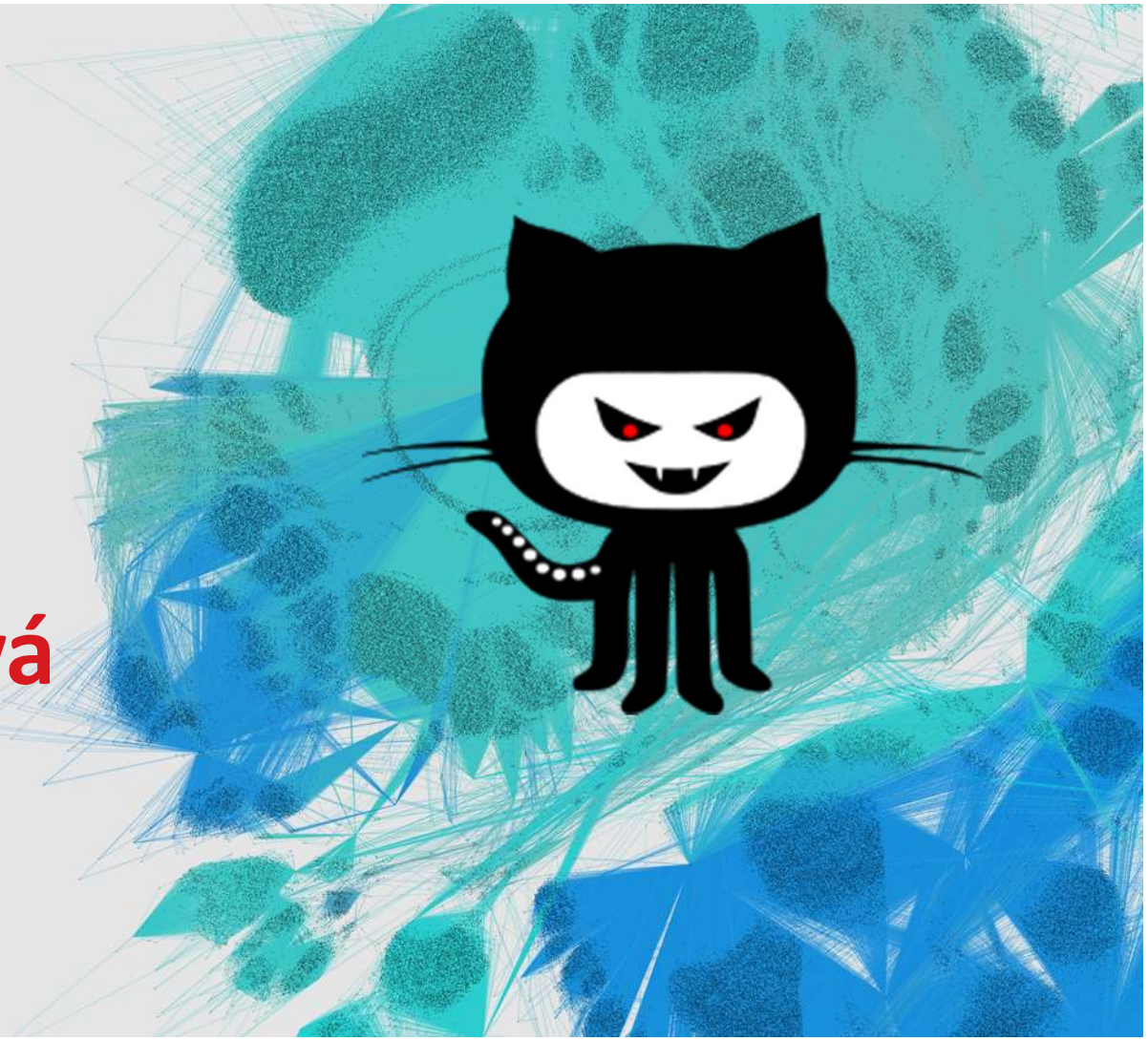
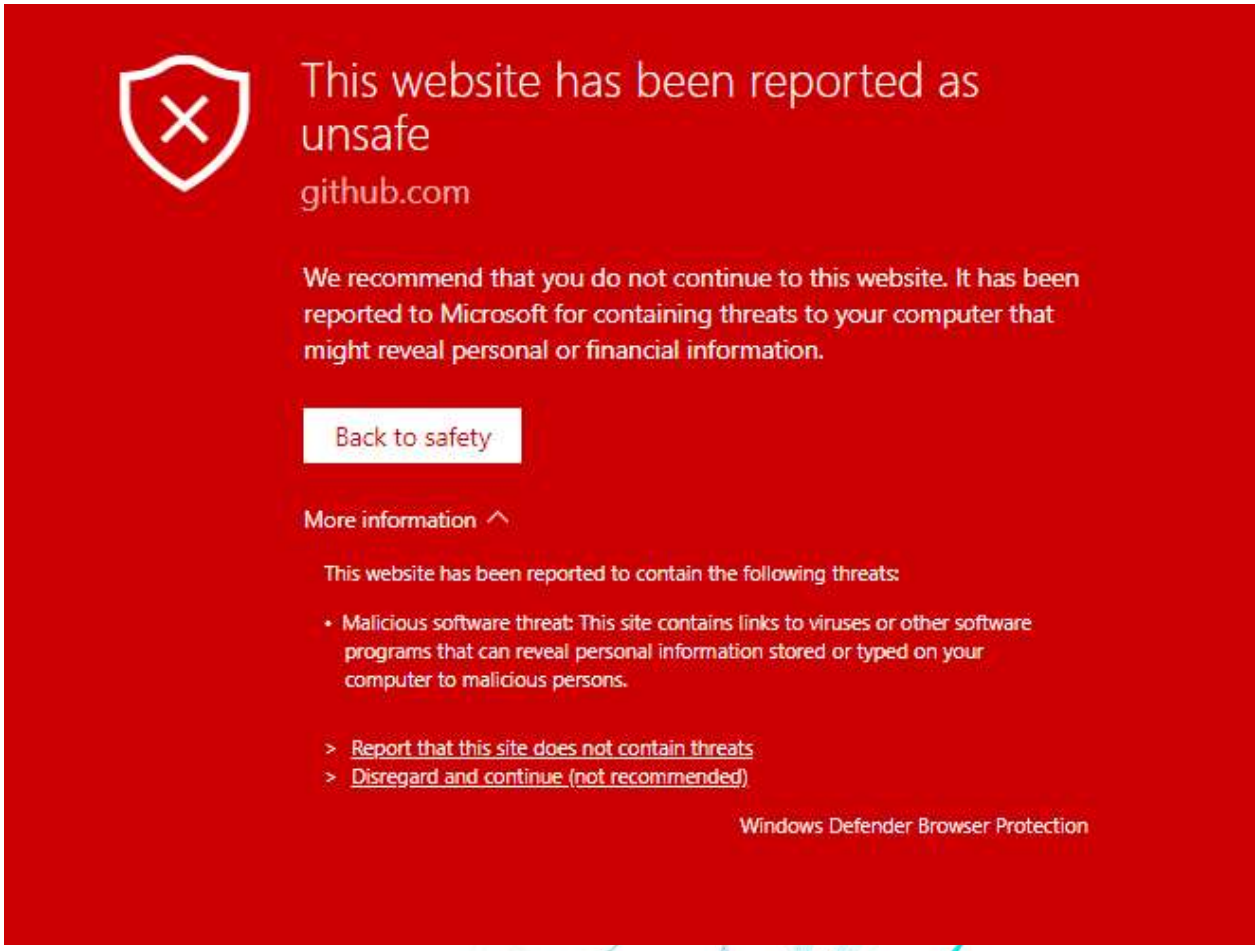
TREND MICRO

