

Automated Malware Detection in Python Package Index

Cristina Muñoz

About Me

- DevOps jack-of-all-trades
- “doing security” < 3 years
- Disillusioned with Big Tech™



The New York Times

Google Fires 4 Workers Active in Labor Organizing



Google's 'Project Nightingale' Gathers Data on Millions of Americans

Search giant is amassing health records from Ascension facilities, sources informed

GOOGLE EMPLOYEES UNCOVER ONGOING WORK ON CENSORED CHINA SEARCH

Illustration: Sohee Cho/The

GOOGLE HIRED GIG ECONOMY WORKERS IMPROVE ARTIFICIAL INTELLIGENCE IN CONTROVERSIAL DRONE-TARGETING PROJECT

Illustration: Sohee Cho/The

How Google Protected Andy Rubin, the 'Father of Android'

Search giant paid Mr. Rubin \$90 million and praised him, sources informed, in a misconduct claim.







(9) seeking advice: implementing cryptographic signing and malware detection on PyPI

From: Sumana Harihareswara <sumanah@pypi.org>

09/03/2019 (6 months ago)

To: Cristina Muñoz

Show details



Cristina:

Hi! I'm a Recurser and I think you and I have talked on Zulip?

Would you take a look at this and potentially comment? And forward it to experts you know who might be interested? If you could, I would be grateful.

Please check out this Request for Information for a Python Software Foundation contract? PSF is seeking developers to implement cryptographic signing and malware detection on PyPI:

<https://github.com/python/request-for/blob/master/2019-Q4-PyPI/RFI.md>

This RFI period will close on September 18th.

During the RFI period, the PSF is hoping to get participation from potential participants and other experts in the discussion forum at <https://discuss.python.org/c/python-software-foundation/pypi-q4-rfi> especially about implementation questions (such as: use The Update Framework or not?).

Then, the Request for Proposals period will be September 23-October 16.


Please feel free to forward and spread the word publicly, if you'd like! <https://pyfound.blogspot.com/2019/08/pypi-security-q4-2019-request-for.html> is the PSF blog post about it.

Thank you.

Sumana Harihareswara
project manager for PyPI, Recurser


PyPI

—
The canonical source of
Python packages




Help Donate Log in Register

Find, install and publish Python packages with the Python Package Index



Or [browse projects](#)

222,166 projects 1,713,923 releases 2,599,584 files 408,016 users



The Python Package Index (PyPI) is a repository of software for the Python programming language.

PyPI helps you find and install software developed and shared by the Python community. [Learn about installing packages](#).

Package authors use PyPI to distribute their software. [Learn how to package your Python code for PyPI](#).


```
pip install requests
```

Request For Proposal

- 1 - Verifiable cryptographic signing of artifacts
- 2 - Systems for Automated Detection of Malicious Uploads

System Requirements

- A pluggable system for development, deployment and execution of checks
- Storage for check results
- Administrator views for reviewing results
- Document the process for development and submission of new checks

Another Perspective

This is a SIEM.



(26) proposal for milestone 2



From: Ernest W. Durbin III <ewdurbin@pyfound.org> ▼ 🔒

10/29/2019 (4 months ago) ☆

To: Cristina Muñoz

[Show details](#)



Hello Cristina!

Thank you for a thoroughly specified proposal! We are excited to let you know that your proposal was selected for Milestone 2!

However, there's a bit of further discussion that needs to happen as we will be engaging another proposer for Milestone 1 that also proposed for Milestone 2.

At this point in time, we need two responses from you:

- Are you still available and interested in performing the work specified in Milestone 2 of the Request for Proposals as described in your Proposal?
- Would collaborating with another contractor in the implementation of Milestone 2 be a concern?

-Ernest W. Durbin III
Director of Infrastructure
Python Software Foundation

Project, Releases, and Files, oh my!

Project > Release > Files

[Help](#)[Donate](#)[Log in](#)[Register](#)

sodapy 2.0.0

`pip install sodapy`[Latest version](#)

Released: Nov 1, 2019

Python library for the Socrata Open Data API

Navigation

[Project description](#)[Release history](#)[Download files](#)

Project links

[Homepage](#)[Download](#)

Statistics

GitHub statistics:

★ Stars: 254

🍴 Forks: 81

Project description

pypi package 2.0.0 build passing

sodapy

sodapy is a python client for the [Socrata Open Data API](#).

