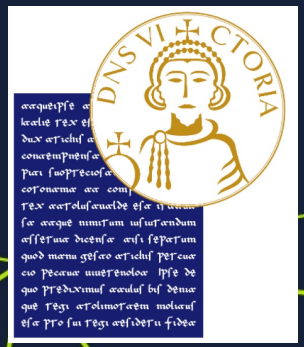
ANDREA DEL VECCHIO

Consortium GARR | THE ITALIAN EDUCATION & RESEARCH NETWORK

SISTEMI DI RILEVAMENTO DELLE INTRUSIONI INFORMATICHE RESILIENTI AD ATTACCHI AVVERSARI

GIORNATA DI INCONTRO
BORSE DI STUDIO GARR
"ORIO CARLINI"
ROMA
21/04/2021

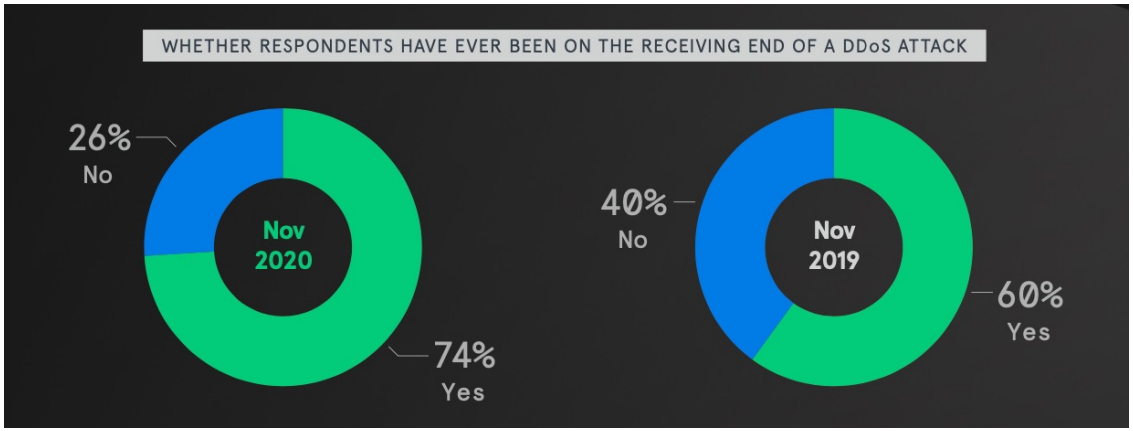


Università degli Studi del Sannio, Dip.to di Ingegneria

Tutor: Prof. Antonio Pecchia

CONTESTO

Sicurezza delle reti



https://www.home.neustar/resources/whitepapers/cyber-threats-and-trends-pandemic-style

