# Supply Chain Shenanigans: Evil npm & shady NuGet

Todor Todorov
@totollygeek
Payhawk

# todor@defCamp:~$ whoami

- Senior Software Engineer @ **Payhawk**;
- **Infosec** junkie;
- **Clean** code fanatic;
- **DevOps** evangelist;
- Speaker;
- Father of **3 boys**;
- Karaoke **enthusiast**;

Payhawk


nuget


python
Package
Index

# NPM supply-chain attack impacts hundreds of websites and apps

By **Sergiu Gatlan**

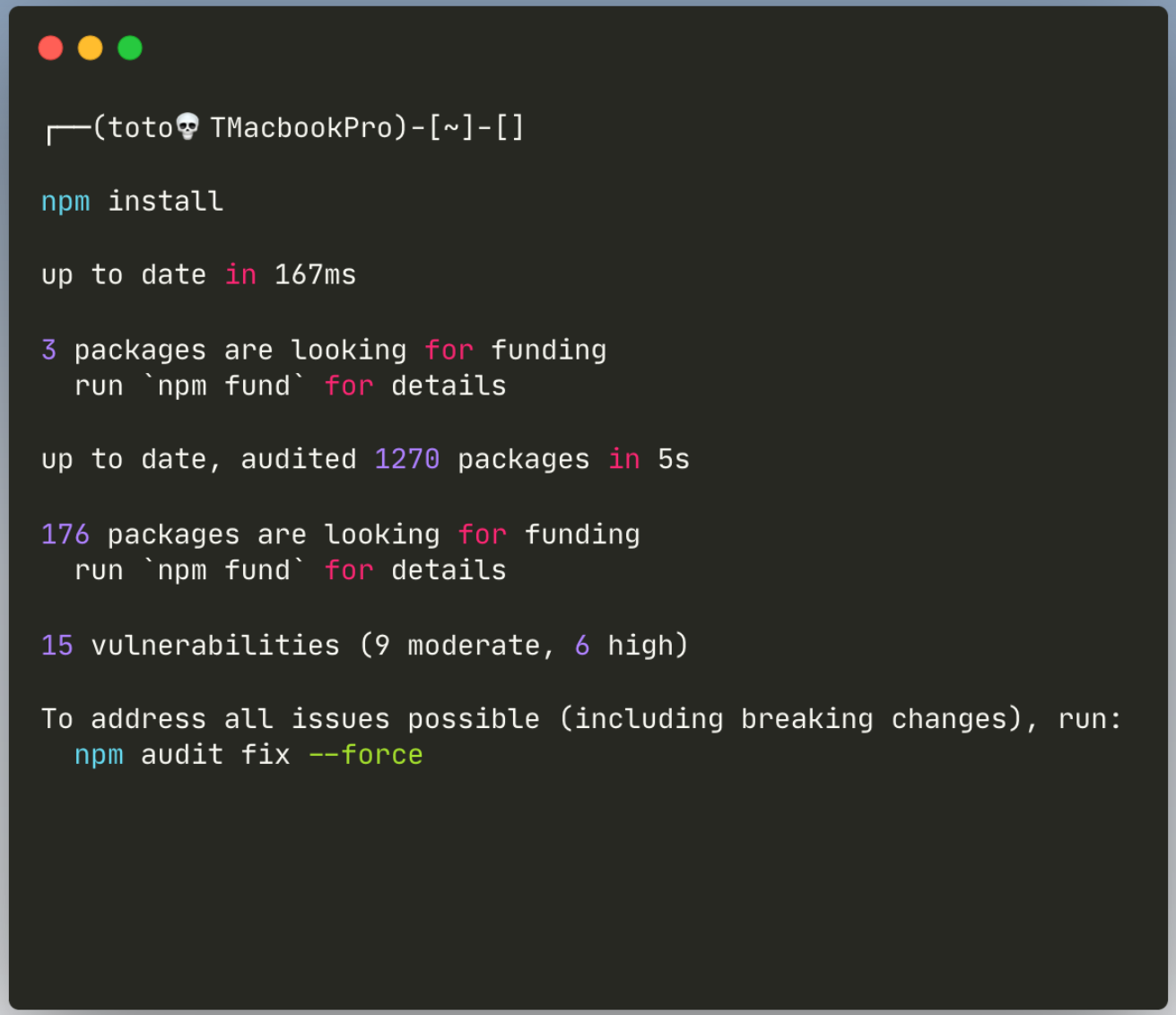
July 5, 2022 01:55 PM 2

# Npm Supply Chain Attack Targets Germany-based Companies with Dangerous Backdoor Malware

The JFrog Security Research team identified and quickly disclosed new npm malicious packages aimed at compromising leading industrial organizations

By Andrey Polkovnychenko and Shachar Menashe | May 10, 2022
9 min read

SHARE:

