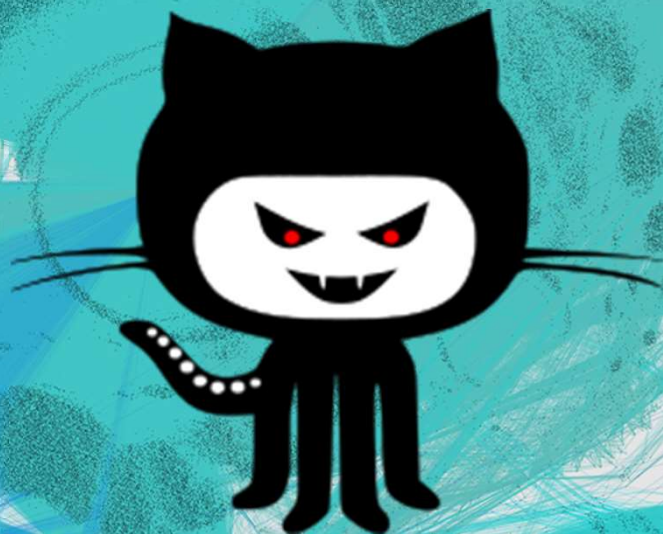




Ďábel se skrývá v GitHubu (?)

Jiří Gogela
Europen 2019





This website has been reported as
unsafe

github.com

We recommend that you do not continue to this website. It has been reported to Microsoft for containing threats to your computer that might reveal personal or financial information.

Back to safety

More information ^

This website has been reported to contain the following threats:

- Malicious software threat: This site contains links to viruses or other software programs that can reveal personal information stored or typed on your computer to malicious persons.
- > [Report that this site does not contain threats](#)
- > [Disregard and continue \(not recommended\)](#)

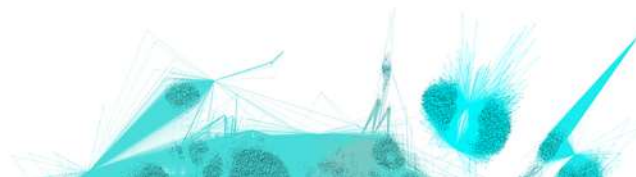
Windows Defender Browser Protection



Motivace



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



Catched by enumeration...

CTFd / CTFd

Watch 89 Unstar 1,824 Fork 671

Code Issues 86 Pull requests 10 Projects 0 Wiki Insights

Fix access to unreleased challenges through /chals/<id> endpoint (#689)

master (#689) 2.0.6 ... 2.0.0

lava authored and ColdHeat committed on Oct 6, 2018 1 parent 14ea952 commit 41933cc367ad3c09ff7d3d0d6c224365c790125f

Showing 1 changed file with 2 additions and 0 deletions. Unified Split

CTFd/challenges.py View file

```
@@ -133,6 +133,8 @@ def chal_view(chal_id):
133 133     teamid = session.get('id')
134 134
135 135     chal = Challenges.query.filter_by(id=chal_id).first_or_404()
136 +     if chal.hidden:
137 +         abort(404)
136 138     chal_class = get_chal_class(chal.type)
137 139
138 140     tags = [tag.tag for tag in Tags.query.add_columns('tag').filter_by(chal=chal.id).all()]
```

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
☐	☆	»	Vanir	Re: [CTFd/CTFd] Registration pass retun...	Apr 21

