The **Python Ecosystem is messed up and here’s why.**

We explored 200k Python packages on PyPI and...

---

I know what you imported last summer

`pip install` runs `python setup.py install` internally allowing arbitrary code execution

Trust me if you can

An average Python package trusts **14** other packages while installing

Something's Phishy

- Sound the same
  - Django and jango
- Low edit distance
  - Jellyfish and Jellyfish
- `Python2 -> Python3`
  - `Dateutil` and `Python3-dateutil`

There is no License to kill

Potential license violations in PyPI due to hierarchical imports

Live Demo!

A wild Jellyfish appeared

Arbitrary code **stealing SSH keys** reported on 2nd Dec '19.

Downloads boom after **typo-squatted** `python3-dateutil` imports `jellyfish`

---

*Aadesh Bagmar is a member of the SEAM Lab (Software Engineering @ Maryland) and is supported by Office of Naval Research under contract N000141812767*

---

Aadesh M Bagmar* and Katie Sullivan

University of Maryland, College Park

**www.rsaconference.com/securityscholar**