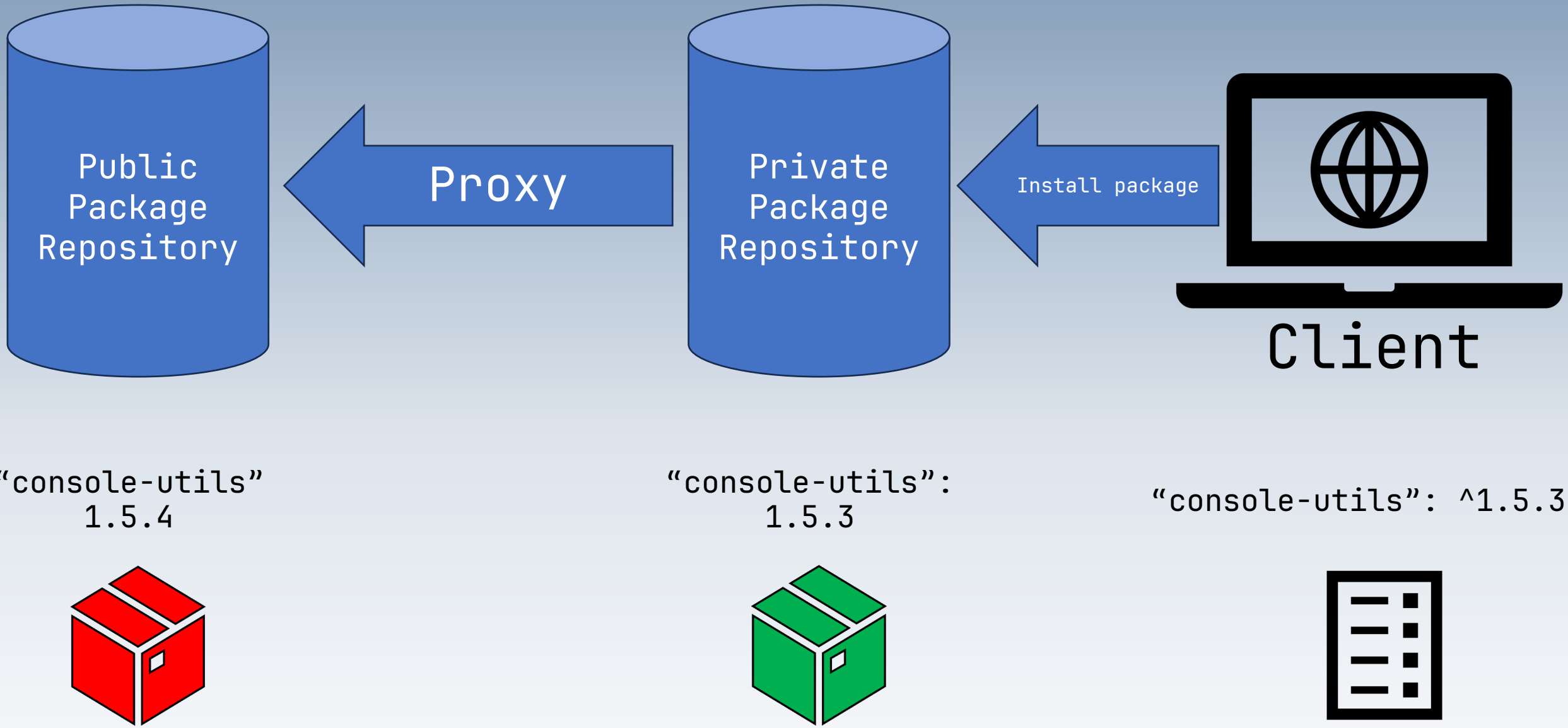

┌──(toto💀 TMacbookPro)-[~]-[]
npm install
up to date in 167ms
3 packages are looking for funding
run `npm fund` for details
up to date, audited 1270 packages in 5s
176 packages are looking for funding
run `npm fund` for details
15 vulnerabilities (9 moderate, 6 high)
To address all issues possible (including breaking changes), run:
npm audit fix --force

```
15 vulnerabilities (9 moderate, 6 high)
```

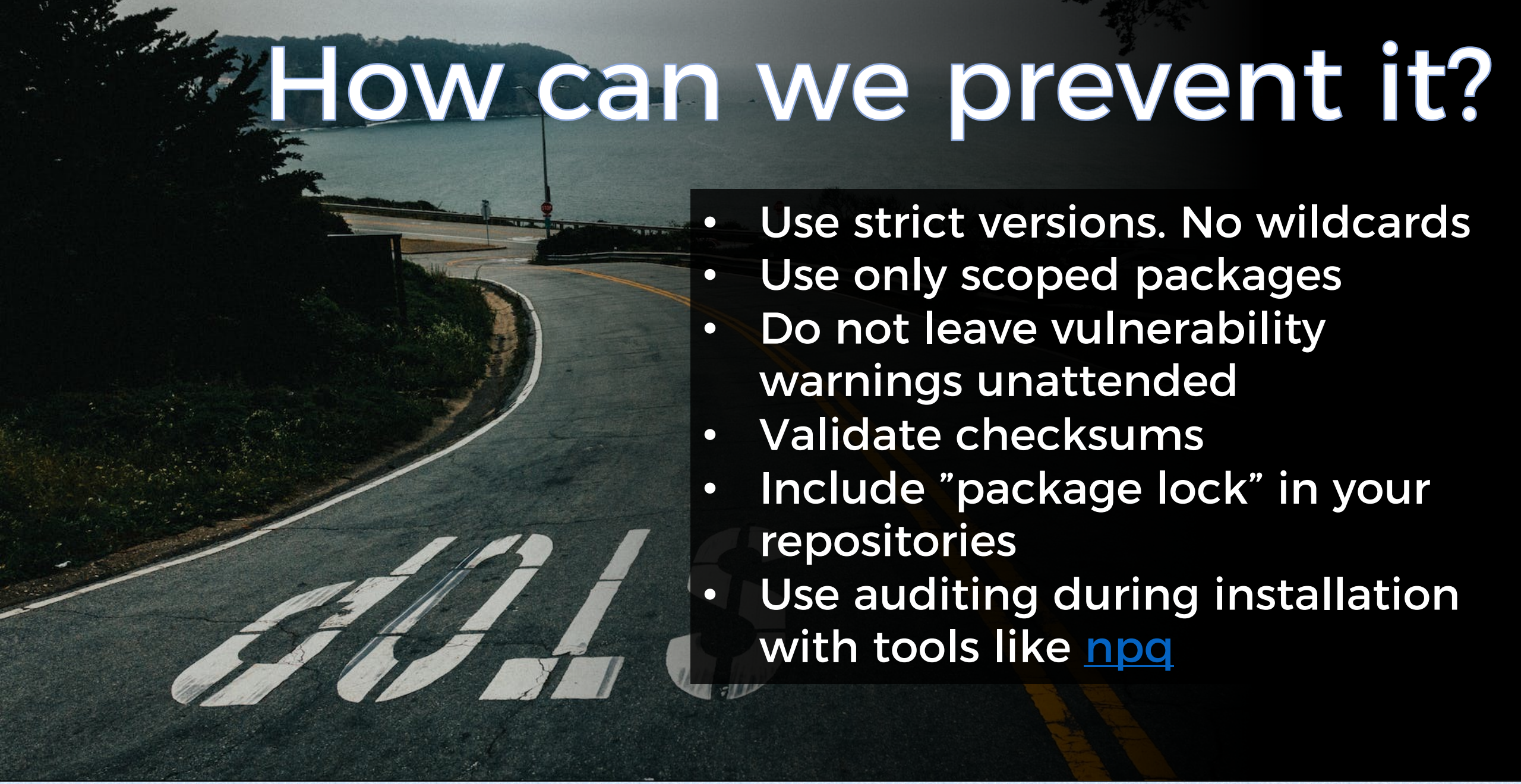

npm

# Types of attacks

# **npm substitution** (dependency confusion)


Public
Package
Repository
Proxy
Private
Package
Repository
Install package
Client
“console-utils”
1.5.4
“console-utils”:
1.5.3
“console-utils”: ^1.5.3

# How can we prevent it?



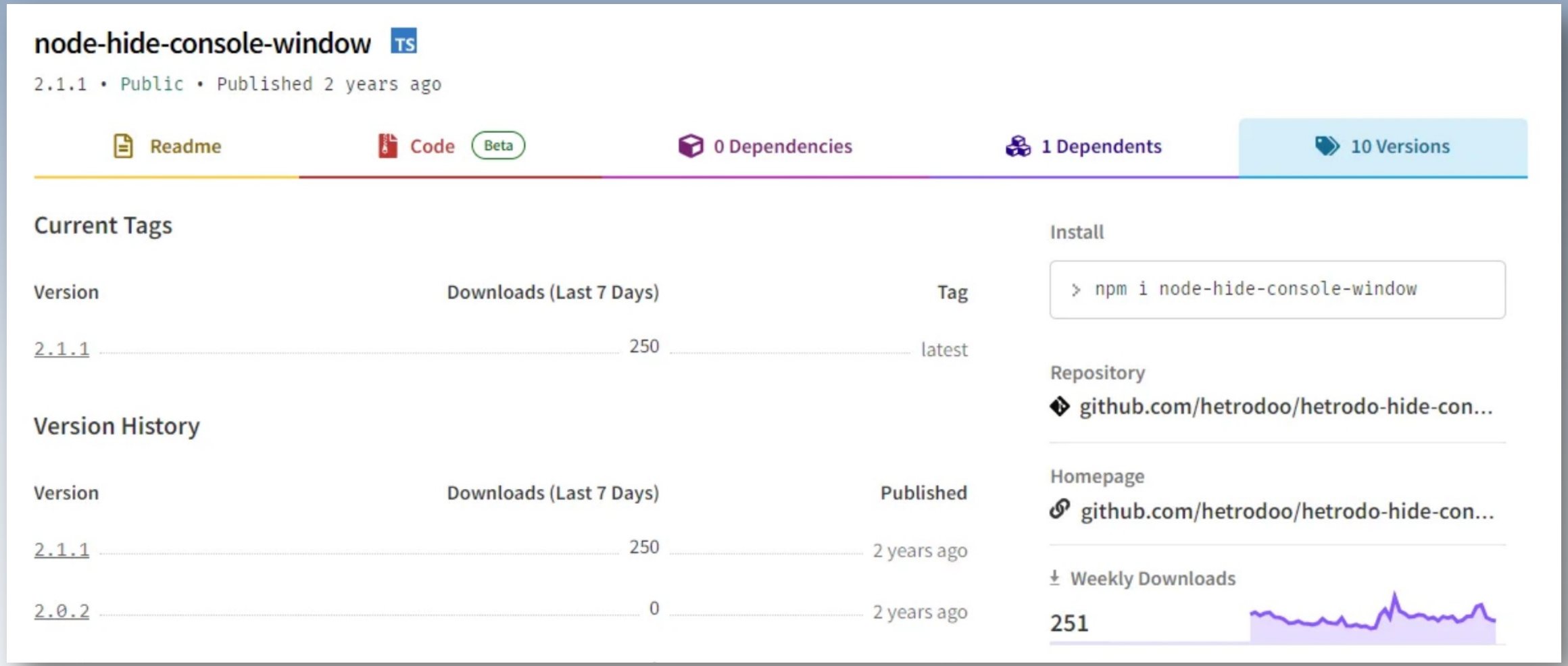
- Use strict versions. No wildcards
- Use only scoped packages
- Do not leave vulnerability warnings unattended
- Validate checksums
- Include ”package lock” in your repositories
- Use auditing during installation with tools like npq

