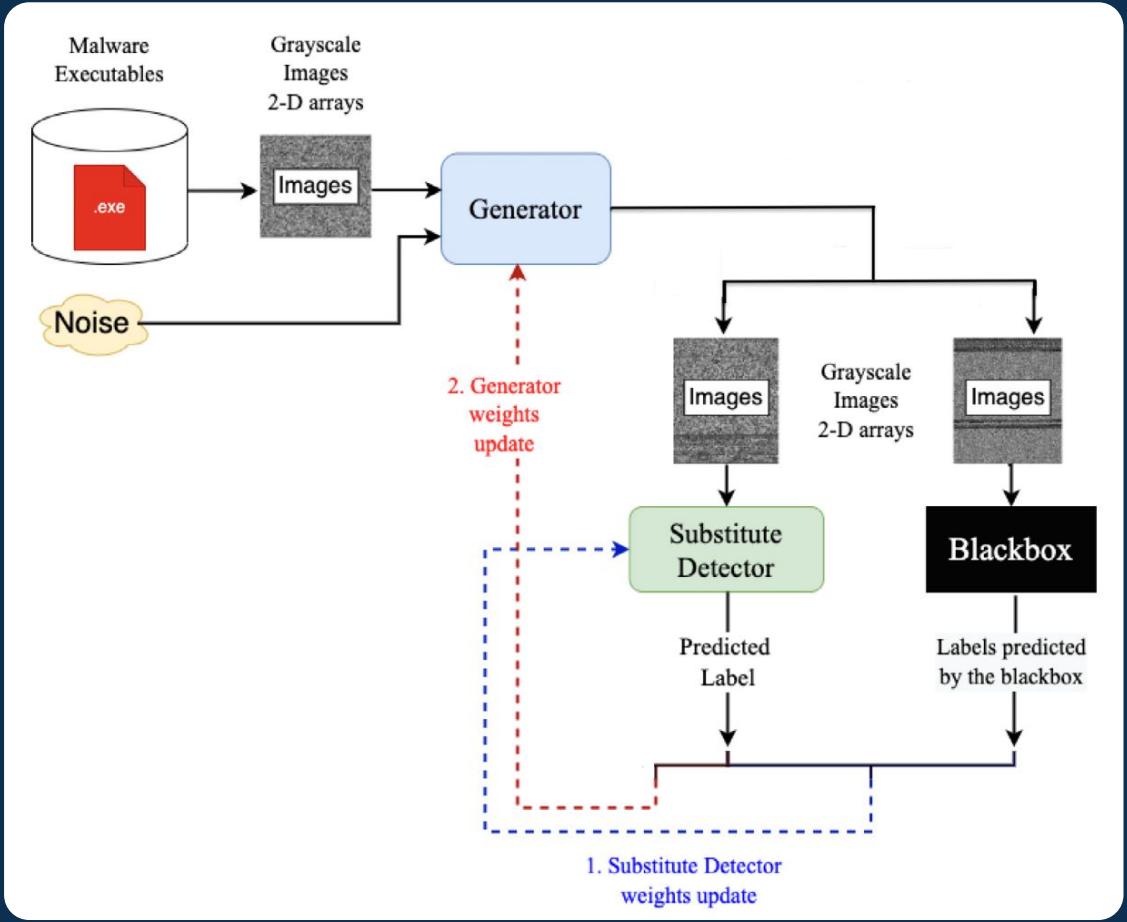
CONVOLUTIONAL NEURAL NETWORK

Metriche del modello CNN sviluppato durante l'addestramento e la validazione



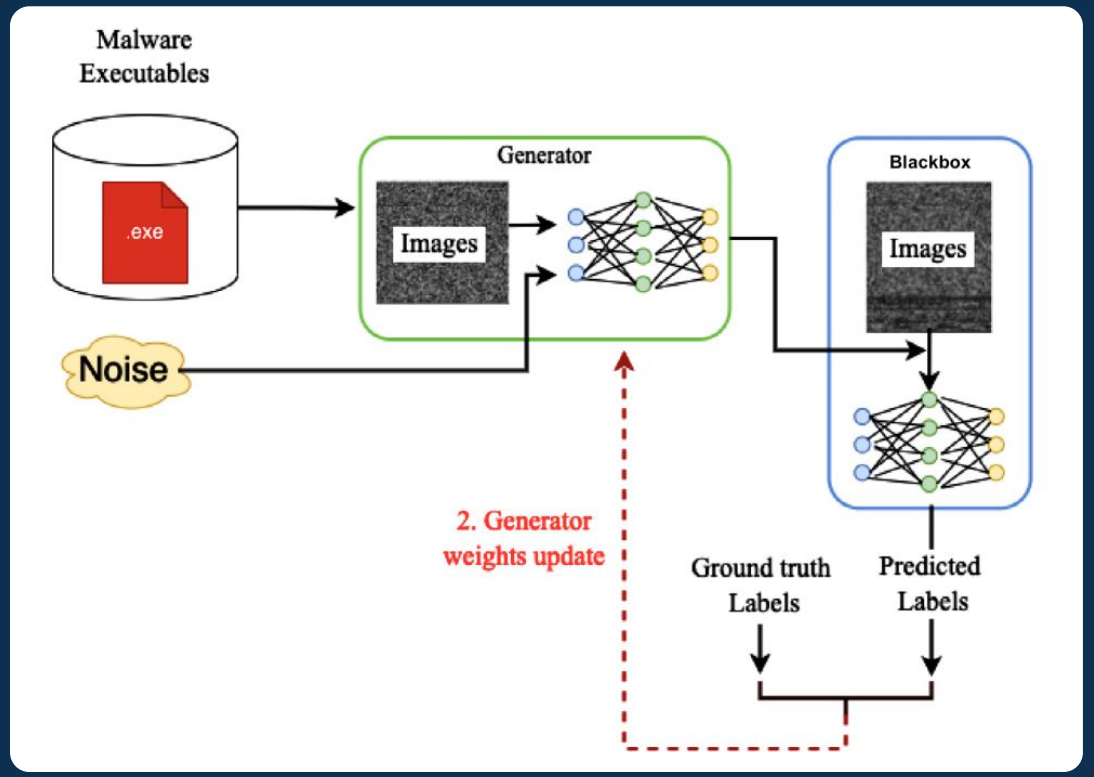
GENERATIVE ADVERSARIAL NETWORK

Architettura del modello GAN sviluppato