Installation

You can install with `pip install sodapy`.If you want to install from source, then clone this repository and run `python setup.py install` from the project root.

Requirements

At its core, this library depends heavily on the [Requests](#) package. All other requirements can be found in [requirements.txt](#). sodapy is currently compatible with Python 3.4, 3.5, 3.6, 3.7 and 3.8.

[Help](#)[Donate](#)[Log in](#)[Register](#)

sodapy 2.0.0

```
pip install sodapy
```

[Latest version](#)

Released: Nov 1, 2019

Python library for the Socrata Open Data API

Navigation

[Project description](#)[Release history](#)[Download files](#)

Project links

[Homepage](#)[Download](#)

Statistics

GitHub statistics:

★ Stars: 254

👤 Forks: 81

Release history

[Release notifications](#)**THIS VERSION****2.0.0**

Nov 1, 2019

**1.5.5**

Sep 26, 2019

**1.5.4**

Jul 17, 2019

**1.5.3**

Jul 4, 2019

[Help](#)[Donate](#)[Log in](#)[Register](#)

sodapy 2.0.0

```
pip install sodapy
```

[Latest version](#)

Released: Nov 1, 2019

Python library for the Socrata Open Data API

Navigation

[Project description](#)[Release history](#)[Download files](#)

Project links

[Homepage](#)[Download](#)

Statistics

GitHub statistics:

★ Stars: 254

🍴 Forks: 81

Download files

Download the file for your platform. If you're not sure which to choose, learn more about [installing packages](#).

Filename, size	File type	Python version	Upload date	Hashes
sodapy-2.0.0-py2.py3-none-any.whl (13.8 kB)	Wheel	py2.py3	Nov 1, 2019	View
sodapy-2.0.0.tar.gz (29.7 kB)	Source	None	Nov 1, 2019	View

Typosquatting and Namesquatting

```
pip install python3-dateutil
```

```
pip install jellyfish
```



[Source: [python-dateutil](#)]

Package: python3-dateutil (2.5.3-2)

powerful extensions to the standard datetime module

It features:

- * computing of relative deltas (next month, next year, next monday, last week of month, etc);
- * computing of relative deltas between two given date and/or datetime objects
- * computing of dates based on very flexible recurrence rules, using a superset of the iCalendar specification. Parsing of RFC strings is supported as well.
- * generic parsing of dates in almost any string format
- * timezone (tzinfo) implementations for tzfile(5) format files (/etc/localtime, /usr/share/zoneinfo, etc), TZ environment string (in all known formats), iCalendar format files, given ranges (with help from relative deltas), local machine timezone, fixed offset timezone, UTC timezone
- * computing of Easter Sunday dates for any given year, using Western, Orthodox or Julian algorithms

Other Packages Related to python3-dateutil

● depends ■ recommends ◆ suggests ▲ enhances

● dep: [python3](#)

interactive high-level object-oriented language (default python3 version)

setup.py

```
#!/usr/bin/env python
from setuptools import setup
from setuptools.command.install import install
from my_evil_module import root_reverse_shell

class PostInstallCommand(install):
    def run(self):
        root_reverse_shell()
        install.run(self)

setup(
    name='0wned',
    version='0.6.0',
    description='Code execution via Python package installation.',
    ...
    cmdclass={
        'install': PostInstallCommand,
    },
)
```

This repository has been archived by the owner. It is now read-only.

dominictarr / event-stream Archived

Used by 469k

Watch 70

Star 2.1k

Fork 149

<> Code

Issues 7

Pull requests 0

Actions

Projects 0

Wiki

Security

Insights

I don't know what to say. #116



FallingSnow opened this issue on Nov 20, 2018 · 666 comments



FallingSnow commented on Nov 20, 2018 • edited

EDIT 26/11/2018:

- **Am I affected?:**

If you are using anything crypto-currency related, then maybe. As discovered by @maths22, the target seems to have been identified as copay related libraries. It only executes successfully when a matching package is in use (assumed to be copay at this point). If you are using a crypto-currency related library and if you see flatmap-stream@0.1.1 after running `npm ls event-stream flatmap-stream`, you are most likely affected. For example:

```
$ npm ls event-stream flatmap-stream
...
flatmap-stream@0.1.1
...
```

- **What does it do:**

Other users have done some good analysis of what these payloads actually do.