Zraniteľné závislosti

Zraniteľné závislosti

GitHub's security alerts for vulnerable dependencies

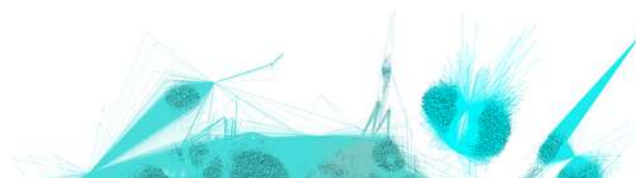
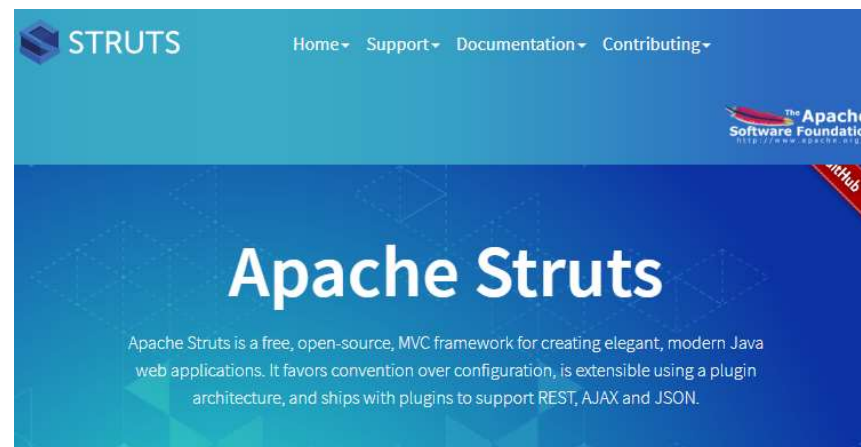
GitHub tracks public vulnerabilities in packages from supported languages on MITRE's [Common Vulnerabilities and Exposures \(CVE\) List](#). We also scan data in public commits on GitHub and use a combination of machine learning and human review to detect vulnerabilities that are not published in the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



ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STOR

BIZ & IT—

Failure to patch two-month-old bug led to massive Equifax breach

...be fixed in March. In May, it bit ~143 million US consumers.

Equifax Suffered Data Breach After It Failed to Patch a Critical Security Flaw

September 14, 2017

Security
Apache
allow
biz s

SECURITYWEEK

INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS Subscribe | 2019 CISO Forum, Present

Malware & Threats Cybercrime Mobile & Wireless Risk & Compliance Security Architecture S

Mobile Security Wireless Security

Home > Virus & Threats



Oracle Releases Patches for Exploited Apache Struts Flaw

By Eduard Kovacs on September 25, 2017



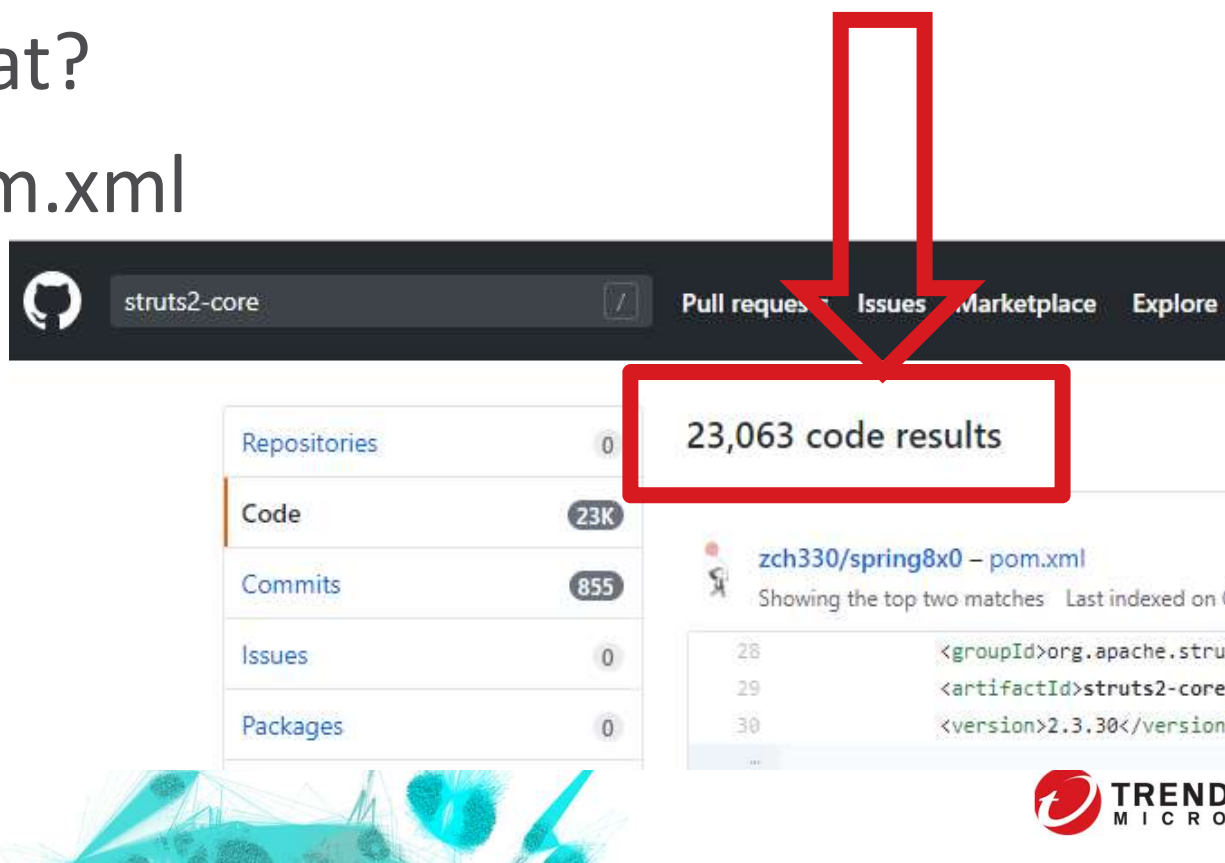
Oracle has released patches for many of its products to address several vulnerabilities in the Apache Struts 2 framework, including one that has been exploited in the wild for