# Ďábel se skrývá v GitHubu (?)



Jiří Gogela

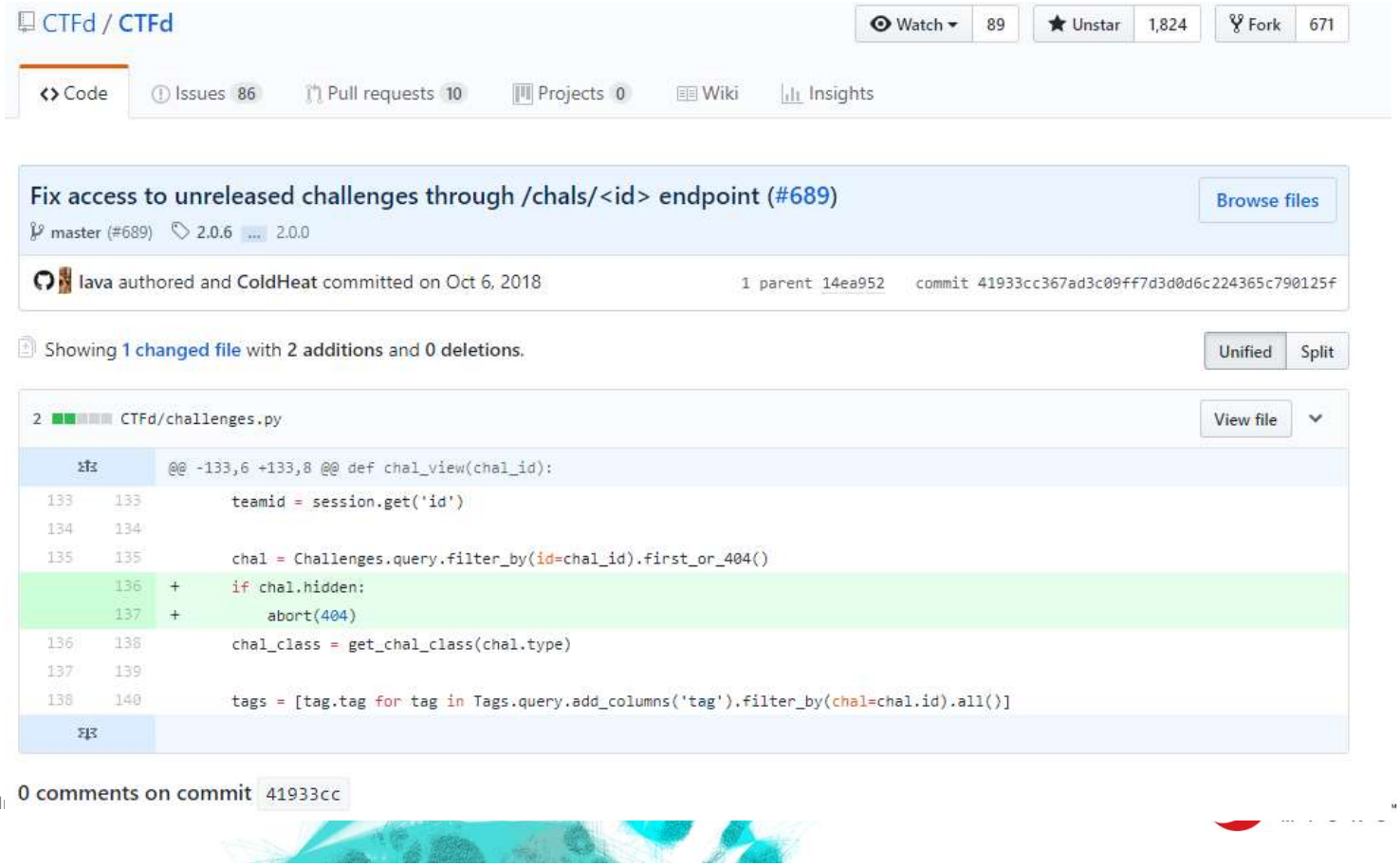
Europen 2019



# Motivace

- The Catch 2018
- CTFd
  - “Můžeme už řešit úkoly pro 2.kolo?“
  - ?...!!!!!!!!!!!

# Catched by enumeration…

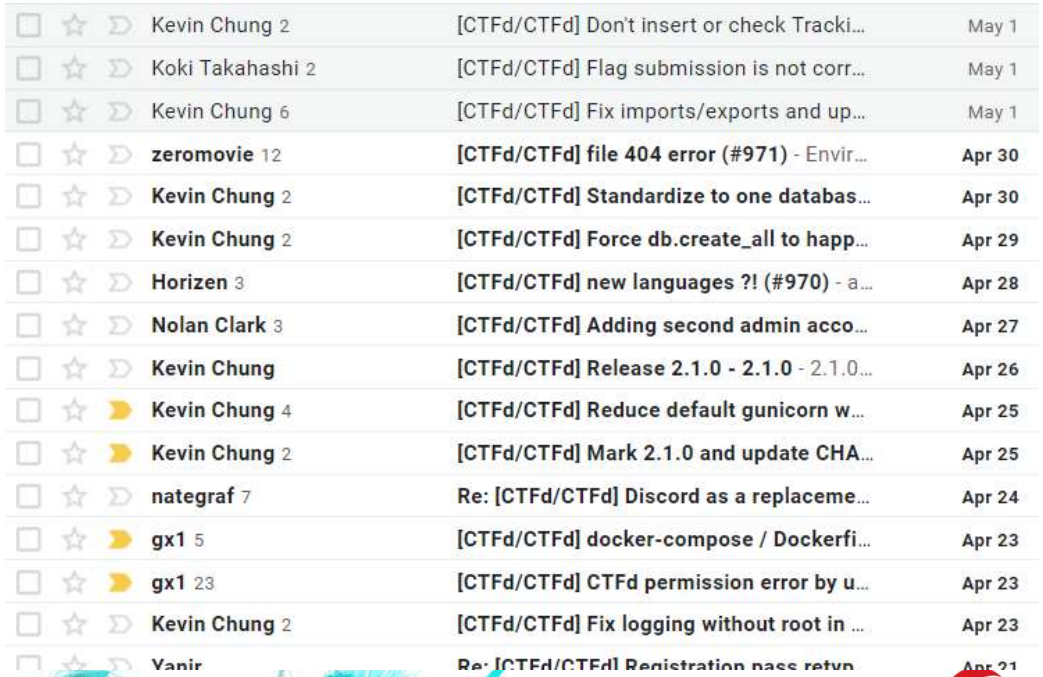


# Jak být v obraze?

- SECURITY.md
  - https://github.com/tensorflow/tensorflow/blob/master/SECURITY.md
- Watcher

# Jak být v obraze?

- Repository Watch



| | | |
|---|---|---|
| Kevin Chung 2 | [CTFd/CTFd] Don't insert or check Tracki... | May 1 |
| Koki Takahashi 2 | [CTFd/CTFd] Flag submission is not corr... | May 1 |
| Kevin Chung 6 | [CTFd/CTFd] Fix imports/exports and up... | May 1 |
| zeromovie 12 | [CTFd/CTFd] file 404 error (#971) - Envir... | Apr 30 |
| Kevin Chung 2 | [CTFd/CTFd] Standardize to one databas... | Apr 30 |
| Kevin Chung 2 | [CTFd/CTFd] Force db.create_all to happ... | Apr 29 |
| Horizen 3 | [CTFd/CTFd] new languages ?! (#970) - a... | Apr 28 |
| Nolan Clark 3 | [CTFd/CTFd] Adding second admin acco... | Apr 27 |
| Kevin Chung | [CTFd/CTFd] Release 2.1.0 - 2.1.0 - 2.1.0... | Apr 26 |
| Kevin Chung 4 | [CTFd/CTFd] Reduce default gunicorn w... | Apr 25 |
| Kevin Chung 2 | [CTFd/CTFd] Mark 2.1.0 and update CHA... | Apr 25 |
| nategraf 7 | Re: [CTFd/CTFd] Discord as a replaceme... | Apr 24 |
| gx1 5 | [CTFd/CTFd] docker-compose / Dockerfi... | Apr 23 |
| gx1 23 | [CTFd/CTFd] CTFd permission error by u... | Apr 23 |
| Kevin Chung 2 | [CTFd/CTFd] Fix logging without root in ... | Apr 23 |
| Yanir | Re: [CTFd/CTFd] Registration pass retyp | Apr 21 |