# typosquatting

Threat Research | October 4, 2023

# Typosquatting campaign delivers r77 rootkit via npm

ReversingLabs discovered that one “s” was all that separated a legit npm package from a malicious twin that delivered the r77 rootkit — and was downloaded more than 700 times.


node-hide-console-window
TS
2.1.1 • Public • Published 2 years ago
Readme
Code
Beta
0 Dependencies
1 Dependents
10 Versions
Current Tags
Version
Downloads (Last 7 Days)
Tag
2.1.1
250
latest
Version History
Version
Downloads (Last 7 Days)
Published
2.1.1
250
2 years ago
2.0.2
0
2 years ago
Install
> npm i node-hide-console-window
Repository
github.com/hetrodoo/hetrodo-hide-con...
Homepage
github.com/hetrodoo/hetrodo-hide-con...
Weekly Downloads
251

# node-hide-console-windows

0.0.1-security • Public • Published 2 months ago

Readme | Code Beta | 0 Dependencies | 0 Dependents | 1 Versions

## Security holding package

This package contained malicious code and was removed from the registry by the npm security team. A placeholder was published to ensure users are not affected in the future.

Please refer to www.npmjs.com/advisories?search=node-hide-console-windows for more information.

### Keywords

none

Install

```
npm i node-hide-console-windows
```

Weekly Downloads

0

Version
0.0.1-security

License
none

Unpacked Size
456 B

Total Files
2

# node-hide-console-window

2.2.0 • Public • Published a month ago

# node-hide-console-windows

0.0.1-security • Public • Published 2 months ago

# localforage-memoryStorageDriver

0.9.2 • Public • Published 7 years ago

# localforage-memorystoragedriver

0.0.1-security • Public • Published 2 years ago



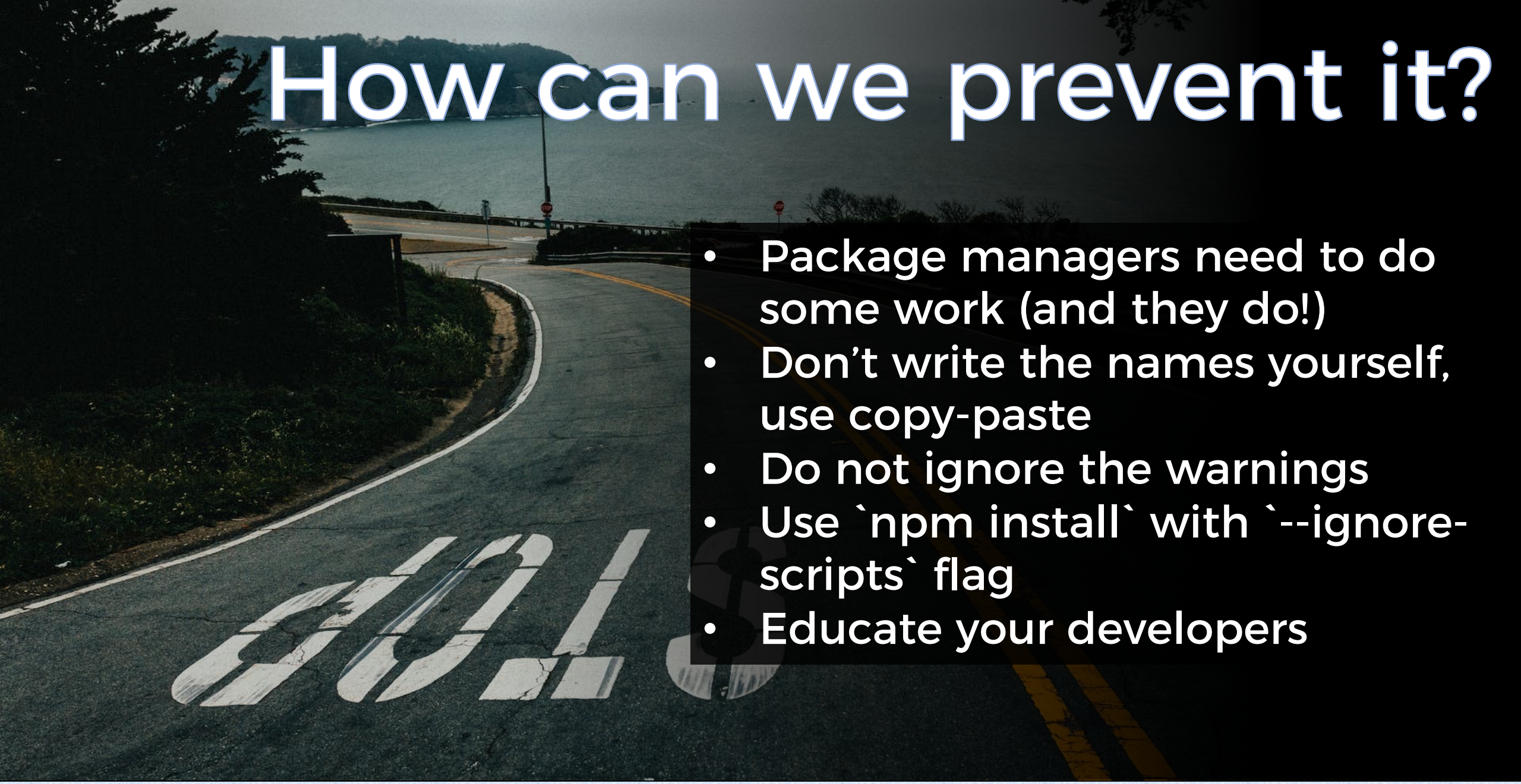
source: [Checkmarx Blog]

# `crossenv` malware on the npm registry

On August 1, a user notified us via Twitter that a package with a name very similar to the popular `cross-env` package was sending environment variables from its installation context out to npm.hacktask.net. We investigated this report immediately and took action to remove the package. Further investigation led us to remove about 40 packages in total.

```
babelcli:        42
cross-env.js:    43
crossenv:        679
d3.js:           72
fabric-js:       46
ffmepg:          44
gruntcli:        67
http-proxy.js:   41
jquery.js:       136
```

| | |
|---|---|
| babelcli: | 42 |
| cross-env.js: | 43 |
| **crossenv:** | **679** |
| d3.js: | 72 |
| fabric-js: | 46 |
| ffmepg: | 44 |
| gruntcli: | 67 |
| http-proxy.js: | 41 |
| jquery.js: | 136 |



# How can we prevent it?

- Package managers need to do some work (and they do!)
- Don’t write the names yourself, use copy-paste
- Do not ignore the warnings
- Use `npm install` with `--ignore-scripts` flag
- Educate your developers

# Open-source dependency injection

# I'm harvesting credit card numbers and passwords from your site. Here's how.

David Gilbertson · Follow

10 min read · Jan 6, 2018

224K 306

# Step 1

Create a seemingly harmless package with the Trojan horse inside...