154%
or over 2.5 times
Increase in number of attacks 2020 vs 2019

1.17 Tbps
Largest attack size in 2020

192%
Increase in the largest attack size in 2020 compared to 2019

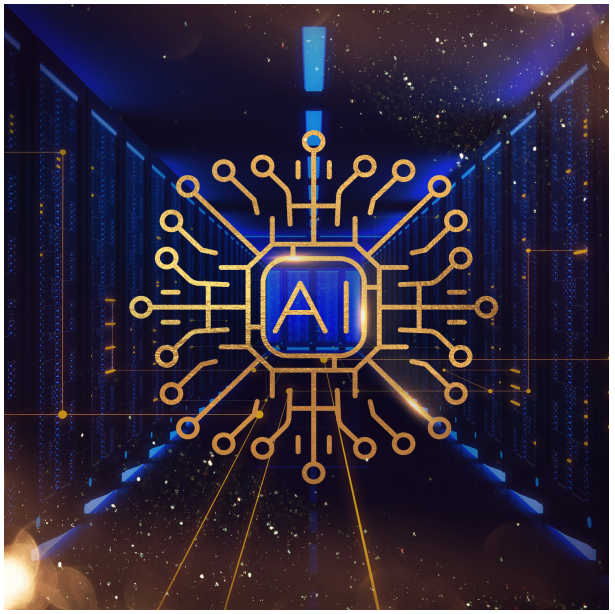
5 DAYS | 18 HRS
Longest attack duration

Intrusion Detection System

Signature Based

VS

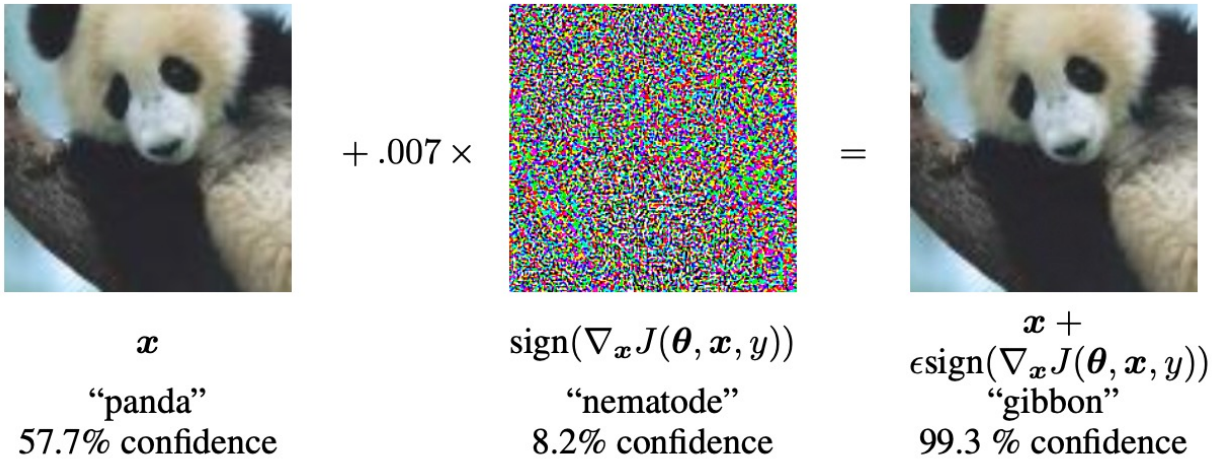
Anomaly Detection



- Efficaci per attacchi noti
- Poco flessibili a 0-day
- Difficile identificare le signature

- Efficaci anche contro 0-day
- Soggetti alle vulnerabilità tipiche del Machine Learning
  - ATTACCHI AVVERSARI

ATTACCO AVVERSARIO

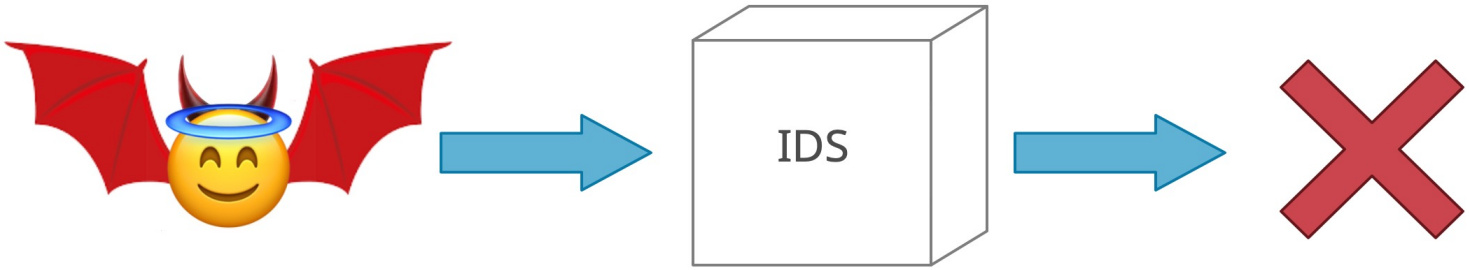


Ian Goodfellow, Jonathan Shlens, Christian Szegedy, "Explaining and Harnessing adversarial examples", 2015

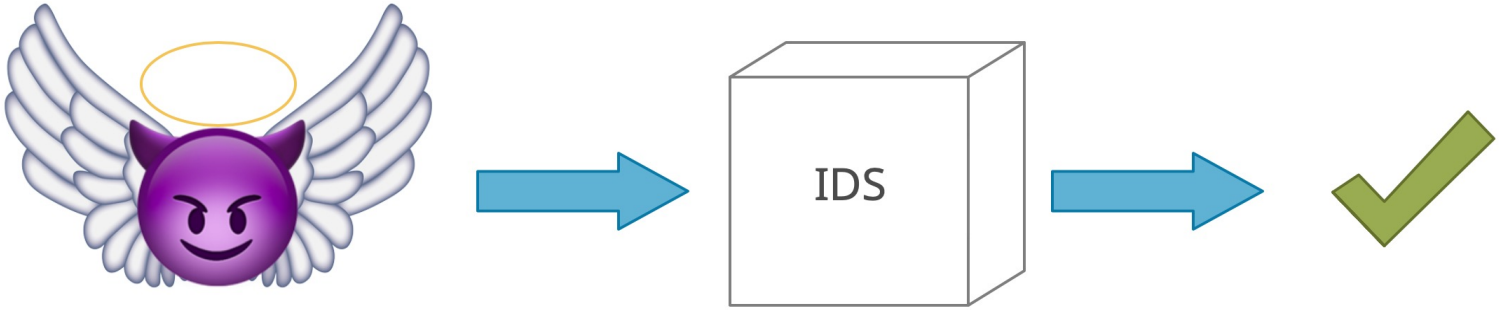
- Nato nel dominio del riconoscimento di immagini
- Obiettivo: misclassificazione

