Machine Learning

Machine Learning as a Tool

Machine Learning as a Tool for Societal Exploitation

A Summary on the Current and Future State of Affairs

A Bit About Me

(I‘m going to pretend you care)

F1F1cin

- Student at Columbia University in New York
- Independent Researcher
- Mostly focus on malware
- Probably younger than you think
- I want to hack a human one day (judge all you want)

Current State

The Common and the Uncommon

Standard Uses
(generally beneficial, sometimes concerning)

The „Human“ Side

- Financial Trading
- Sports Injuries – [courtesy of Quantum Black]

The „Technical“ Side

- Data Security
- Antivirus Software
- Endpoint Detection Systems

The „Technical“ Side

- Data Security
- Antivirus Software
- Endpoint Detection Systems

„Normal“ people don‘t think about this… (?)

Uncommon Uses

(usually concerning, generally cool)



ˆ »–Š Š ‘

Crazy Dystopian S**t

Ambient Sound Mapping

- Determine precise location and orientation through microphone-embedded devices [without consent]

Individual Profiling

- Recreating the human based on digital fingerprints

Ambient Sound Mapping

Crazy Dystopian S**t

Ambient Sound Mapping

- Determine precise location and orientation through microphone-embedded devices [without consent]

Individual Profiling

- Recreating the human based on digital fingerprints
- Actually more common than I give it credit for

Individual Profiling

The Future of Attack

FIRST THING TO REMEMBER

AI is NOT Attackproof

(I‘m sure you know this)

1919

AI is NOT Attackproof

- „Attack“ isn‘t limited to using AI as a weapon

AI is NOT Attackproof

- „Attack“ isn‘t limited to using AI as a weapon
- „Attack“ can mean attacks targetted towards AI systems

AI as a Weapon

Current Experiments / Research / whatever you want to call it

„Whatever you want to call it“

- Wargames – [courtesy of Endgame]
- Intelligent Malware
- Adapting to a changing environment

Attacks on AI Systems

This is not what I Typically Do

- BUT

This is not what I Typically Do

- BUT
- Accidentally joining an AI-based IDS research group drags you into things

This is not what I Typically Do

- BUT
- Accidentally joining an AI-based IDS research group drags you into things
- Saying you‘re interested in malware makes people think you write it for fun (and no profit)

This is not what I Typically Do

- BUT
- Accidentally joining an AI-based IDS research group drags you into things
- Saying you‘re interested in malware makes people think you write it for fun (and no profit)
- So you‘re put in the attack/testing team

This is not what I Typically Do

- BUT
- Accidentally joining an AI-based IDS research group drags you into things
- Saying you‘re interested in malware makes people think you write it for fun (and no profit)
- So you‘re put in the attack/testing team, and then you realize you actually like it

What Can We Do?

- The research scenario and its limitations

What Can We Do?

- The research scenario and its limitations
- Let‘s remember things that happened throughout the weekend.

What Can We Do?

- The research scenario and its limitations
- Let‘s remember things that happened throughout the weekend. (and things coming up)
- What else is can be treated in a similar manner?

Attacking the Human

(one of my goals, but kind of far-fetched at the moment)

Attacking the Human

(one of my goals, but kinds of far-fetched at the moment)

The Future of Defense

Tricking AI in Practice

(and why this is importatnt for defense mechanisms)

The Overlaps

- You might notice overlaps between attack and defense
- Like any other tool, AI can be used on both ends of the spectrum, sometimes without much modification

Defense for the Common Man

. . .

(Attack against the algorithm)

A Sample of Defense :

Avoiding Identification

We Have Seen This Before

Demo time ?