- [#116](#) (comment)
- [#116](#) (comment)
- [#116](#) (comment)

- **What can I do:**

By this time fixes are being deployed and npm has yanked the malicious version. Ensure that the developer(s) of the package you are using are aware of this post. If you are a developer update your event-stream dependency to `event-stream@3.3.4`. **This protects people with cached versions of event-stream.**

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Linked pull requests

Successfully merging a pull request may close this issue.

[chore\(core\): update deps and fix ...](#)

Notifications

Customize

🔔 Subscribe

You're not receiving notifications from this thread.

341 participants

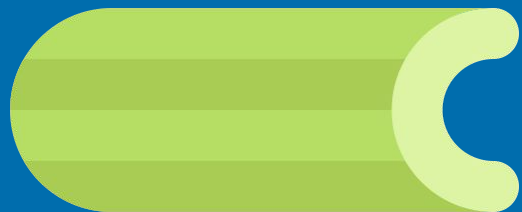
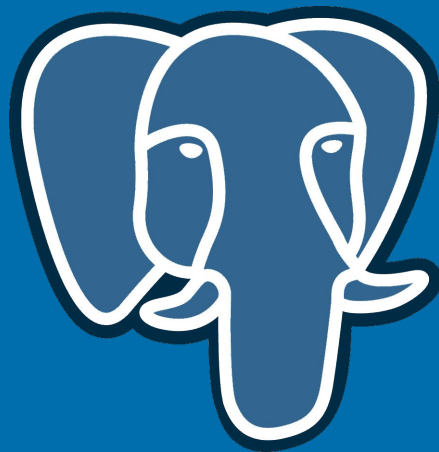
MALWARE

MALWARE EVERYWHERE

Warehouse



SQLAlchemy



Types of Checks

- Project/Release/File creation time hooks for *events*
- Scheduled investigations to look for *behaviors*

Event-based checks

Upload release files to VirusTotal

Pattern match malicious code signatures using YaraRules

Run static or dynamic analyzers

SetupPatternCheck

Yara rules looking for:

- Process spawn
- Network connections
- Deserialization
- Metaprogramming

```
def query(self, attr_name):
    """Spawn the pg_config executable, querying for the given config
    name, and return the printed value, sanitized. """
    try:
        pg_config_process = subprocess.Popen(
            [self.pg_config_exe, "--" + attr_name],
            stdin=subprocess.PIPE,
            stdout=subprocess.PIPE,
            stderr=subprocess.PIPE)
    except OSError:
        raise Warning("Unable to find 'pg_config' file in '%s'" %
                      self.pg_config_exe)
    pg_config_process.stdin.close()
    result = pg_config_process.stdout.readline().strip()
    if not result:
        raise Warning(pg_config_process.stderr.readline())
    if not isinstance(result, str):
        result = result.decode('ascii')
    return result
```