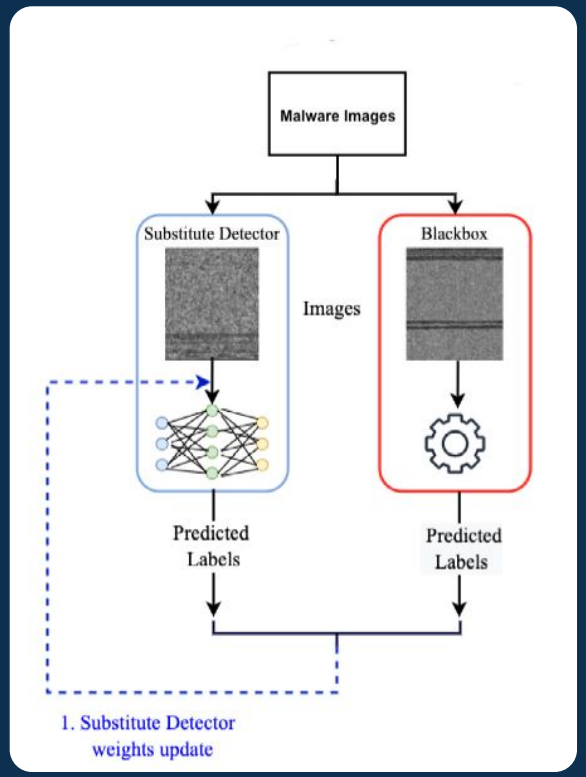


GENERATIVE ADVERSARIAL NETWORK

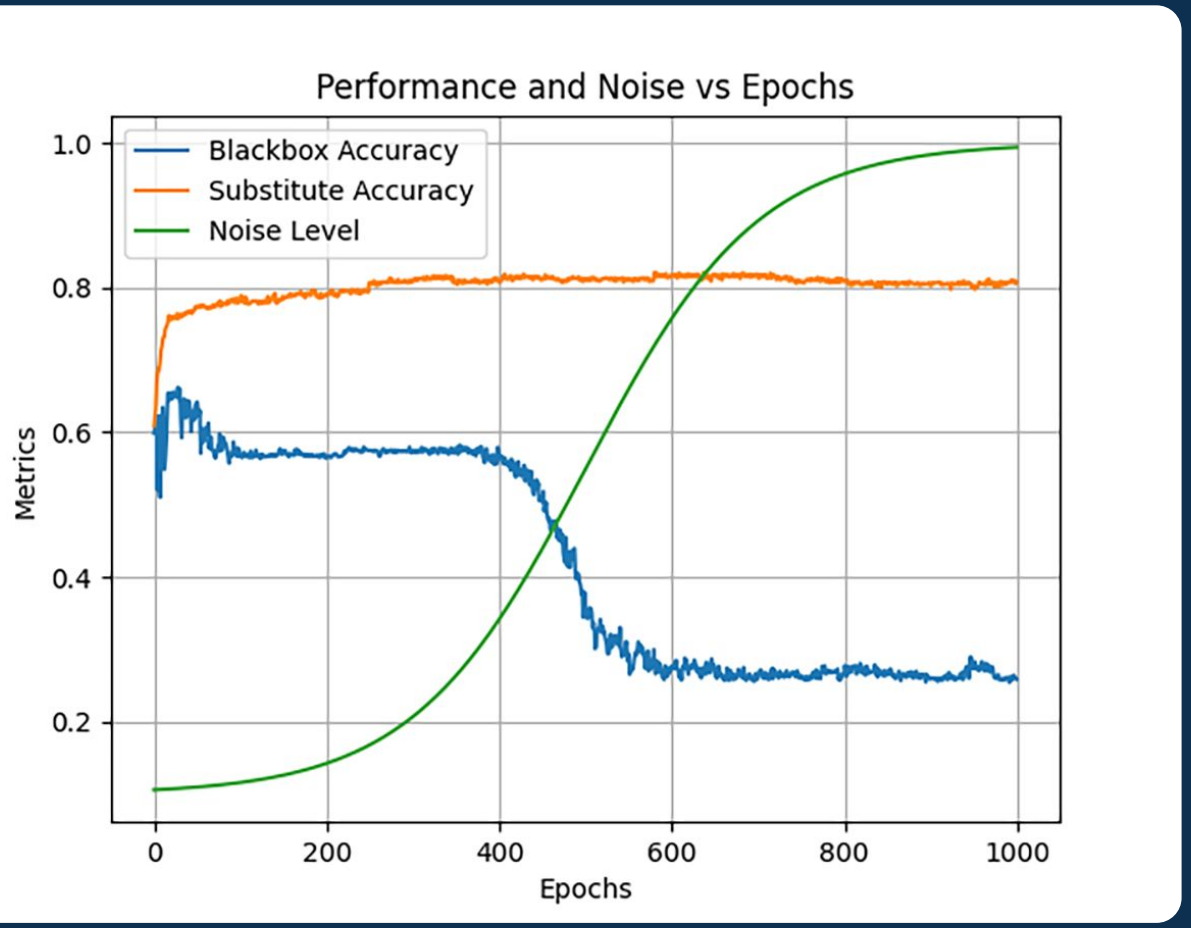
Processo di addestramento
del generatore



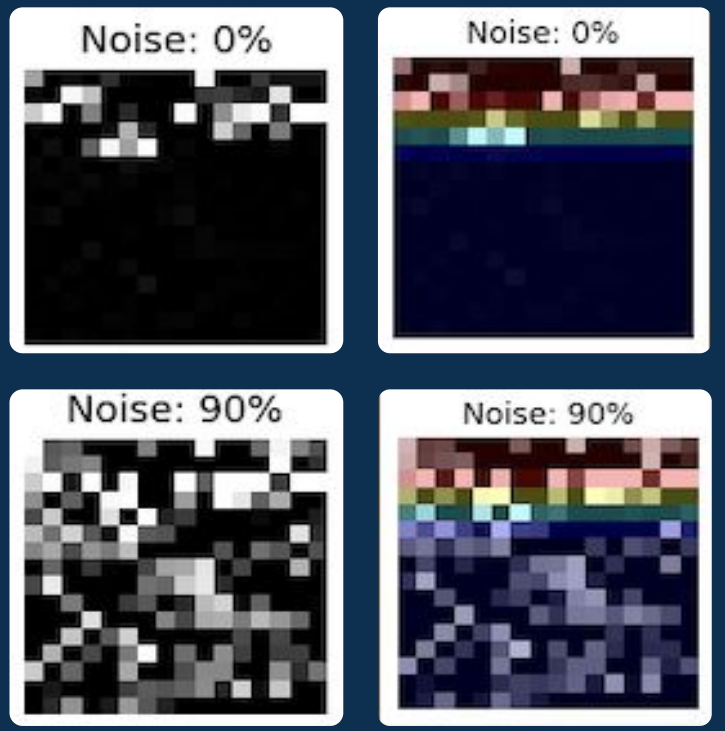
Processo di addestramento
del Substitute detector



ESPERIMENTI CONDOTTI



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



EVOLUZIONI FUTURE E POSSIBILI AMBITI DI APPLICAZIONE

- Integrazione in scenari reali
- Pubblicazione scientifica a riguardo

Università
degli Studi
di Padova

Corso di Laurea in Informatica

Tiozzo Matteo