# Zranitelné závislosti

# Zranitelné závislosti

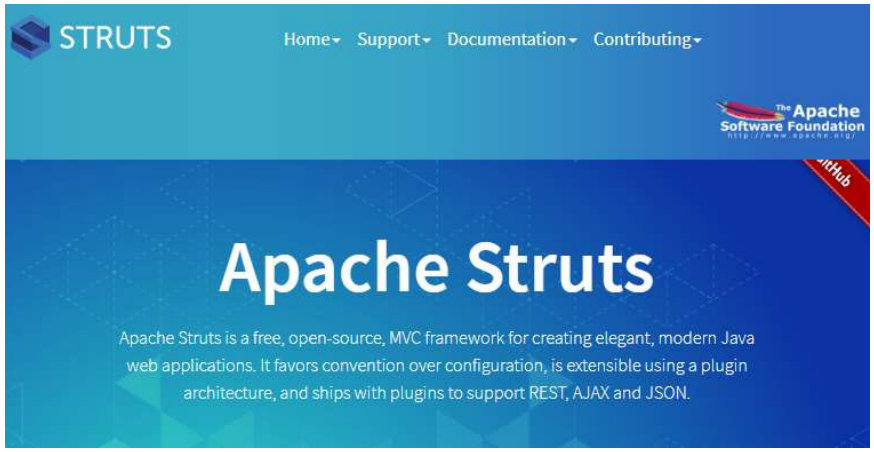
## GitHub's security alerts for vulnerable dependencies

GitHub tracks public vulnerabilities in packages from supported languages on MITRE's Common Vulnerabilities and Exposures (CVE) List. We also scan data in public commits on GitHub and use a combination of machine learning and human review to detect vulnerabilities that are not published in the CVE list.

When GitHub discovers or is notified of a new vulnerability, we identify public repositories (and private repositories that have opted in to vulnerability detection) that use the affected version of the dependency and send a security alert. By default, we send security alerts to owners and people with admin access in the affected repositories. You can also enable security alerts for additional people or teams working in organization-owned repositories. For more information, see "Managing alerts for vulnerable dependencies in your organization's repositories."

# Pokus s Apache Struts

- Co je Apache Struts?



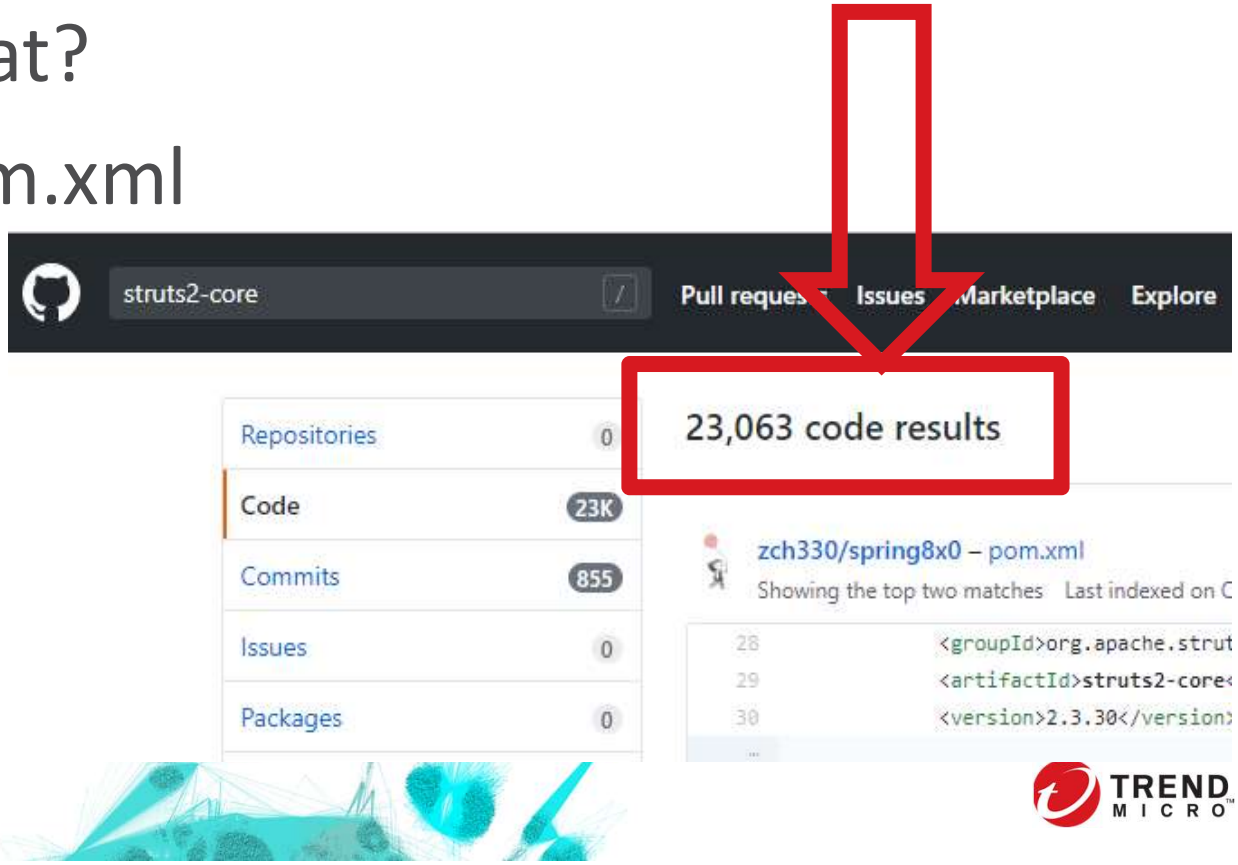
# Proč zrovna v Apache Struts

# RCE zranitelnosti s dostupnými exploity

- CVE-2017-5638
  - 2.3.x - 2.3.32 and 2.5. - 2.5.10.1
  - https://www.rapid7.com/db/modules/exploit/multi/http/struts2_content_type_ognl
- CVE-2017-9805
  - 2.1.2 - 2.3.33 and 2.5. - 2.5.12
  - https://www.rapid7.com/db/modules/exploit/multi/http/struts2_rest_xstream
- CVE-2017-9791
  - 2.3 – 2.3.32
  - https://www.rapid7.com/db/modules/exploit/multi/http/struts2_code_exec_showcase
- CVE-2018-11776
  - 2.3-2.3.33., 2.5-2.5.16
  - https://www.rapid7.com/db/modules/exploit/multi/http/struts2_namespace_ognl

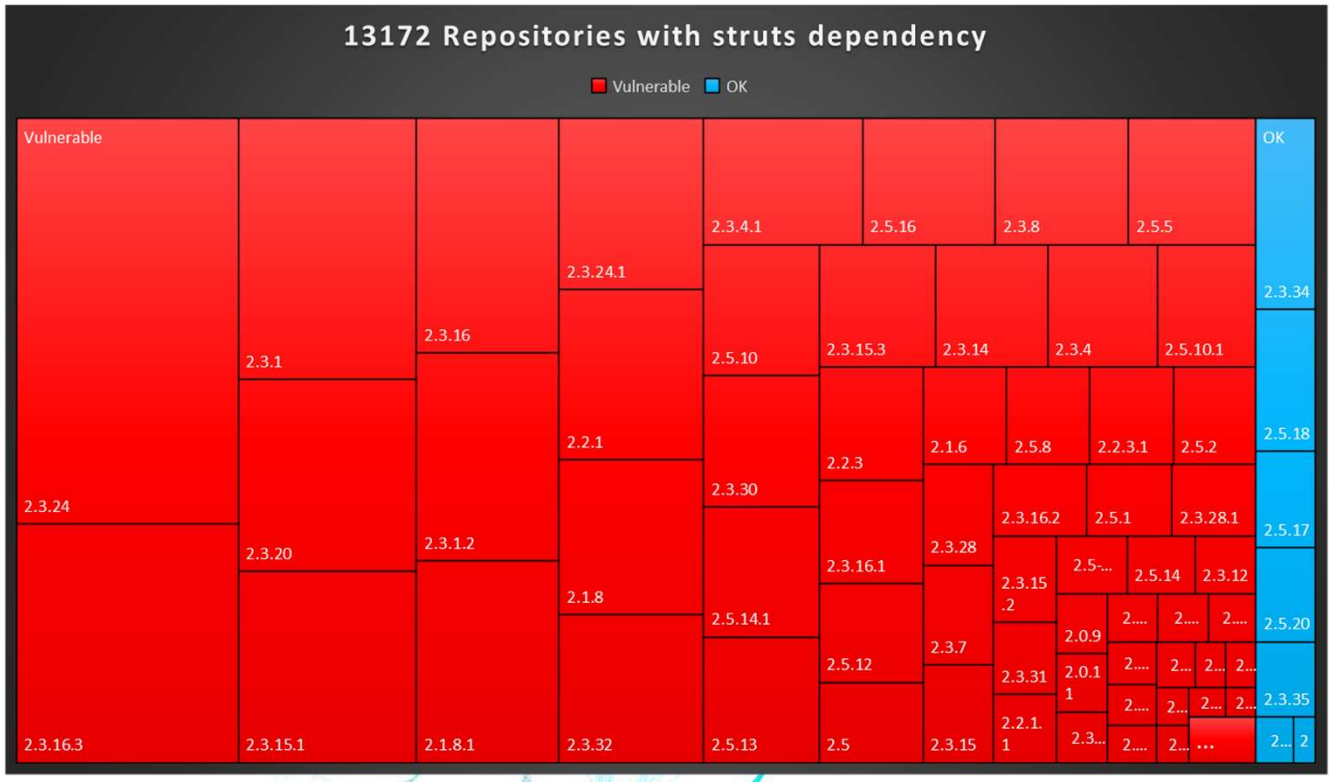
# Hledání v githubu...