ATTACCHI AVVERSARI AGLI IDS

Overstimulation



Evasion



VULNERABILITÀ DEGLI ATTACCHI

Consistenza

N° Packets	Duration	Packets/s	SYN Flag	°°°
100	10	10	1	°°°

VULNERABILITÀ DEGLI ATTACCHI

Consistenza

N° Packets	Duration	Packets/s	SYN Flag	°°°
100	10	10	1	°°°

Algoritmo di generazione

N° Packets	Duration	Packets/s	SYN Flag	°°°
101	11	5	-1	°°°

VULNERABILITÀ DEGLI ATTACCHI

Consistenza

N° Packets	Duration	Packets/s	SYN Flag	°°°
100	10	10	1	°°°

Algoritmo di generazione

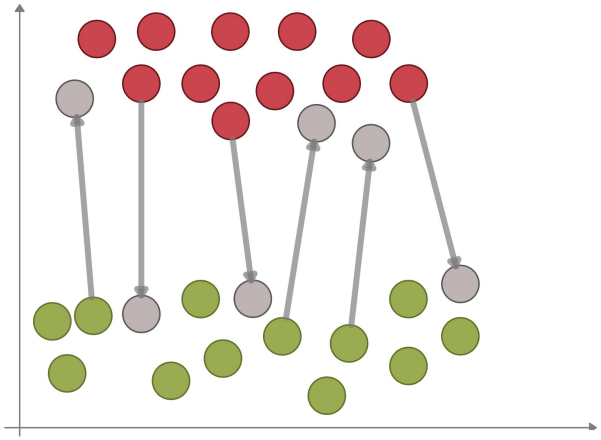
N° Packets	Duration	Packets/s	SYN Flag	°°°
101	11	5	-1	°°°

Vincoli di dominio

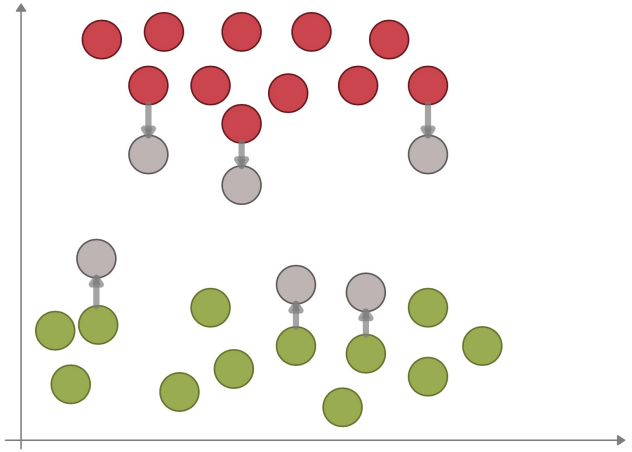
Vincoli intra-flusso

Rispetto dei vincoli a valle della perturbazione

Rappresentatività



Esempi non rappresentativi



Esempi rappresentativi

- FLUSSI BENIGNI
- FLUSSI MALEVOLI
- FLUSSI PERTURBATI

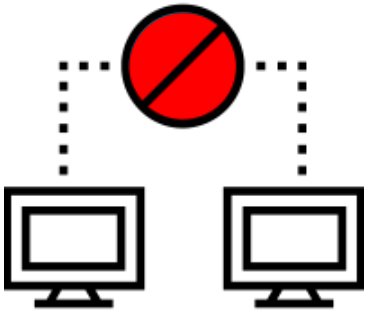
Capacità di preservare le caratteristiche a valle della perturbazione

OBIETTIVO

- Sfruttare le informazioni associate ad attacchi *Consistenti* e *Rappresentativi* per

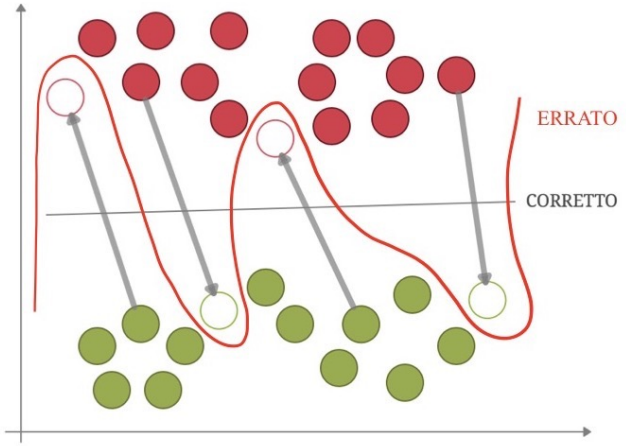
SISTEMI DI RILEVAMENTO RESILIENTI AD ATTACCHI

PERCHÉ



Realizzabilità dell'attacco

Correttezza del modello



COME

- Analisi e valutazione su dataset reali
  - CICIDS2017
  - USB-IDS-1

- Tecnologie
  - Python
  - Cleverhans

BENEFICI ATTESI

- Riduzione nella latenza di rilevamento degli attacchi

- Miglioramento nell'identificazione di falsi positivi/negativi

- Miglioramento di reaction e recovery

«Quis custodiet ipsos custodes?»

Giovenale