

Mapping Deception Feasibility Across MITRE ATT&CK®

Veronica Valeros¹, Carlos Catania², Viliam Lisý¹, Harm Griffioen³

¹ Czech Technical University in Prague, ² National University of Cuyo, ³ Delft University of Technology

PROBLEM

In cybersecurity we assume we can use deception to catch **any** attacker behaviour.

Nobody has checked, until now.

SCORING RUBRIC

We scored all **250 ATT&CK v18.1 techniques** on:

Feasibility: Can the asset be faked?

Interaction: Will the attacker interact with it?

Intelligence Yield: Do we learn from it?

Malice Fidelity: Are we sure it was malicious?

RESEARCH QUESTIONS

RQ1: Which attacker behaviours **admit a decoy**? What **signal** would those decoys produce?

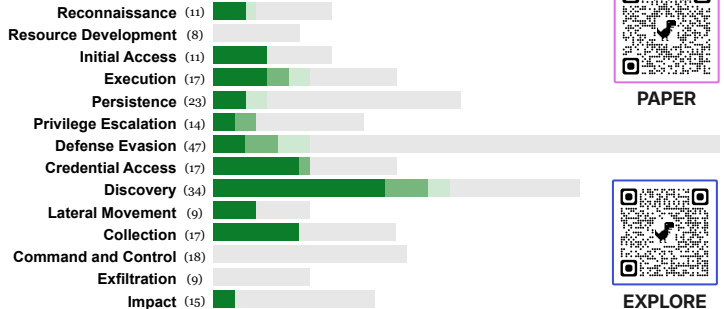
RQ2: **Why** do some attacker behaviours admit a decoy and others do not?

RESULTS

- Only **80 of 250** of techniques admit a decoy
- **No decoy** can be placed on tactics: Resource Development, Command and Control, or Exfiltration
- Every decoy must **sit on a Sweep path** or **imitate a sought asset**.

THE DECEPTION ATTACK SURFACE IS SPARSE

Feasibility: ■ Yes ■ Mostly Yes ■ Mostly No ■ No decoy possible



PAPER



EXPLORE

IF WE HAVE INTERACTION, INTELLIGENCE IS THERE