- Jak detekovat?
- Maven - pom.xml
- Github API



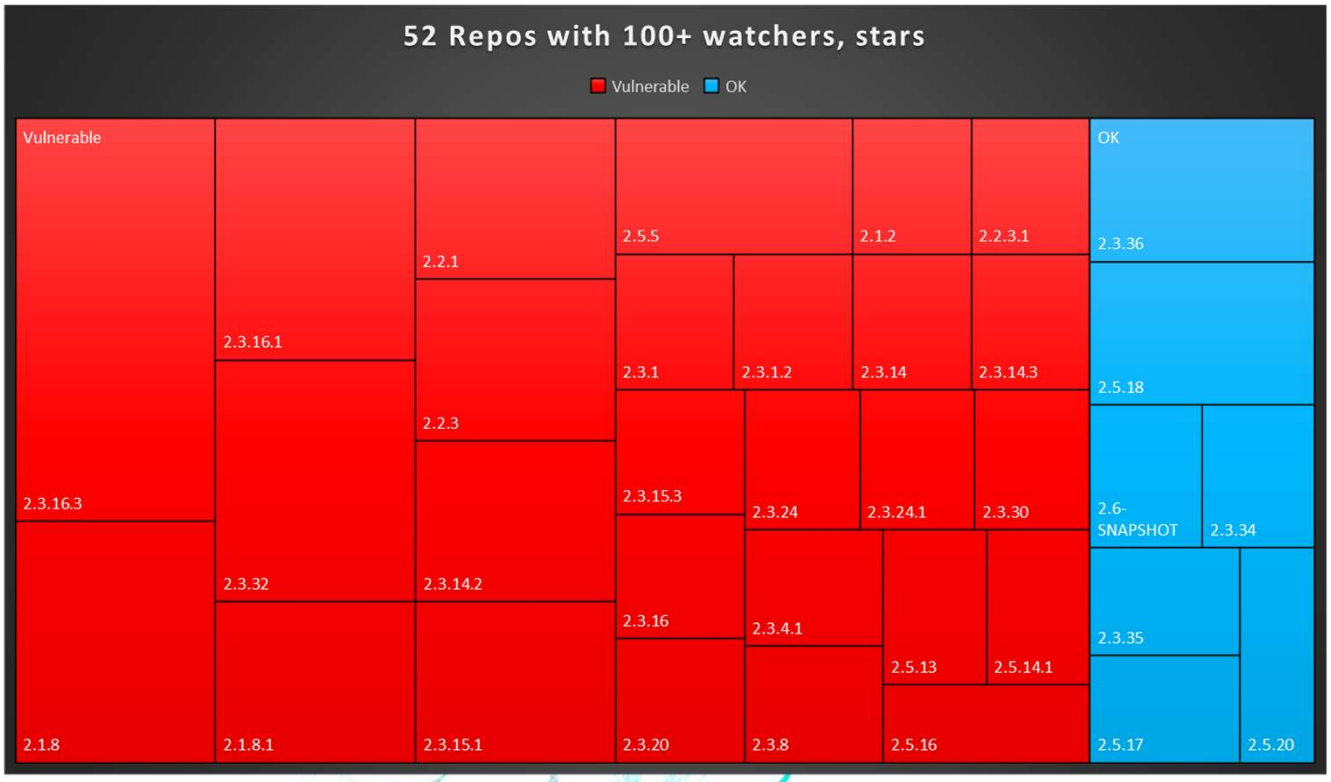
# Statistika

5%



# Statistika – top 52

17%



# And the winner is...

- Zdaleka ne všechno co odkazuje na zastaralou dependenci se dá zneužít
- Některé aplikace mají celkem legitimní důvody

| version | repo | stargazers | watchers | vulnerable |
|---|---|---|---|---|
| 2.5.5 | eugenp/tutorials | 13973 | 1202 | True |
| 2.3.32 | thx/RAP | 9906 | 682 | True |
| 2.3.1 | apache/skywalking | 8319 | 655 | True |
| 2.2.1 | google/guice | 8056 | 556 | True |
| | roboguice/roboguice | 3866 | 334 | True |
| 2.1.2 | jeremylong/DependencyCheck | 1653 | 120 | True |
| 2.5.13 | wkeyuan/DWSurvey | 1012 | 80 | True |
| 2.3.16.3 | wmzsoft/JXADF | 744 | 122 | True |
| 2.2.3 | opensagres/xdocreport | 545 | 69 | True |
| 2.5.16 | SonarSource/sonar-java | 495 | 61 | True |
| 2.3.20 | appfuse/appfuse | 398 | 113 | True |
| 2.3.24 | javamonkey/beetl2.0 | 363 | 48 | True |
| 2.3.16.1 | javamonkey/beetl2.0 | 363 | 48 | True |
| | xautlx/s2jh | 329 | 89 | True |
| 2.3.4.1 | httl/httl | 318 | 65 | True |
| 2.1.8.1 | apache/tomee | 280 | 53 | True |
| | nutzam/nutzmore | 279 | 58 | True |
| 2.3.14.2 | Agilefant/agilefant | 270 | 58 | True |

# Vsuvka – OWASP Dependency Check

- https://www.owasp.org/index.php/OWASP_Dependency_Check

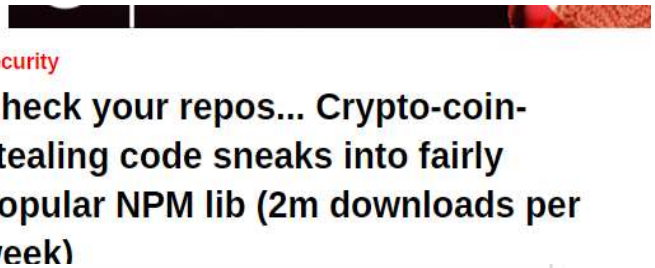
| version | repo | stargazers | watchers | vulnerable |
|---|---|---|---|---|
| 2.5.5 | eugenp/tutorials | 13973 | 1202 | True |
| 2.3.32 | thx/RAP | 9906 | 682 | True |
| 2.3.1 | apache/skywalking | 8319 | 655 | True |
| 2.2.1 | google/guice | 8056 | 556 | True |
| | roboguice/roboguice | 3866 | 334 | True |
| 2.1.2 | jeremylong/DependencyCheck | 1653 | 120 | True |
| 2.5.13 | wkeyuan/DWSurvey | 1012 | 80 | True |
| 2.3.16.3 | wmzsoft/JXADF | 744 | 122 | True |
| 2.2.3 | opensagres/xdocreport | 545 | 69 | True |
| 2.5.16 | SonarSource/sonar-java | 495 | 61 | True |
| 2.3.20 | appfuse/appfuse | 398 | 113 | True |
| 2.3.24 | javamonkey/beetl2.0 | 363 | 48 | True |
| 2.3.16.1 | javamonkey/beetl2.0 | 363 | 48 | True |
| | xautlx/s2jh | 329 | 89 | True |
| 2.3.4.1 | httl/httl | 318 | 65 | True |
| 2.1.8.1 | apache/tomee | 280 | 53 | True |
| | nutzam/nutzmore | 279 | 58 | True |
| 2.3.14.2 | Agilefant/agilefant | 270 | 58 | True |