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



The screenshot shows the GitHub search interface for the query 'struts2-core'. A red rectangle highlights the search bar containing the text 'struts2-core'. A red arrow points from this rectangle down to another red rectangle that highlights the text '23,063 code results'. Below this, a snippet of XML code is visible, showing the top two matches for the search. The code is from the repository 'zch330/spring8x0' and is a 'pom.xml' file. The XML snippet shows the following structure:

```
28 <groupId>org.apache.strut</groupId>
29 <artifactId>struts2-core</artifactId>
30 <version>2.3.30</version>
```

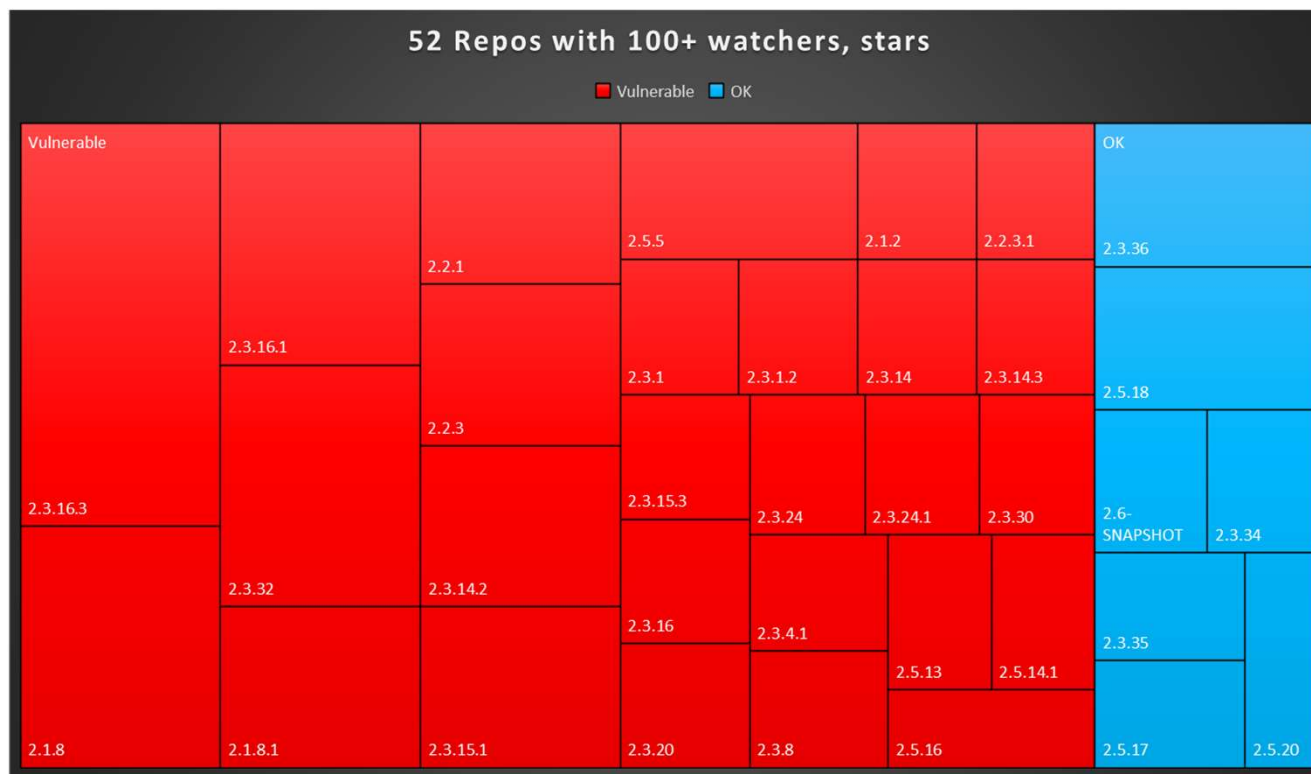
The bottom of the image features a decorative graphic of blue and green geometric shapes and the Trend Micro logo.