People love pretty colours — it's what separates us from dogs — so I wrote a package that lets you log to the console in any colour.

```
158     log.tomato('I am tomato');
159     log.chocolate('I am chocolate');
160     log.cornflowerblue('I am cornflowerblue');
161     log.darkcyan('I am darkcyan');
162     log.goldenrod('I am goldenrod');
```

{} Line 163, Column 6

Console | Animations | Rendering | Search | What'

top | Filter

```
Console was cleared
I am tomato
I am chocolate
I am cornflowerblue
I am darkcyan
I am goldenrod
```

# Step 2

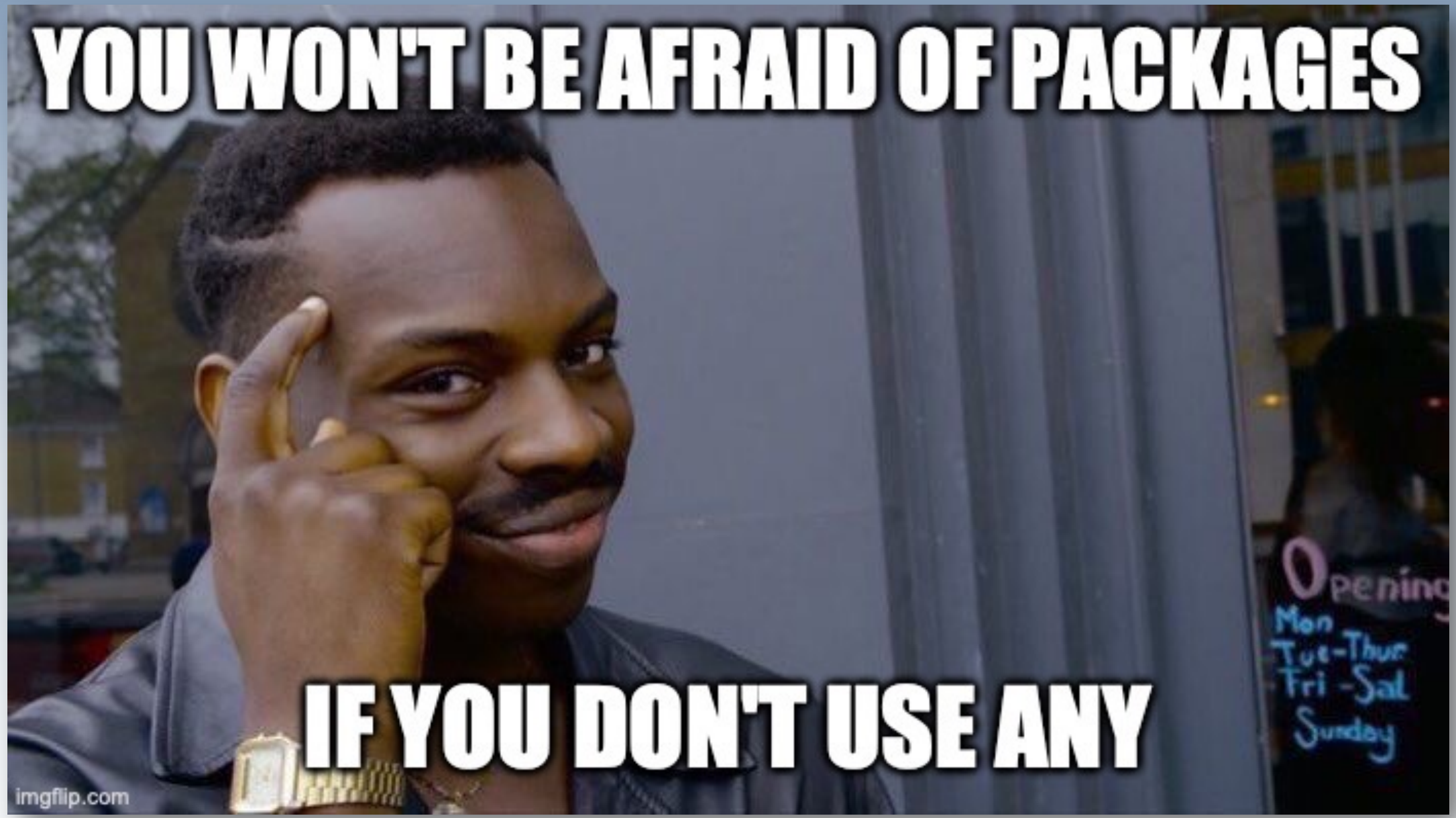
Open PRs in hundreds of frontend packages: “Hey I fixed issue X and added some logging”

# Step 3

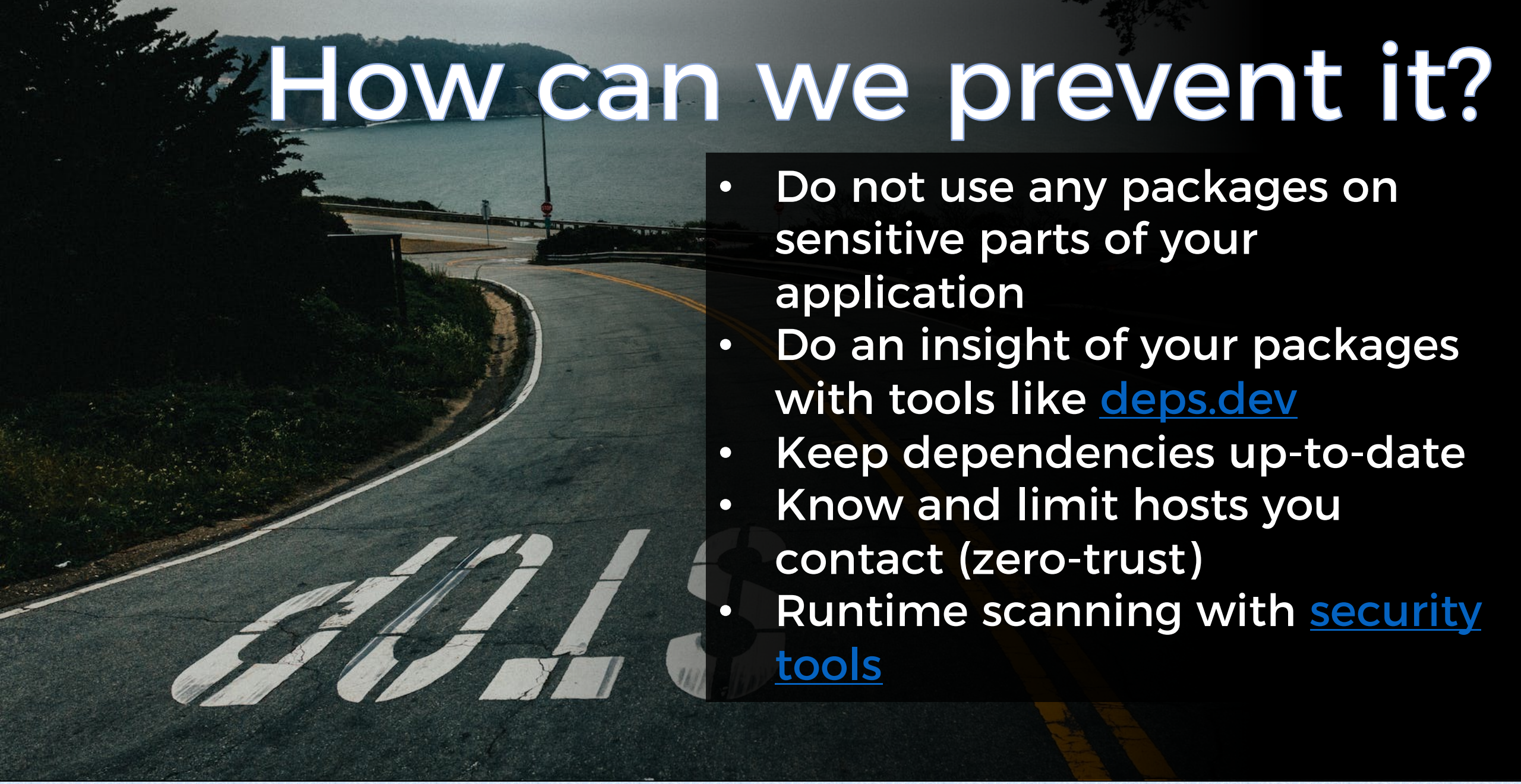
Profit !!!