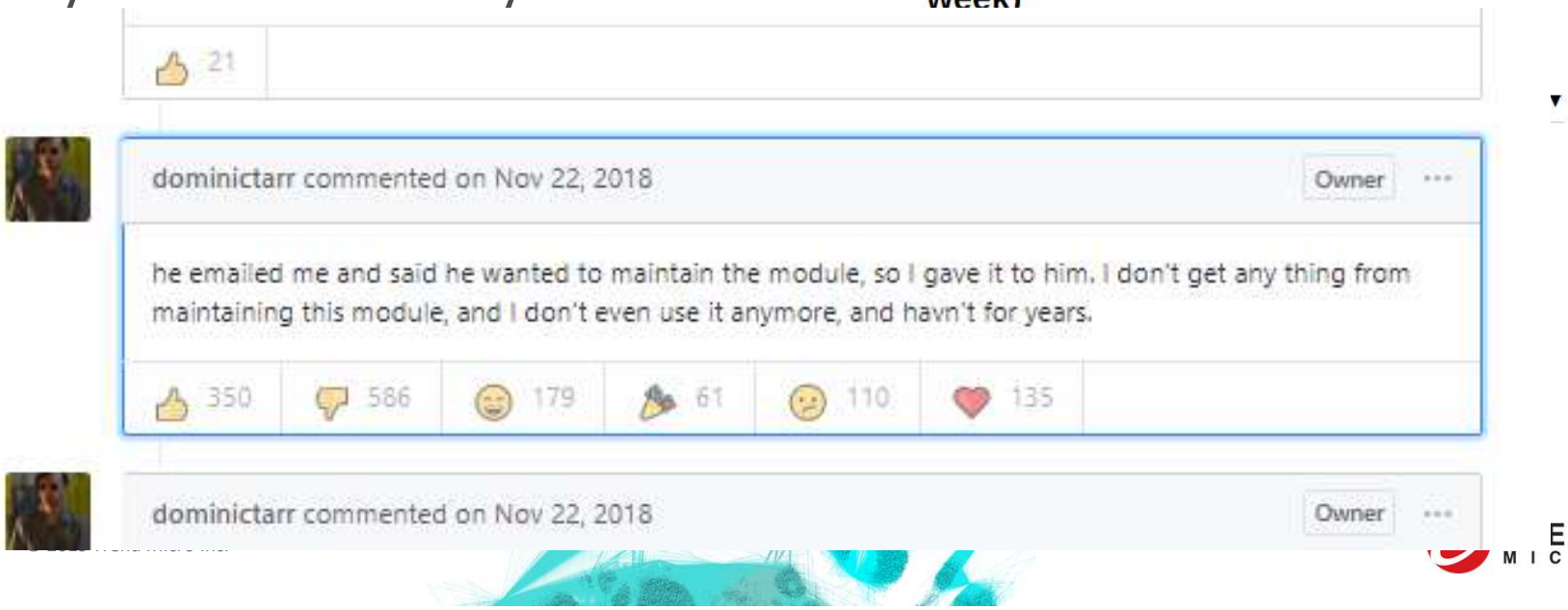
# OWASP Dependency Check

- https://www.owasp.org/index.php/OWASP_Dependency_Check

# Vsuvka – NPM – event-stream

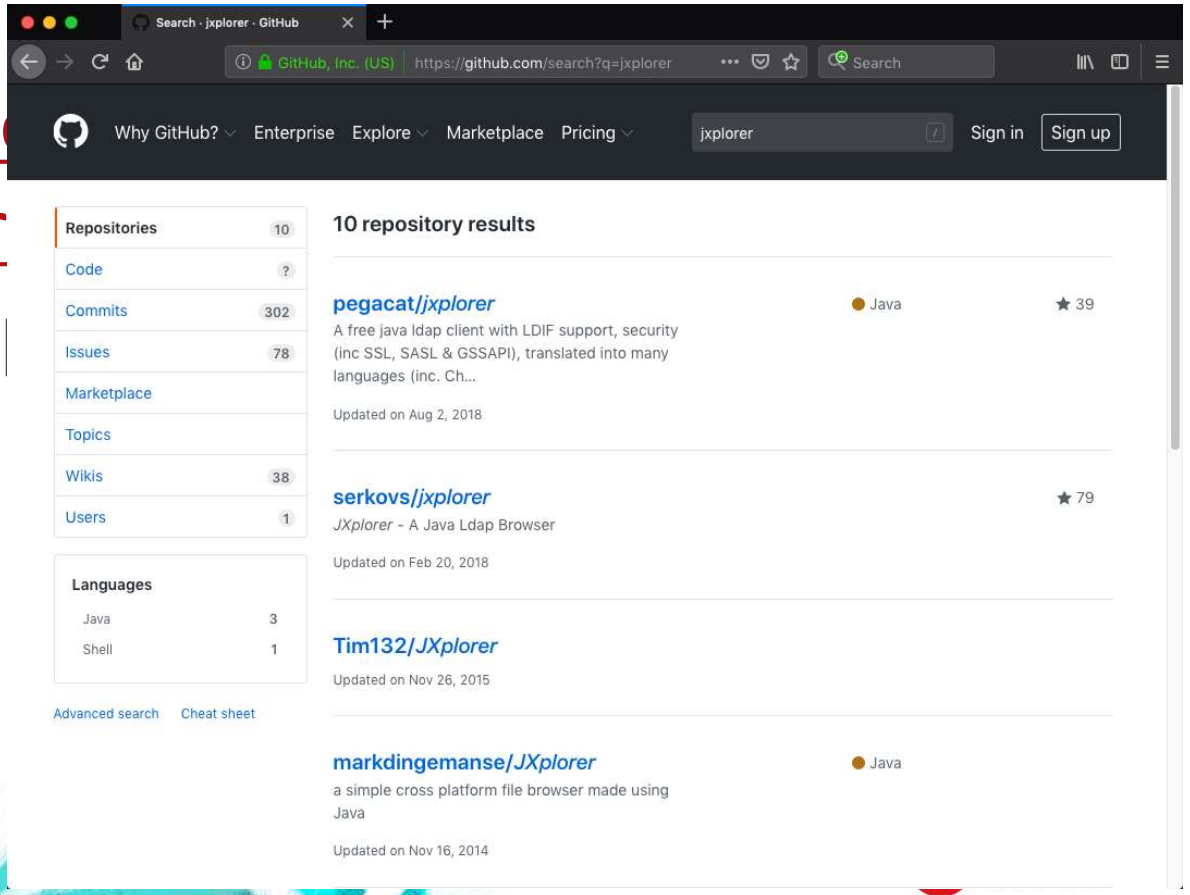
- NPM (nodejs)
- Do knihovny `event-stream` byl vložen kód na vykrádání BTC