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/xdcreport	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	html/html	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	html/html	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

Security

Check your repos... Crypto-coin-stealing code sneaks into fairly popular NPM lib (2m downloads per week)

👍 21



dominictarr commented on Nov 22, 2018

Owner

...

he emailed me and said he wanted to maintain the module, so I gave it to him. I don't get any thing from maintaining this module, and I don't even use it anymore, and havn't for years.

👍 350

👎 586

😊 179

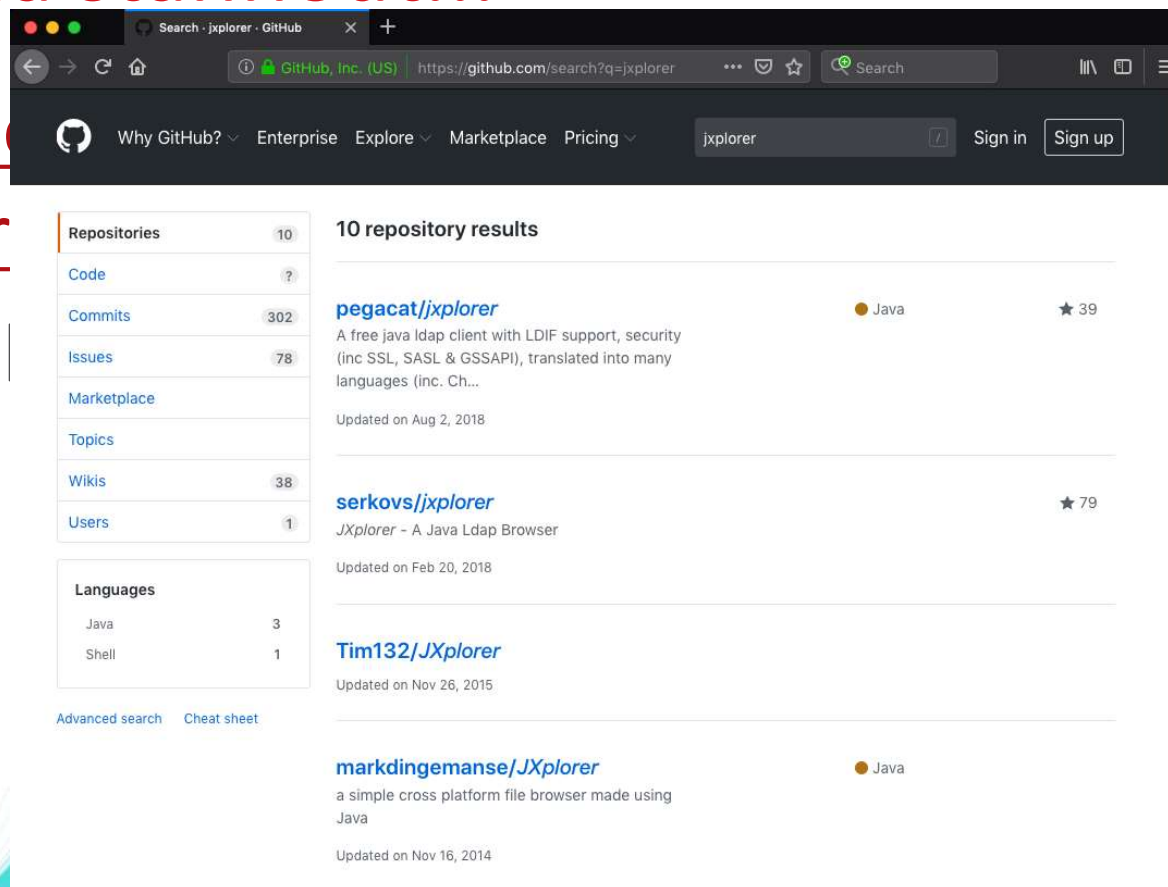
🍷 61

😞 110

❤️ 135

Co všechno se dá stáhnout...