# How can we prevent it?

# How can we prevent it?


YOU WON'T BE AFRAID OF PACKAGES
IF YOU DON'T USE ANY
imgflip.com
Opening
Mon
Tue-Thur
Fri-Sat
Sunday

# How can we prevent it?



- Do not use any packages on sensitive parts of your application
- Do an insight of your packages with tools like deps.dev
- Keep dependencies up-to-date
- Know and limit hosts you contact (zero-trust)
- Runtime scanning with security tools


TELL ME HOW
YOU DON'T USE
EXTERNAL DEPENDENCIES
imgflip.com

“Open-source projects have an average of **180** package dependencies.”

- GitHub State of the Octoverse Report, 2019

# Visual Studio Code

Visual Studio Code

ELECTRON

# electron

27.0.3 • Public • Published 3 days ago

Readme | Code Beta | 3 Dependencies | 1,256 Dependents | 1,107 Versions



📝 Available Translations: 🇨🇳 🇧🇷 🇪🇸 🇯🇵 🇷🇺 🇫🇷 🇺🇸 🇩🇪. View these docs in other languages on our Crowdin project.

The Electron framework lets you write cross-platform desktop applications using JavaScript, HTML and CSS. It is based on Node.js and Chromium and is used by the Atom editor and many other apps.

Follow @electronjs on Twitter for important announcements.

This project adheres to the Contributor Covenant code of conduct. By participating, you are expected to uphold this code. Please report unacceptable behavior to coc@electronjs.org.

## Installation

To install prebuilt Electron binaries, use `npm`. The preferred method is to install Electron as a development dependency in your app:

```
npm install electron --save-dev
```

Install

```
npm i electron
```

Repository
github.com/electron/electron

Homepage
github.com/electron/electron#readme

Weekly Downloads
635,911

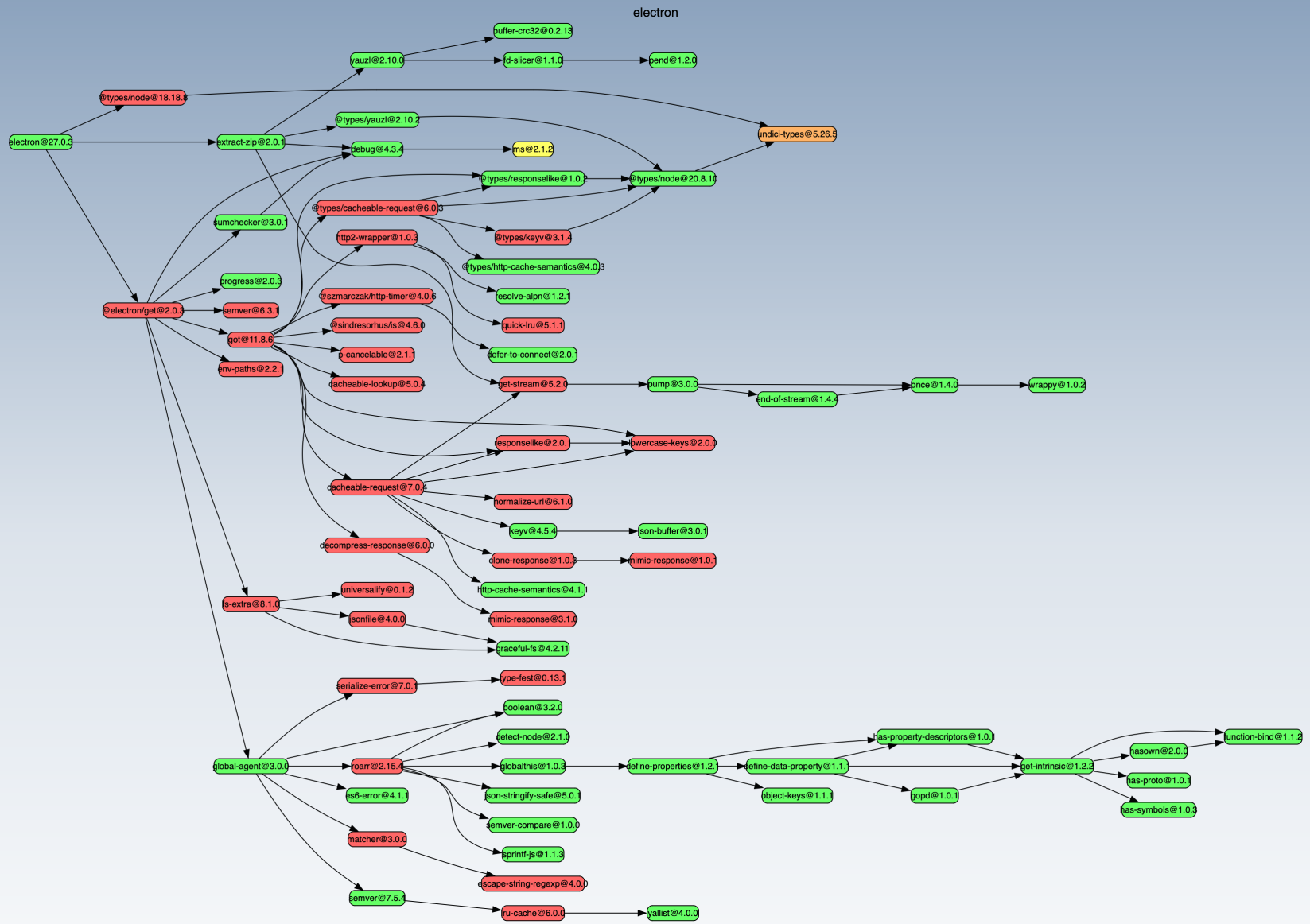
| Version | License |
|---|---|
| 27.0.3 | MIT |