# Co všechno se dá stáhnout...

- https://dfir.it/bl
  backdoor-factor
- Podvržená insta



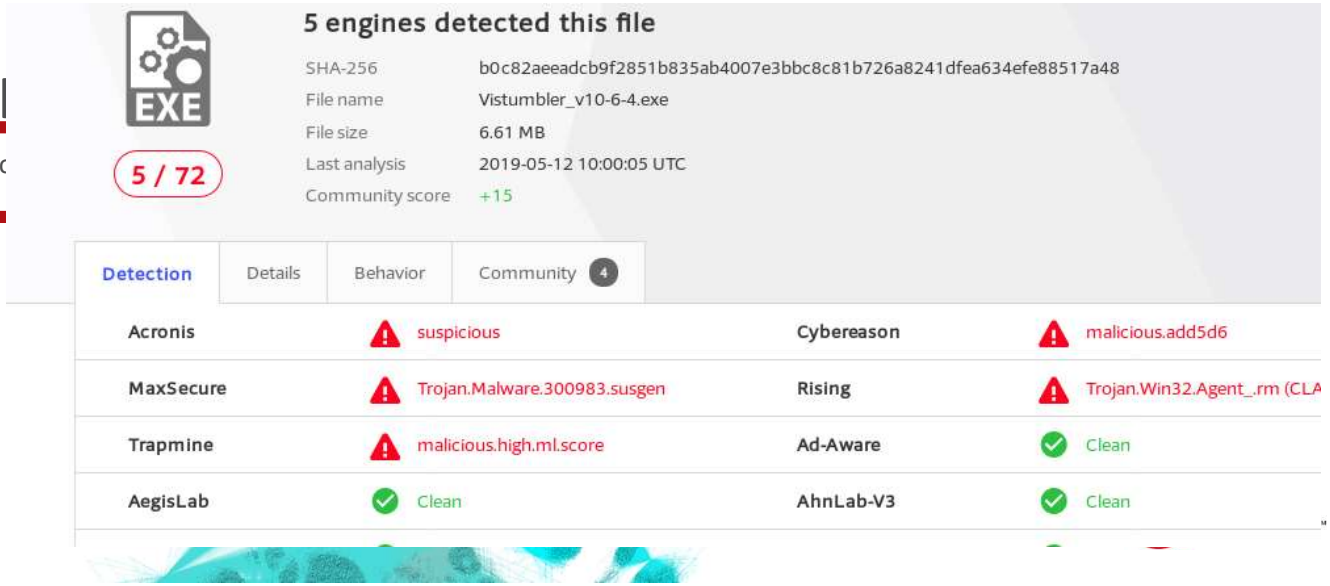
# Co všechno se dá stáhnout...

- Powershell - akamai logs

t=1555893933 i=xxx.xxx.xxx.xxx ho=gist.github.com pa=/n-fukuju/8487308/raw/ccb42ef8ace78f9eb861780b0a6ac16fda62b8fa/progress.ps1
t=1556196762 i=xxx.xxx.xxx.xxx ho=github.com pa=/cybersecgit/PowershellMimiKatz/raw/master/Invoke-Adios.ps1
t=1556199582 i=xxx.xxx.xxx.xxx ho=github.com pa=/PowerShellMafia/PowerSploit/raw/master/Exfiltration/Invoke-Mimikatz.ps1
t=1556262099 i=xxx.xxx.xxx.xxx ho=raw.github.com pa=/krlmlr/r-appveyor/master/scripts/appveyor-tool.ps1