- <https://dfir.it/blog/backdoor-factor>
- Podvržená instalace



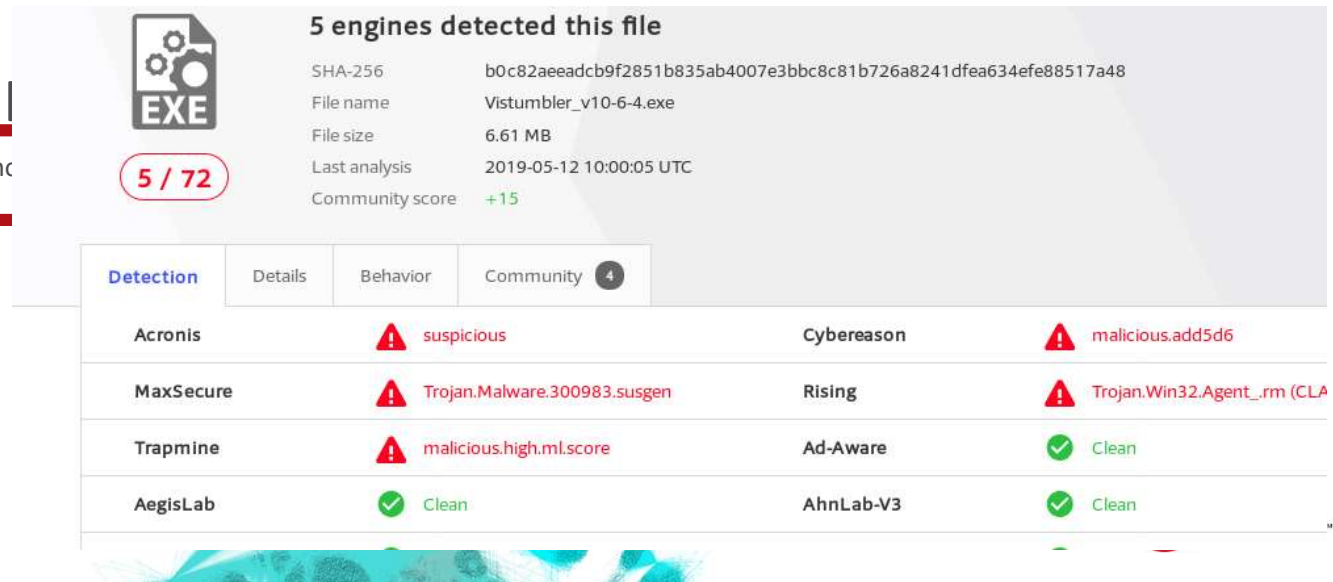
Co všechno se dá stáhnout...

- Powershell - akamai logs

t=1555893933	i=xxx.xxx.xxx.xxx	ho=gist.github.com	pa=/n-fukuii/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
--------------	-------------------	----------



The screenshot shows the VirusShare analysis interface for the file Vistumbler_v10-6-4.exe. At the top, it states '5 engines detected this file'. Below this, file metadata is provided: SHA-256 hash (b0c82aeedcb9f2851b835ab4007e3bbc8c81b726a8241dfea634efe88517a48), File name (Vistumbler_v10-6-4.exe), File size (6.61 MB), Last analysis (2019-05-12 10:00:05 UTC), and Community score (+15). A tabbed interface shows 'Detection' as the active tab, with 'Details', 'Behavior', and 'Community' (4 items) as other options. Below the tabs, a table lists the detection results from various engines:

Engine	Detection Result
Acronis	suspicious
MaxSecure	Trojan.Malware.300983.susgen
Trapmine	malicious.high.ml.score
AegisLab	Clean
Cybereason	malicious.add5d6
Rising	Trojan.Win32.Agent_rm (CLA
Ad-Aware	Clean
AhnLab-V3	Clean