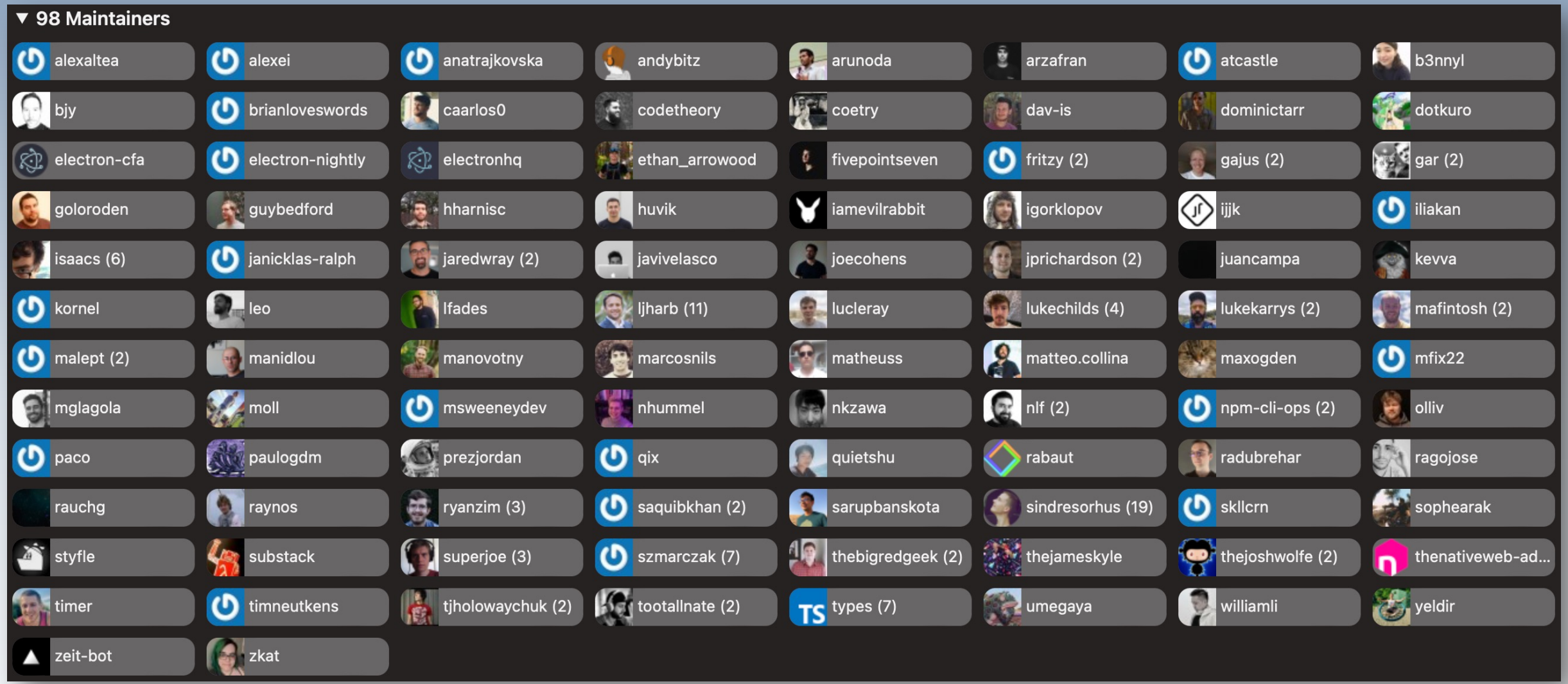
| Unpacked Size | Total Files |
|---|---|
| 828 kB | 8 |

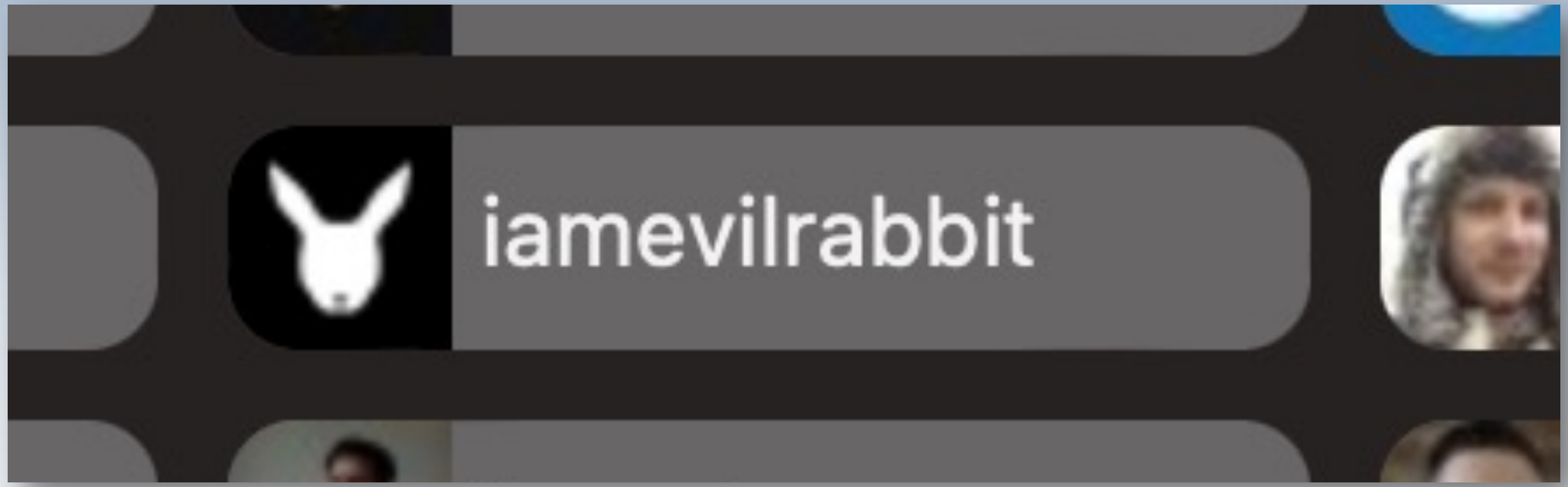
| Issues | Pull Requests |
|---|---|
| 801 | 71 |

Last publish
2 days ago


electron
TS
27.0.3 • Public • Published 3 days ago
Readme
Code
Beta
3 Dependencies
1,256 Dependents
1,107 Versions
ELECTRON
Install
npm i electron