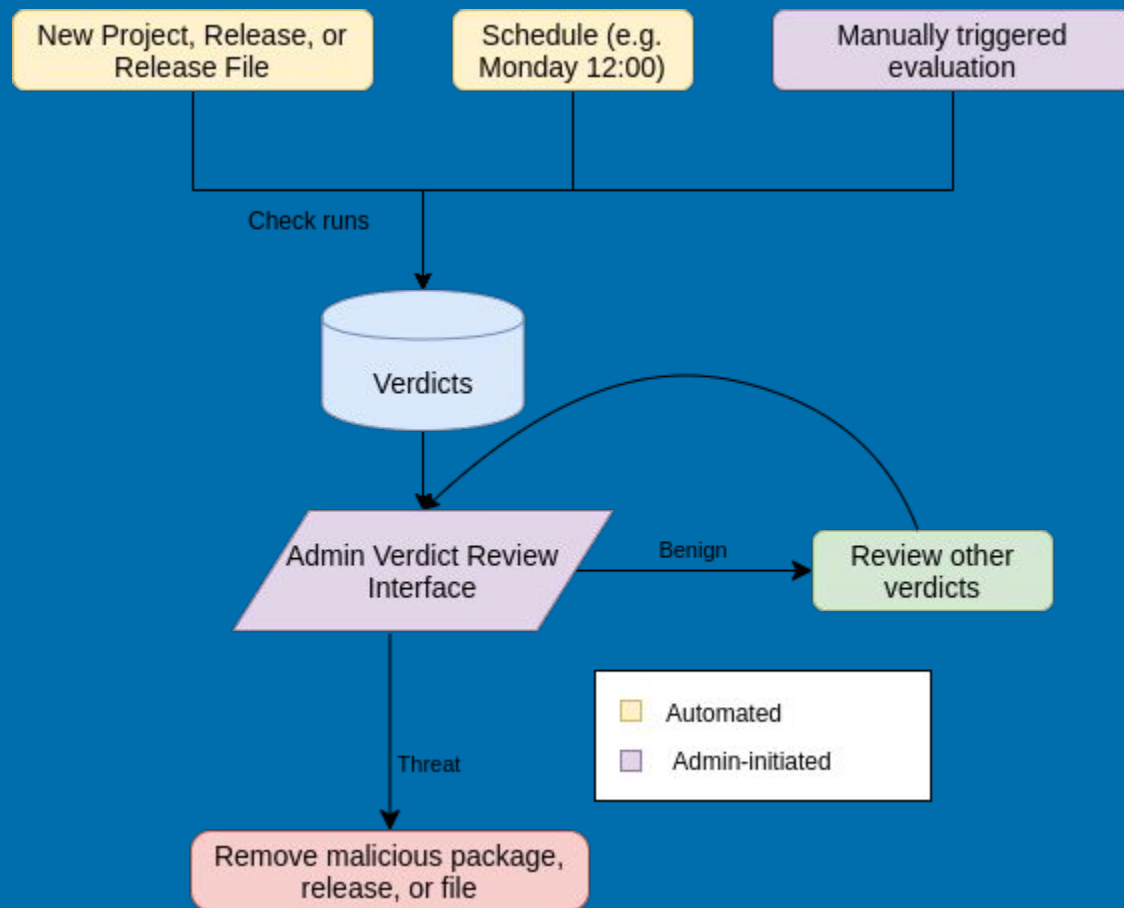
Scheduled Checks

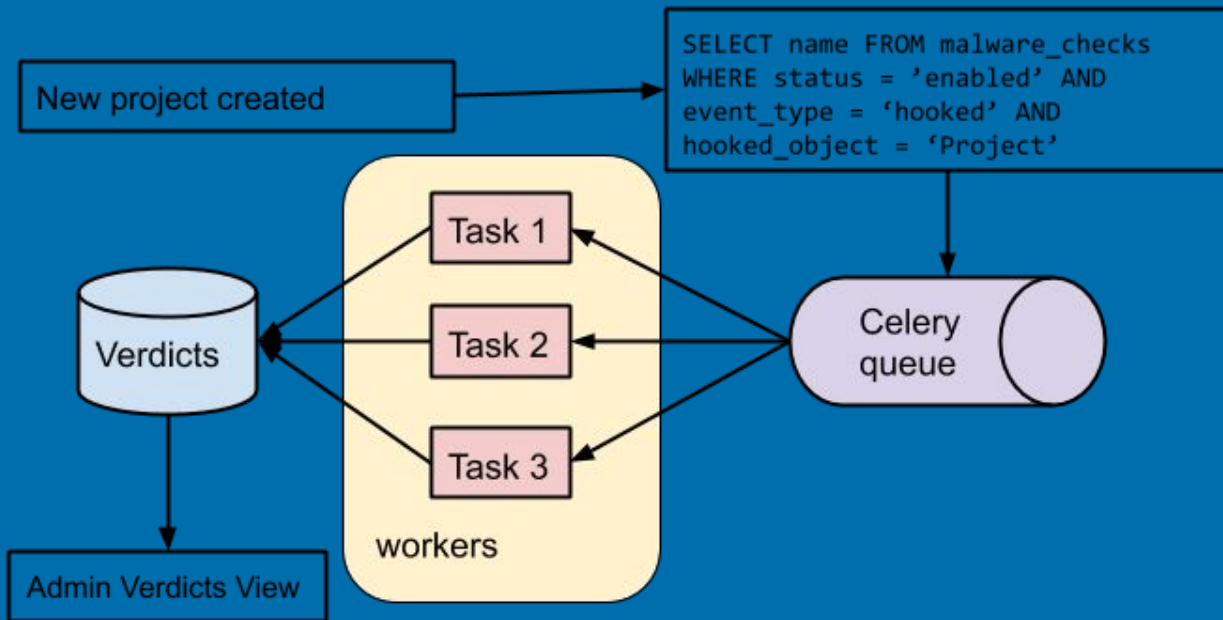
The maintainer of a popular package disabled 2-factor authentication and then transfers ownership of the popular package to another user