Open

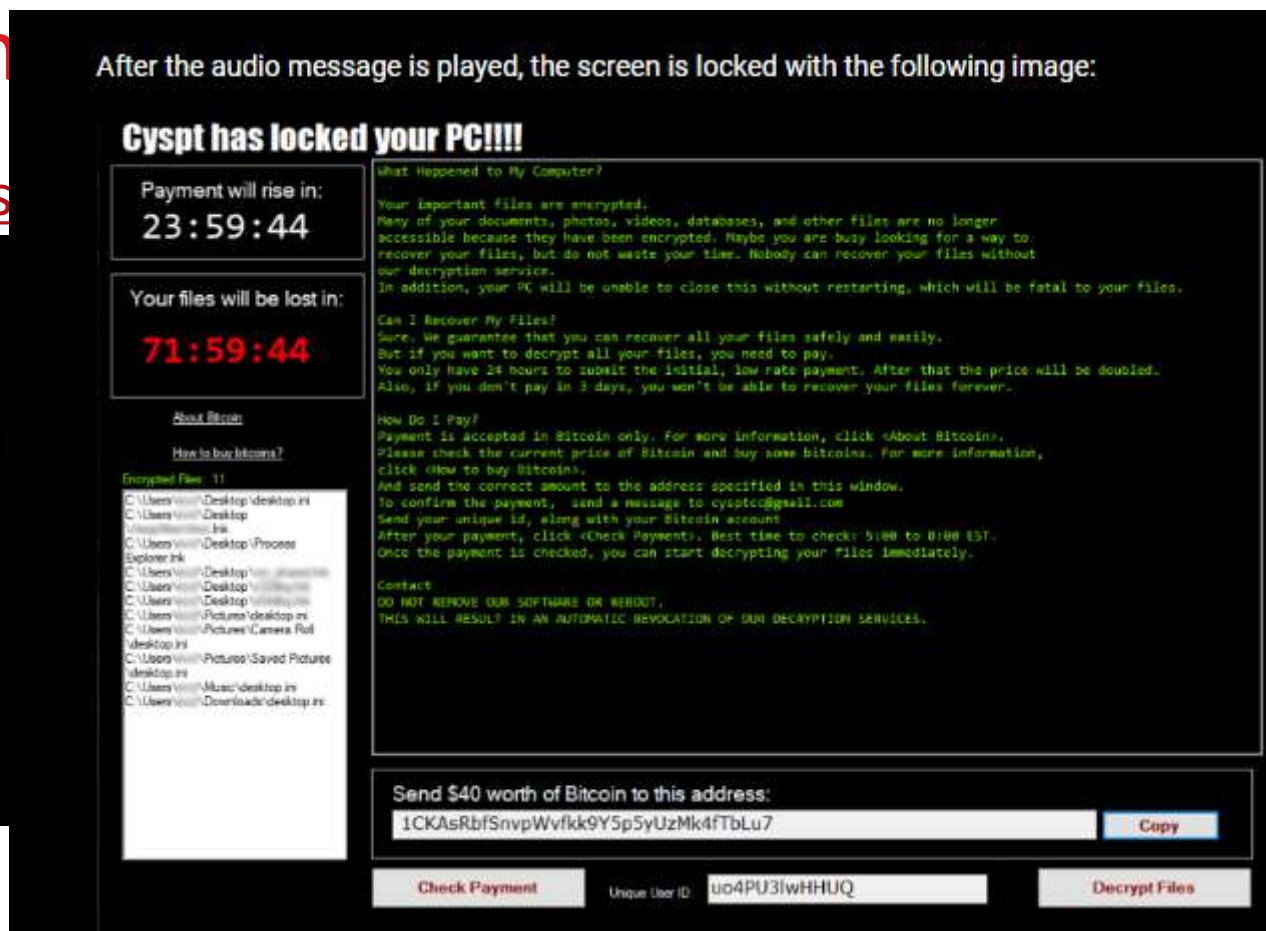
- <https://www.trendmicro.com/>



- <https://www.trendmicro.com/>

- <https://www.trendmicro.com/>

After the audio message is played, the screen is locked with the following image:



THE WILD

ce ransomware
acked. In the
and-crafted. So, I

Open source ransomware II

<https://github.com/ismae147/SistemaCodificacionBinaria>

1ES14c7qLb5CYhLMUekctxLgc1FV2Ti9DA Pull requests Issues Marketplace Explore

Search or jump to... Pull requests Issues Marketplace Explore

Sort: Recently indexed

ismae147 / SistemaCodificacionBinaria

Watch 1 Star 2 Fork 2

Code Issues 0 Pull requests 0 Projects 0 Wiki Insights

Branch: master SistemaCodificacionBinaria / warning Find file Copy path

gitbackup WARNING 2f794ba 15 days ago

0 contributors

2 lines (1 sloc) 465 Bytes Raw Blame History

```
1 To recover your lost code and avoid leaking it: Send us 0.1 Bitcoin (BTC) to our Bitcoin address 1ES14c7qLb5CYhLMUekctxLgc1FV2Ti9DA and con
```

our Bitcoin address
up.com with your Git
t us and we will send
t receive your
wise.