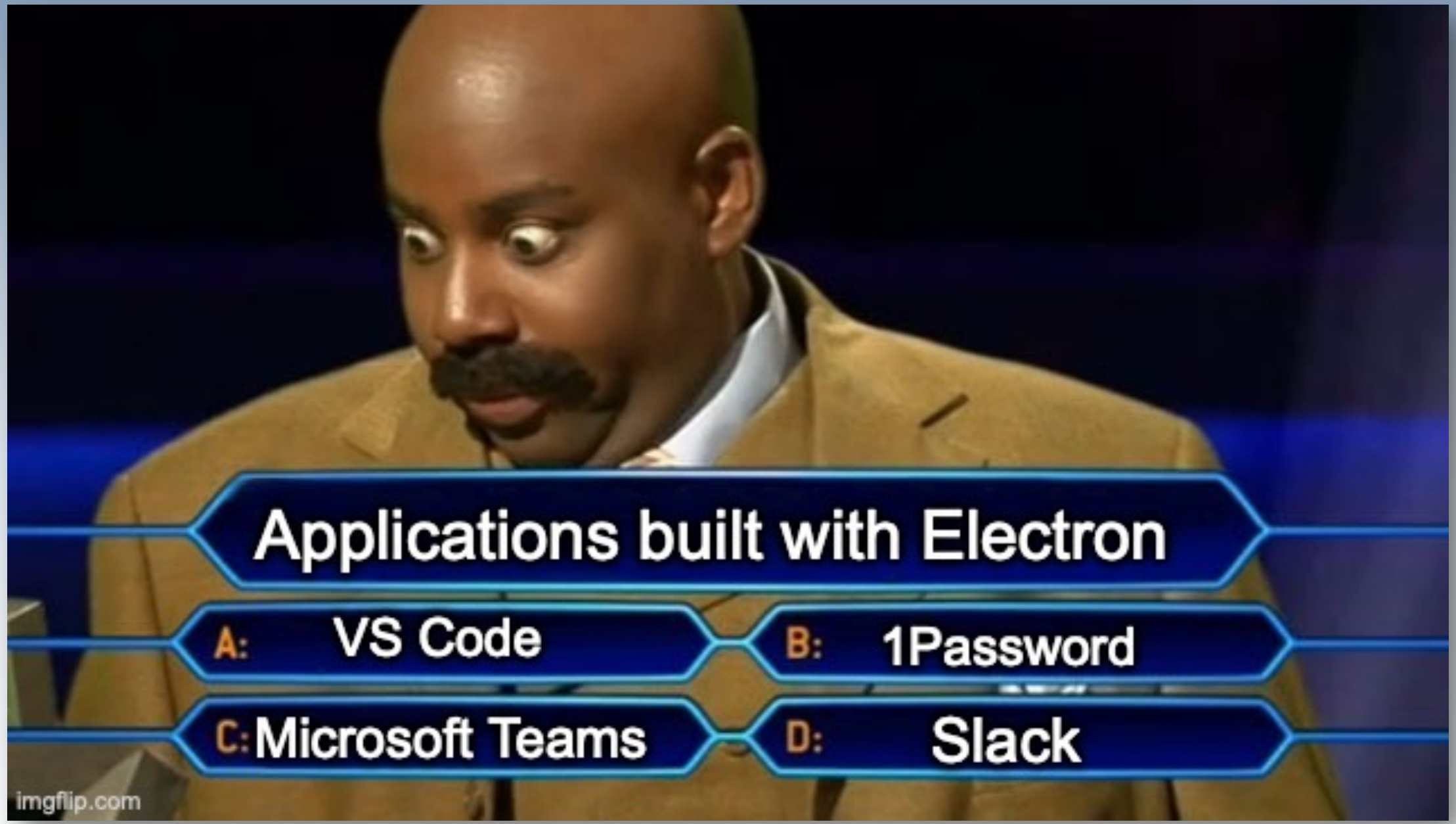

electron
buffer-crc32@0.2.13
yauzl@2.10.0
fd-slicer@1.1.0
pend@1.2.0
@types/node@18.18.8
electron@27.0.3
extract-zip@2.0.1
@types/yauzl@2.10.2
undici-types@5.26.5
debug@4.3.4
ms@2.1.2
@types/responselike@1.0.2
@types/node@20.8.10
@types/cacheable-request@6.0.3
sumchecker@3.0.1
@types/keyv@3.1.4
http2-wrapper@1.0.3
@types/http-cache-semantics@4.0.3
progress@2.0.3
@electron/get@2.0.3
semver@6.3.1
@szmarczak/http-timer@4.0.6
resolve-alpn@1.2.1
@sindresorhus/is@4.6.0
quick-lru@5.1.1
got@11.8.6
p-cancelable@2.1.1
defer-to-connect@2.0.1
env-paths@2.2.1
cacheable-lookup@5.0.4
get-stream@5.2.0
pump@3.0.0
end-of-stream@1.4.4
once@1.4.0
wrappy@1.0.2
responselike@2.0.1
lowercase-keys@2.0.0
cacheable-request@7.0.4
normalize-url@6.1.0
keyv@4.5.4
json-buffer@3.0.1
decompress-response@6.0.0
clone-response@1.0.3
mimic-response@1.0.1
http-cache-semantics@4.1.1
mimic-response@3.1.0
universalify@0.1.2
fs-extra@8.1.0
jsonfile@4.0.0
graceful-fs@4.2.11
type-fest@0.13.1
serialize-error@7.0.1
boolean@3.2.0
detect-node@2.1.0
global-agent@3.0.0
boolean@3.2.0
globalthis@1.0.3
define-properties@1.2.1
define-data-property@1.1.1
has-property-descriptors@1.0.1
get-intrinsic@1.2.2
function-bind@1.1.2
hasown@2.0.0
has-proto@1.0.1
has-symbols@1.0.3
gopd@1.0.1
object-keys@1.1.1
es6-error@4.1.1
json-stringify-safe@5.0.1
semver-compare@1.0.0
matcher@3.0.0
sprintf-js@1.1.3
escape-string-regexp@4.0.0
semver@7.5.4
lru-cache@6.0.0
yallist@4.0.0


▼ 98 Maintainers
alexaltea
alexei
anatrajkovska
andybitz
arunoda
arzafran
atcastle
b3nnyl
bjy
brianloveswords
caarlos0
codetheory
coetry
dav-is
dominictarr
dotkuro
electron-cfa
electron-nightly
electronhq
ethan_arrowood
fivepointseven
fritzy (2)
gajus (2)
gar (2)
goloroden
guybedford
hharnisc
huvik
iamevilrabbit
igorklopov
ijjk
iliakan
isaacs (6)
janicklas-ralph
jaredwray (2)
javivelasco
joecohens
jprichardson (2)
juancampa
kevva
kornel
leo
lfades
ljharb (11)
lucleray
lukechilds (4)
lukekarrys (2)
mafintosh (2)
malept (2)
manidlou
manovotny
marcosnils
matheuss
matteo.collina
maxogden
mfix22
mglagola
moll
msweeneydev
nhummel
nkzawa
nlf (2)
npm-cli-ops (2)
olliv
paco
paulogdm
prezjordan
qix
quietshu
rabaut
radubrehar
ragojose
rauchg
raynos
ryanzim (3)
saquibkhan (2)
sarupbanskota
sindresorhus (19)
skllcrn
sophearak
styfle
substack
superjoe (3)
szmarczak (7)
thebigredgeek (2)
thejameskyle
thejoshwolfe (2)
thenativeweb-ad...
timer
timneutkens
tjholowaychuk (2)
tootallnate (2)
types (7)
umegaya
williamli
yeldir
zeit-bot
zkat