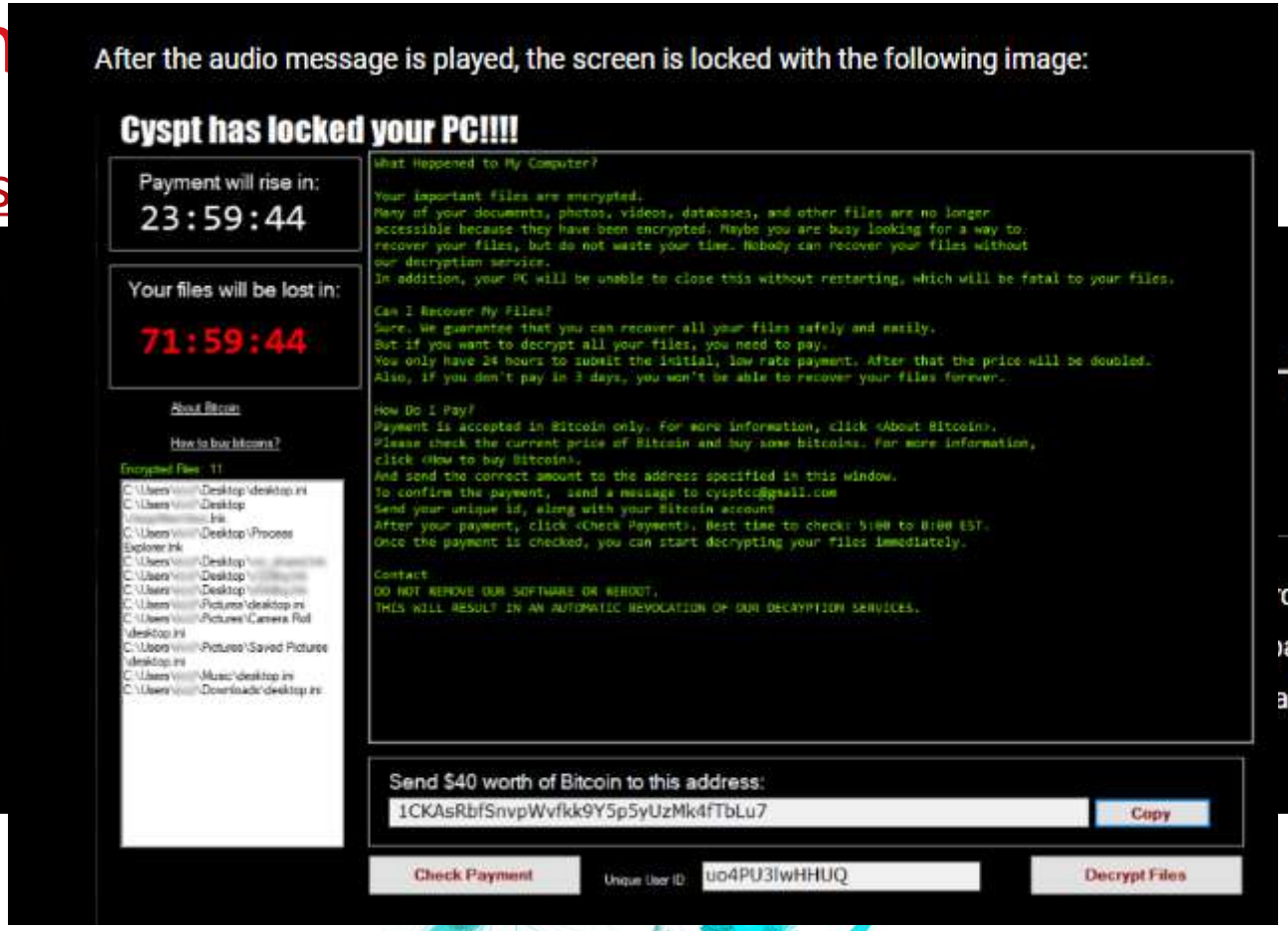
- .exe - aka

t=1557655813 i=xxx.xxx.xxx.xxx ho
4.exe



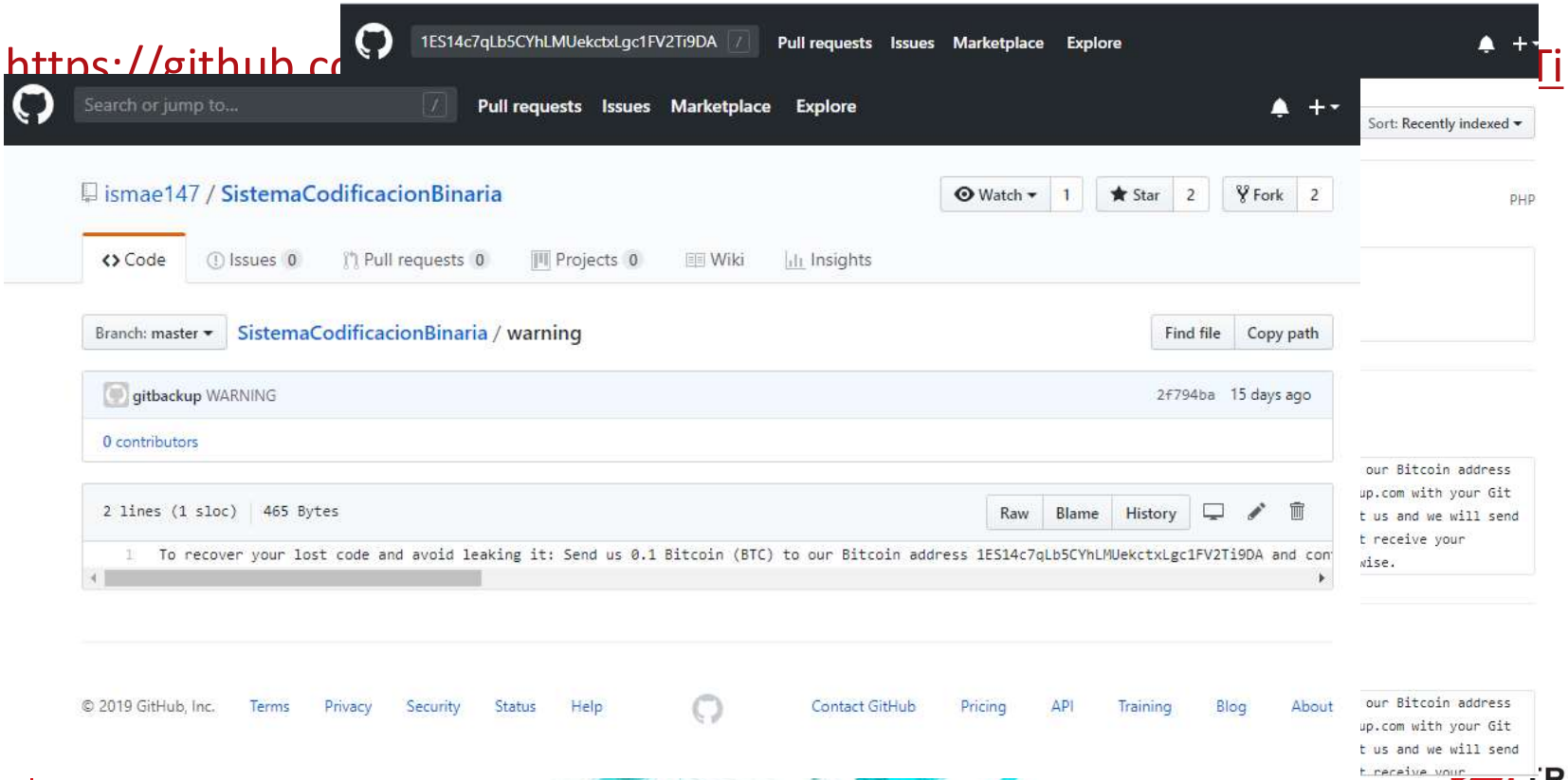
# Open

- https
- h
- h

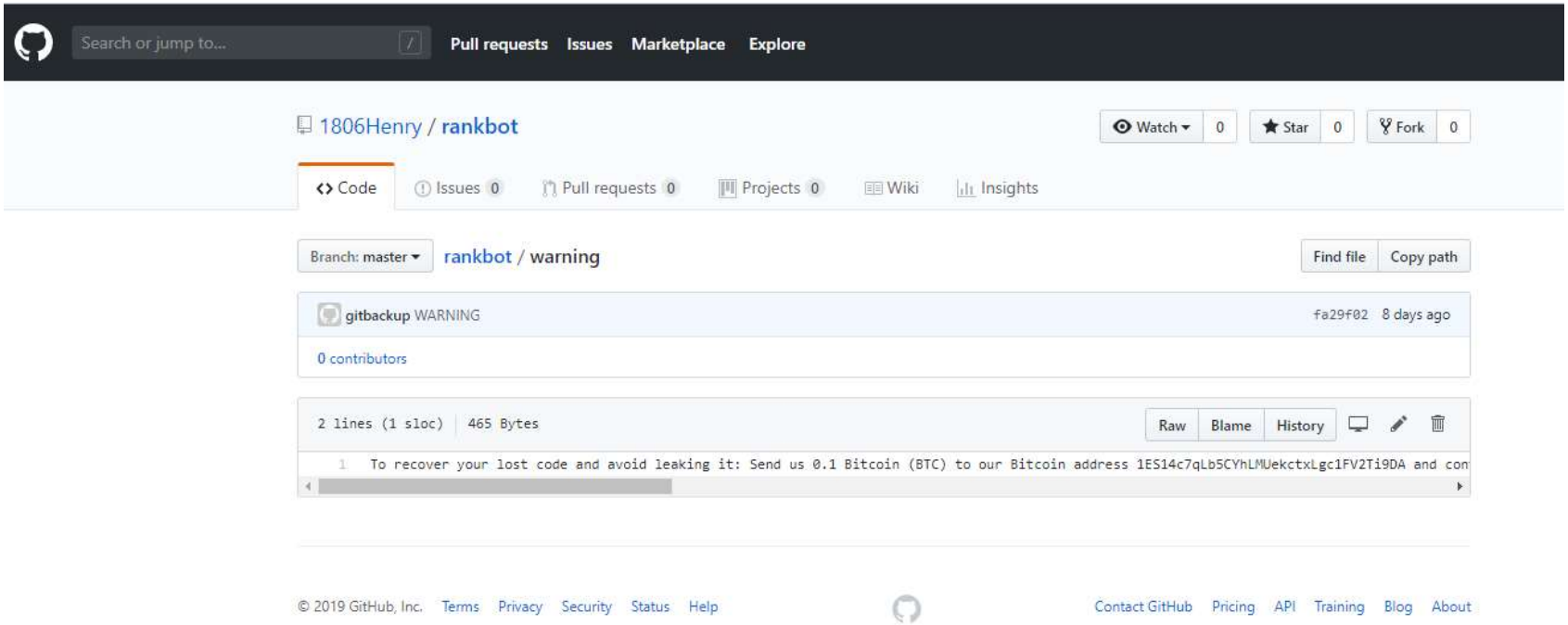


# Open source ransomware II

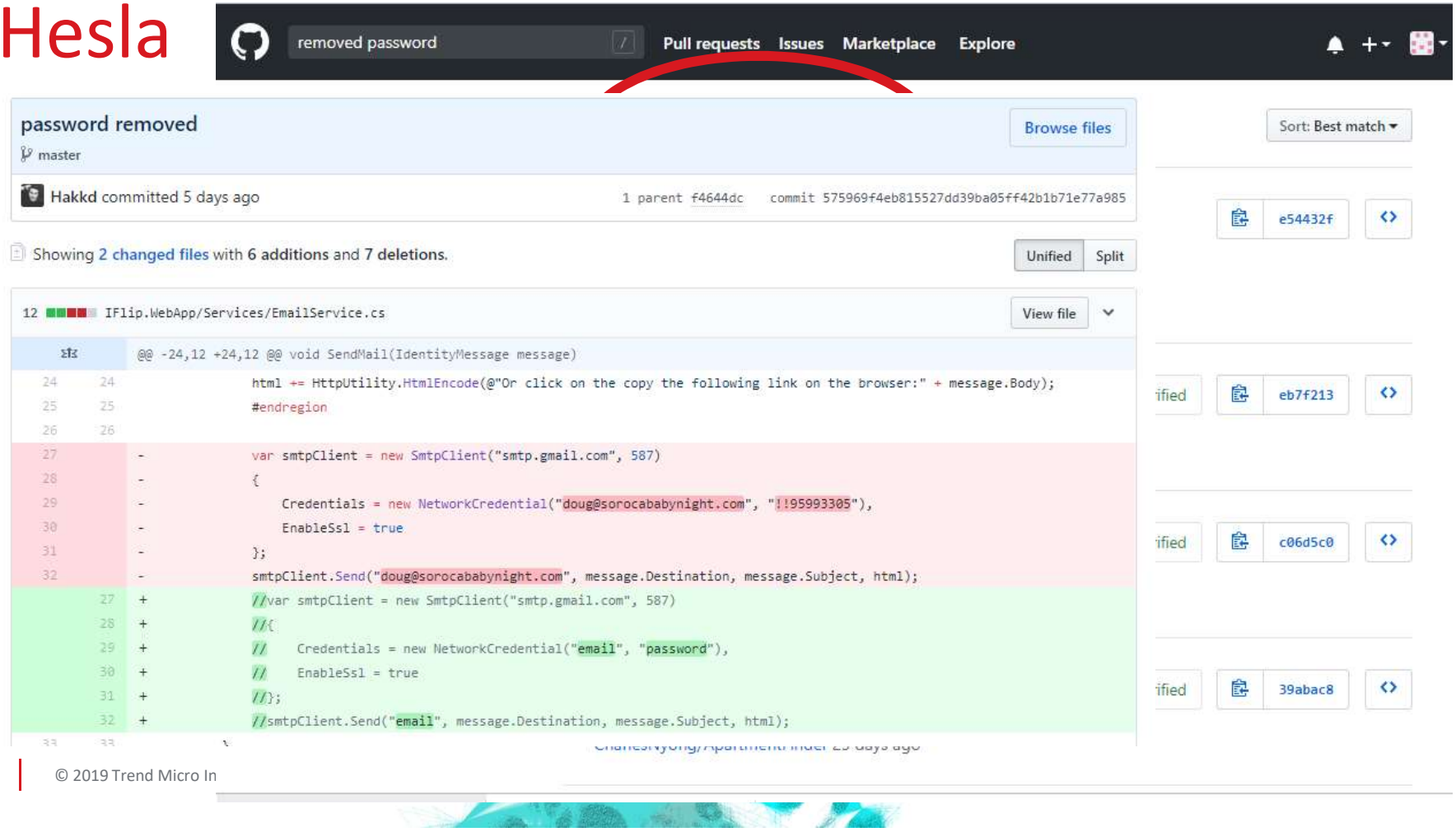
https://github.co



https://github.com/search?o=desc&q=1ES14c7qLb5CYhLMUekctxLgc1FV2Ti9DA&s=indexed&type=Code

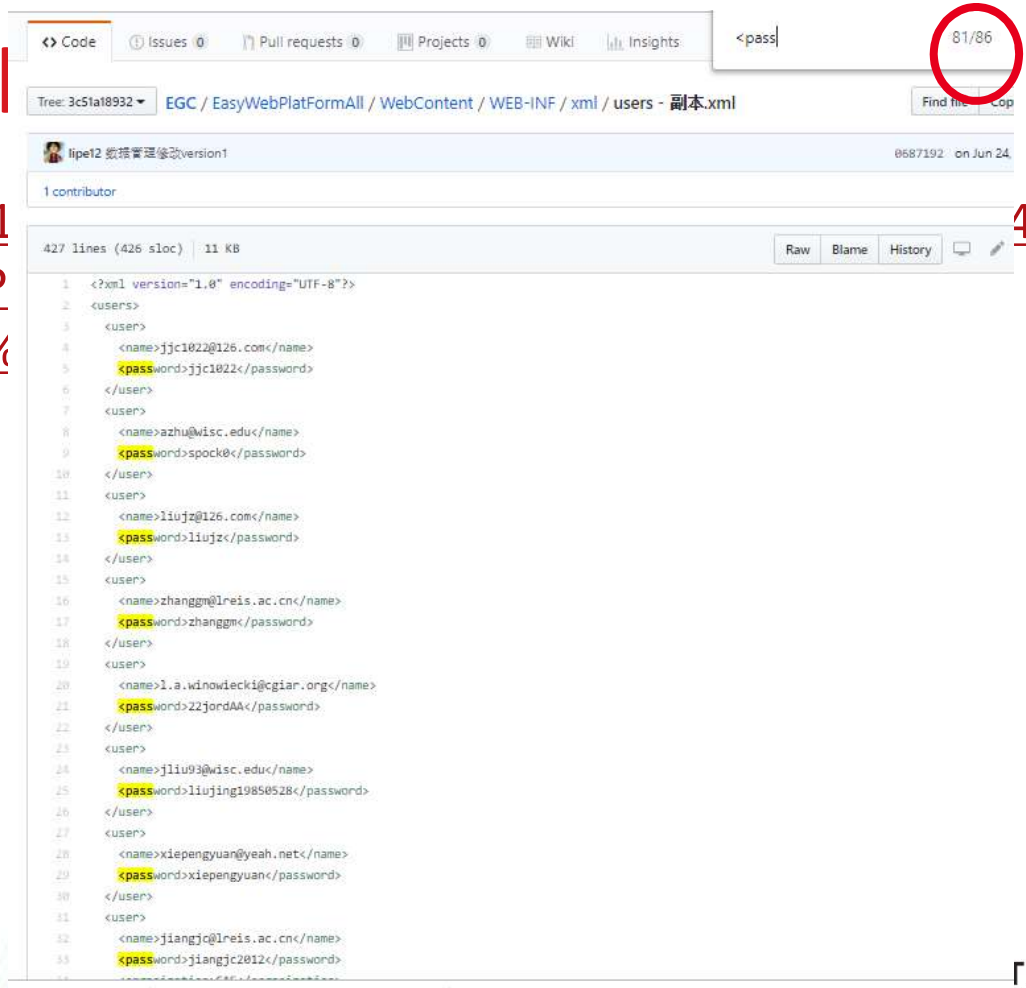


# Hesla



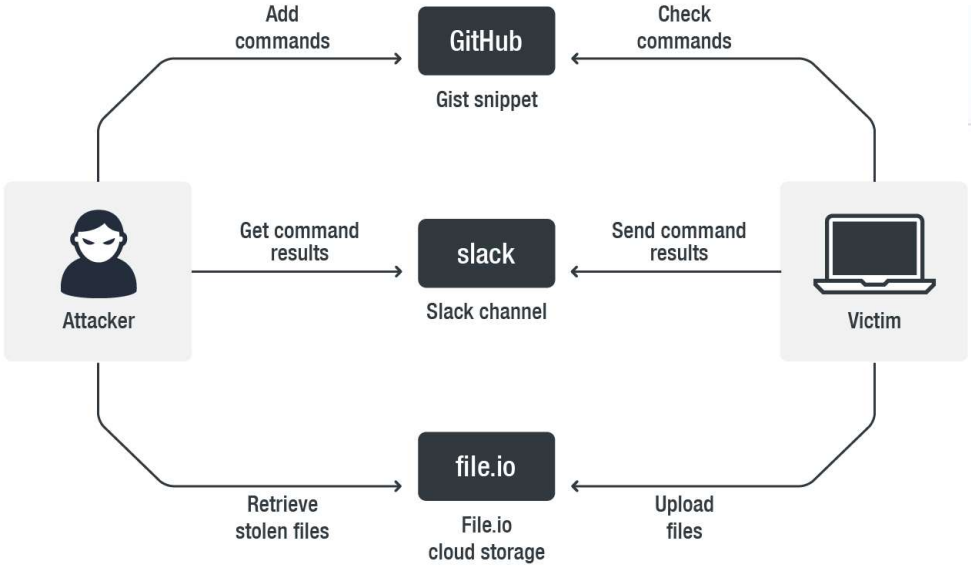
# ...ve velkém styl

- https://github.com/lipe1 4b
  7f7d800d785/EasyWebP
  INF/xml/users%20-%20%



# Command and control

- https://blog.trendmicro.com/trendlabs-security-intelligence/new-slub-backdoor-uses-github-communicates-via-slack/




**gistfile1.txt**

```
1  exec,tasklist
2  ^capture$
3  drive,list
4  file,list,C:\ProgramData\update\
```

TREND MICRO


TREND MICRO
THE ART OF CYBERSECURITY
Automated hybrid cloud workload protection via calls to Trend Micro APIs. **Created with real data by Trend Micro threat researcher and artist Jindrich Karasek.**

# Backup info

https://snyk.io/blog/ten-git-hub-security-best-practices/

Colourama pypi - typosquatting
https://medium.com/@bertusk/cryptocurrency-clipboard-hijacker-discovered-in-pypi-repository-b66b8a534a8
NPM – crossenv
https://blog.npmjs.org/post/163723642530/crossenv-malware-on-the-npm-registry
Linux backdoor
https://freedom-to-tinker.com/2013/10/09/the-linux-backdoor-attempt-of-2003/
Event-stream
https://github.com/dominictarr/event-stream/issues/116#issuecomment-440927400
https://blog.npmjs.org/post/180565383195/details-about-the-event-stream-incident