A low-reputation user registers a new package that has a similar name to a very well-established package

PackageTurnoverCheck

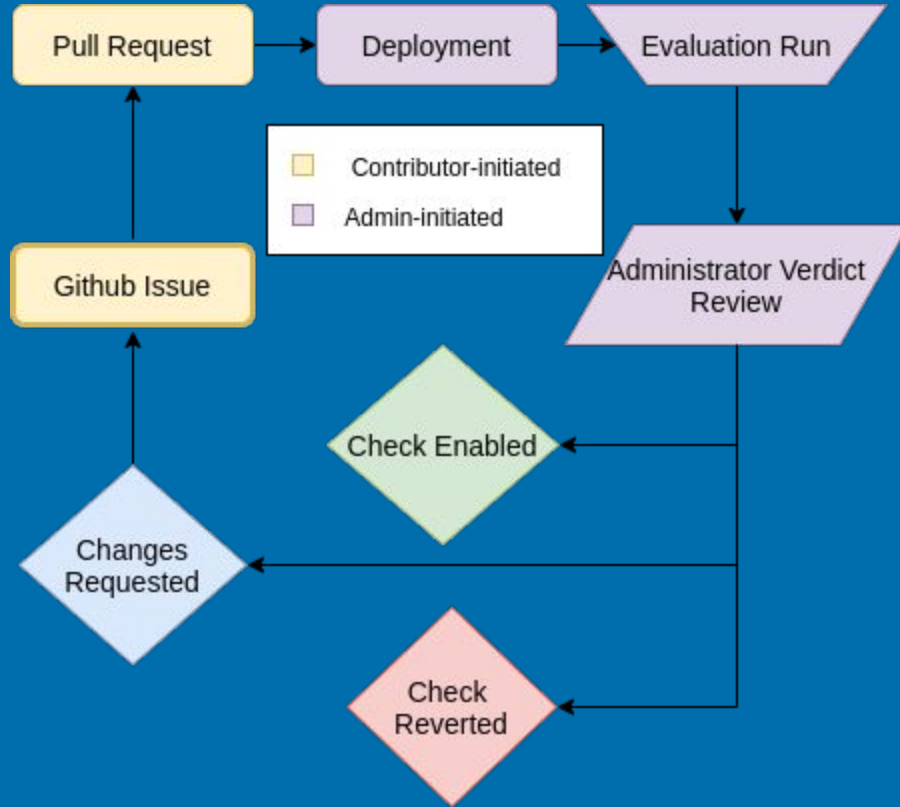
Threat vectors: A user changes or decreases the security of their account, transfers ownership to of their project to a newly created user.





Developing New Checks

- Download Warehouse
- Inherit the `MalwareCheckBase` class and write your check
- Change an environment variable, and deploy your check
- Enable it in the admin
- Execute it!



Admin View

<https://test.pypi.org/admin/>

Recap

<https://warehouse.pypa.io/development/malware-checks/>

Tooling for automated detection of malware #7377

🔗 Merged ewdurbin merged 16 commits into master from malware-detection 23 days ago

💬 Conversation 0

🔗 Commits 16

📄 Checks 0

📄 Files changed 59

+4,174 -4



ewdurbin commented on Feb 11

Member

+ 😊 ...

Design and implementation work by @xmuno, example checks by @woodruffw.



3



2

Reviewers



di

Assignees

No one assigned

Labels

None yet

Projects

None yet



xmuno mentioned this pull request on Feb 11

Automated detection of malware: add documentation. Fixes #7095.

#7369

🔗 Merged



di self-requested a review 27 days ago

How to build a custom SIEM in 4,174 lines of code, or less!

Cristina Muñoz

How to quit Big Tech and bootstrap your own startup

Cristina Muñoz

Questions? Comments?

—

[hmu hi@xmunoz.com](mailto:hmuhi@xmunoz.com)