iamevilrabbit

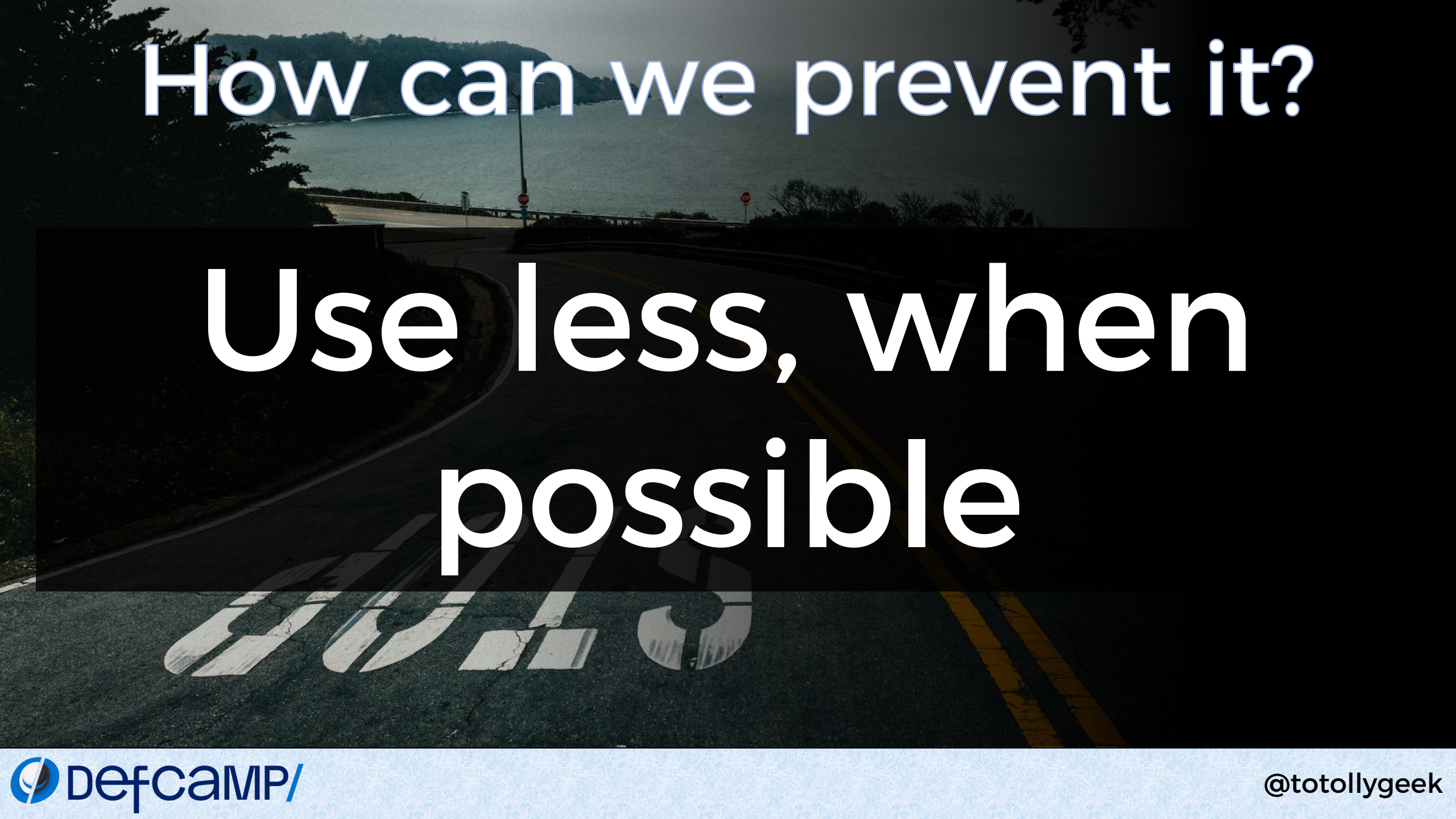
# Don’t trust people on the Internet

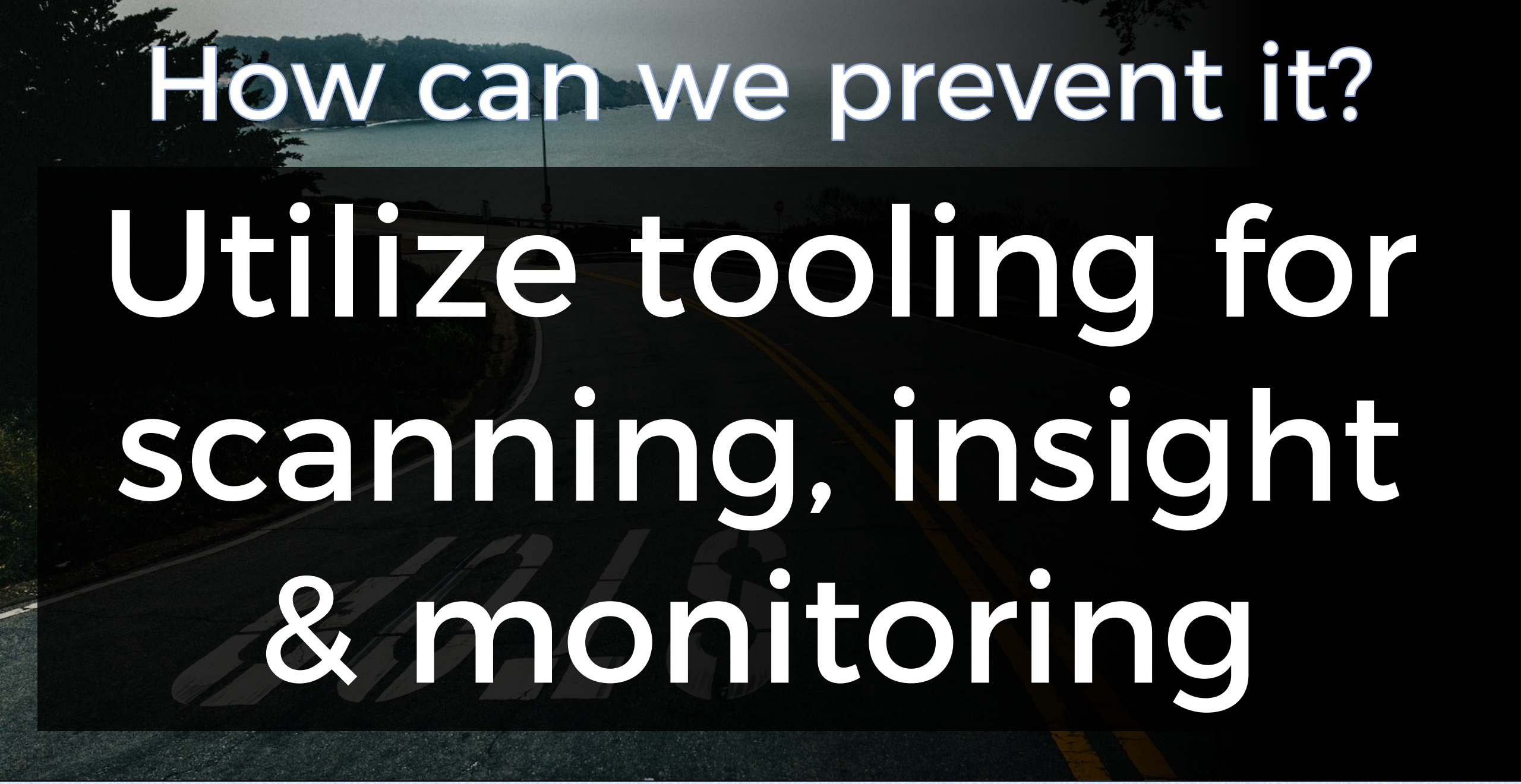

I DON'T
USE EXTERNAL
DEPENDENCIES
VS CODE
WITH
ELECTRON
imgflip.com


Applications built with Electron
A: VS Code
B: 1Password
C: Microsoft Teams
D: Slack
imgflip.com


TAKE
A
CHILL
PILL


How can we prevent it?
Know your depencencies


How can we prevent it?
Use less, when possible


How can we prevent it?
Utilize tooling for scanning, insight & monitoring


How can we prevent it?
EDUCATE YOUR DEVELOPERS!

# Thank you!
# Where to find me?

- todor.todorov.bg
- x.com/totollygeek
- infosec.exchange/@totollygeek
- linkedin.com/in/totollygeek
- github.com/totollygeek

Image sources: pixabay Pexels imgflip rawpixel Unsplash