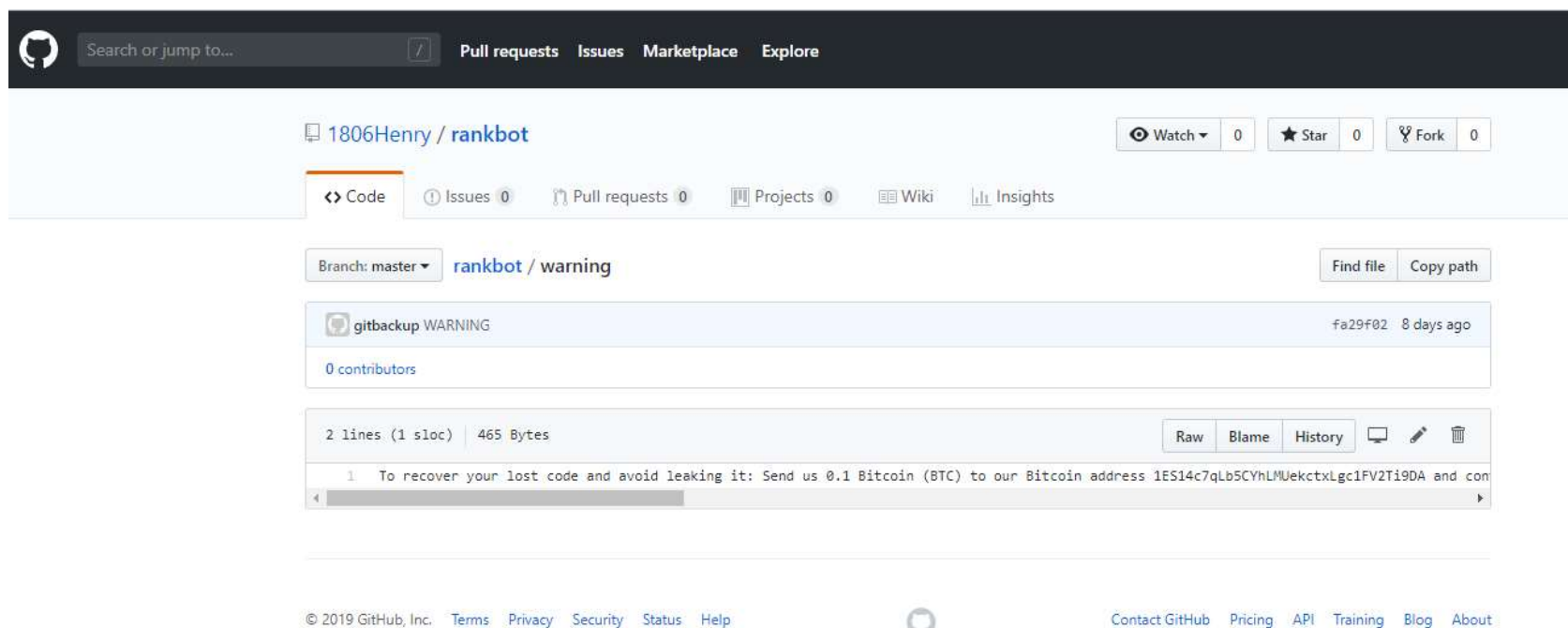
our Bitcoin address
up.com with your Git
t us and we will send
t receive your

© 2019 GitHub, Inc. Terms Privacy Security Status Help Contact GitHub Pricing API Training Blog About

© 2019 Trend Micro Inc.

TREND MICRO

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



The screenshot shows a GitHub repository page for a user named '1806Henry' with the repository name 'rankbot'. The repository is in the 'master' branch and shows a file named 'warning' with 2 lines of code. The code contains a warning message about recovering lost code by sending 0.1 Bitcoin to a specific address.

Branch: master **rankbot** / warning

gitbackup WARNING fa29f02 8 days ago

0 contributors

2 lines (1 sloc) 465 Bytes

Raw Blame History

```
1 To recover your lost code and avoid leaking it: Send us 0.1 Bitcoin (BTC) to our Bitcoin address 1ES14c7qLb5CYhLMUekctxLgc1FV2Ti9DA and con
```



Hesla

password removed

master

Browse files

Sort: Best match ▾

Hakd committed 5 days ago

1 parent f4644dc commit 575969f4eb815527dd39ba05ff42b1b71e77a985

Showing 2 changed files with 6 additions and 7 deletions.

Unified Split

View file ▾

```
12 IFlip.WebApp/Services/EmailService.cs
@@ -24,12 +24,12 @@ void SendMail(IdentityMessage message)
24 24      html += HttpUtility.HtmlEncode(@"Or click on the copy the following link on the browser:" + message.Body);
25 25      #endregion
26 26
27 -      var smtpClient = new SmtpClient("smtp.gmail.com", 587)
28 -      {
29 -          Credentials = new NetworkCredential("doug@sorocababynight.com", "!!95993305"),
30 -          EnableSsl = true
31 -      };
32 -      smtpClient.Send("doug@sorocababynight.com", message.Destination, message.Subject, html);
+      //var smtpClient = new SmtpClient("smtp.gmail.com", 587)
+      //{
+      //    Credentials = new NetworkCredential("email", "password"),
+      //    EnableSsl = true
+      //};
+      //smtpClient.Send("email", message.Destination, message.Subject, html);
```

Unified eb7f213 <>

Unified c06d5c0 <>

Unified 39abac8 <>

...ve velkém styl

- <https://github.com/lipe17f7d800d785/EasyWebPlatformAll/WebContent/WEB-INF/xml/users-副本.xml>

81/86

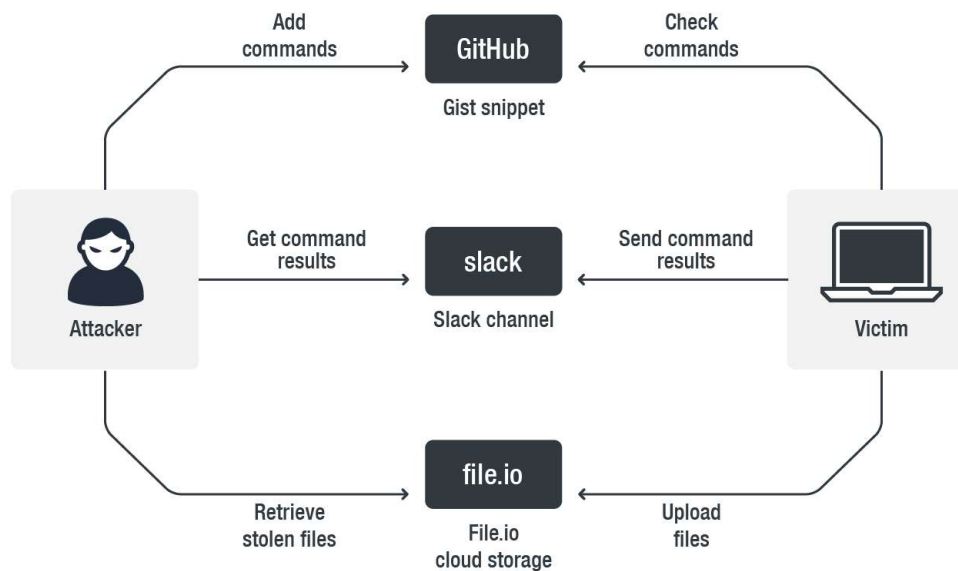
4b

```
<?xml version="1.0" encoding="UTF-8"?>
<users>
  <user>
    <name>jjc1022@126.com</name>
    <pass>jjc1022</password>
  </user>
  <user>
    <name>azhu@wisc.edu</name>
    <pass>spock0</password>
  </user>
  <user>
    <name>liujz@126.com</name>
    <pass>liujz</password>
  </user>
  <user>
    <name>zhanggm@lreis.ac.cn</name>
    <pass>zhanggm</password>
  </user>
  <user>
    <name>l.a.winowiecki@cgiar.org</name>
    <pass>22jordaA</password>
  </user>
  <user>
    <name>jliu93@wisc.edu</name>
    <pass>liujing19850528</password>
  </user>
  <user>
    <name>xiepengyuan@yeah.net</name>
    <pass>xiepengyuan</password>
  </user>
  <user>
    <name>jiangjc@lreis.ac.cn</name>
    <pass>jiangjc2012</password>
  </user>

```

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\
```



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>

