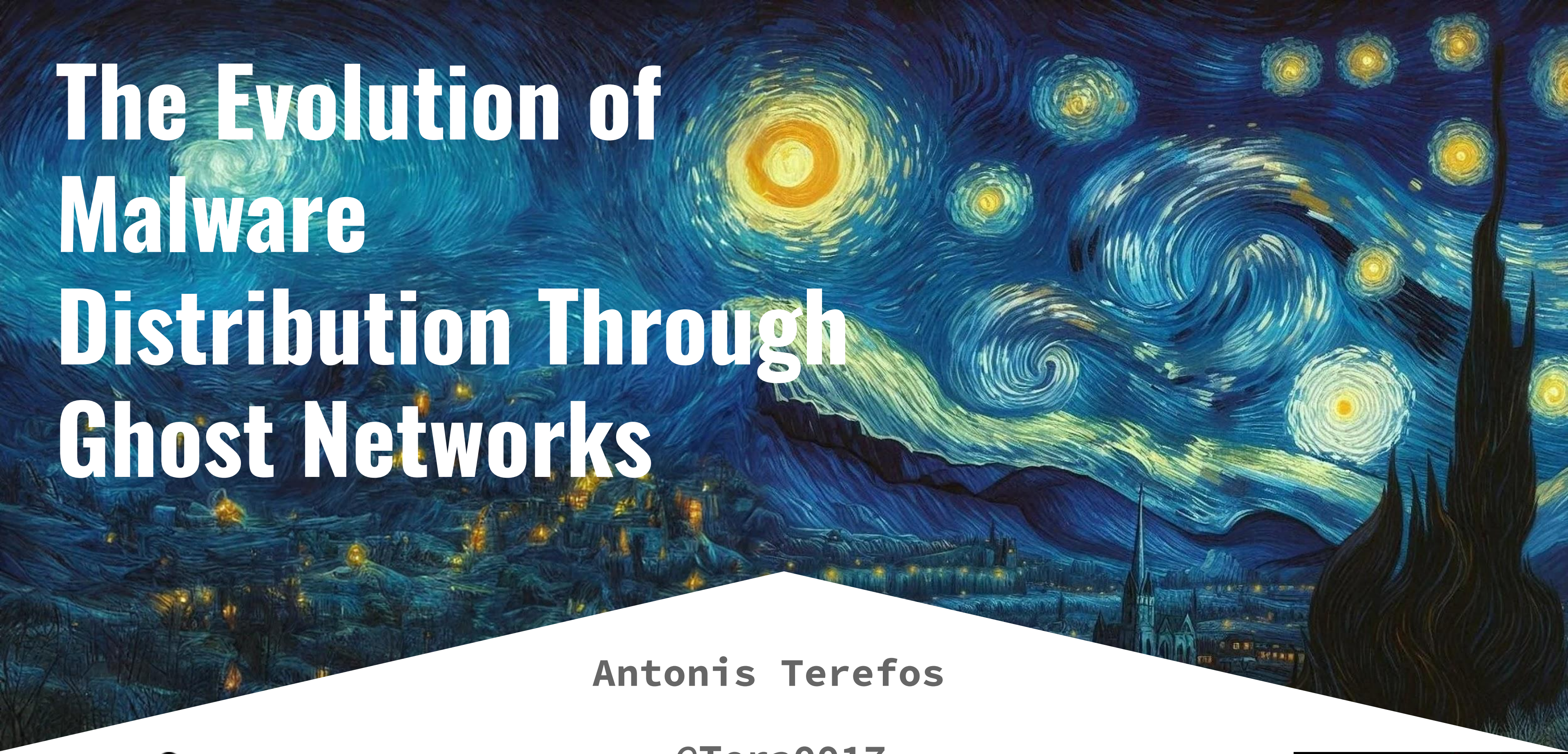
The Evolution of Malware Distribution Through Ghost Networks



Antonis Terefos

@Tera0017

BOTCONF 2025

CHECK POINT

cp<r>

CHECK POINT RESEARCH

WHOAMI

- Antonis Terefos (@Tera0017)
- Malware Reverse Engineer @ CP<r>
  - Reversing Malware
  - Automating Config Extraction
  - Researching Threats
  - Tracking & Monitoring Cyber Criminals
- Enjoy
  - Reversing
  - Web App Penetration testing
  - CTFs
  - Reading Books

Agenda

- Gh0st Network
- Stargazers Ghost Network
- Operator: Stargazer Goblin
- Present Ghost Networks
- New Discoveries
- Statistics
- Conclusion

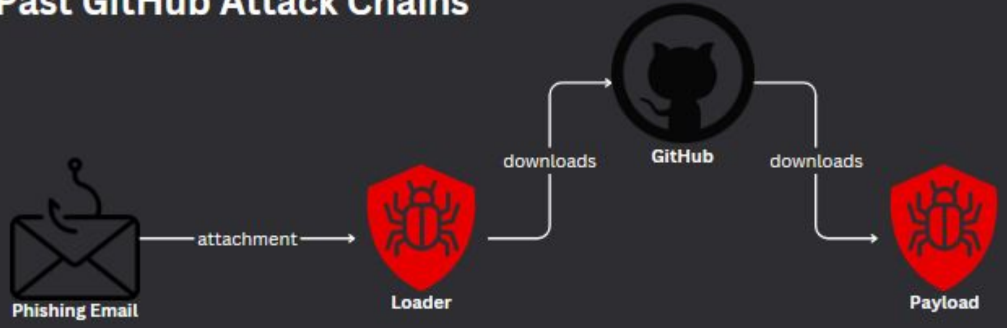
What is a Ghost Network

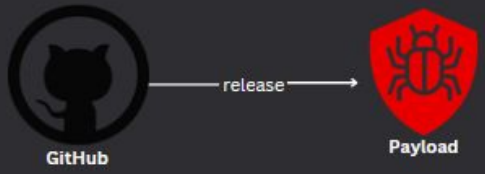
Ghost Network is a network of “ghost”/fake accounts that operate as a service on legitimizing malware distribution activities on various platforms.

Stargazers Ghost Network

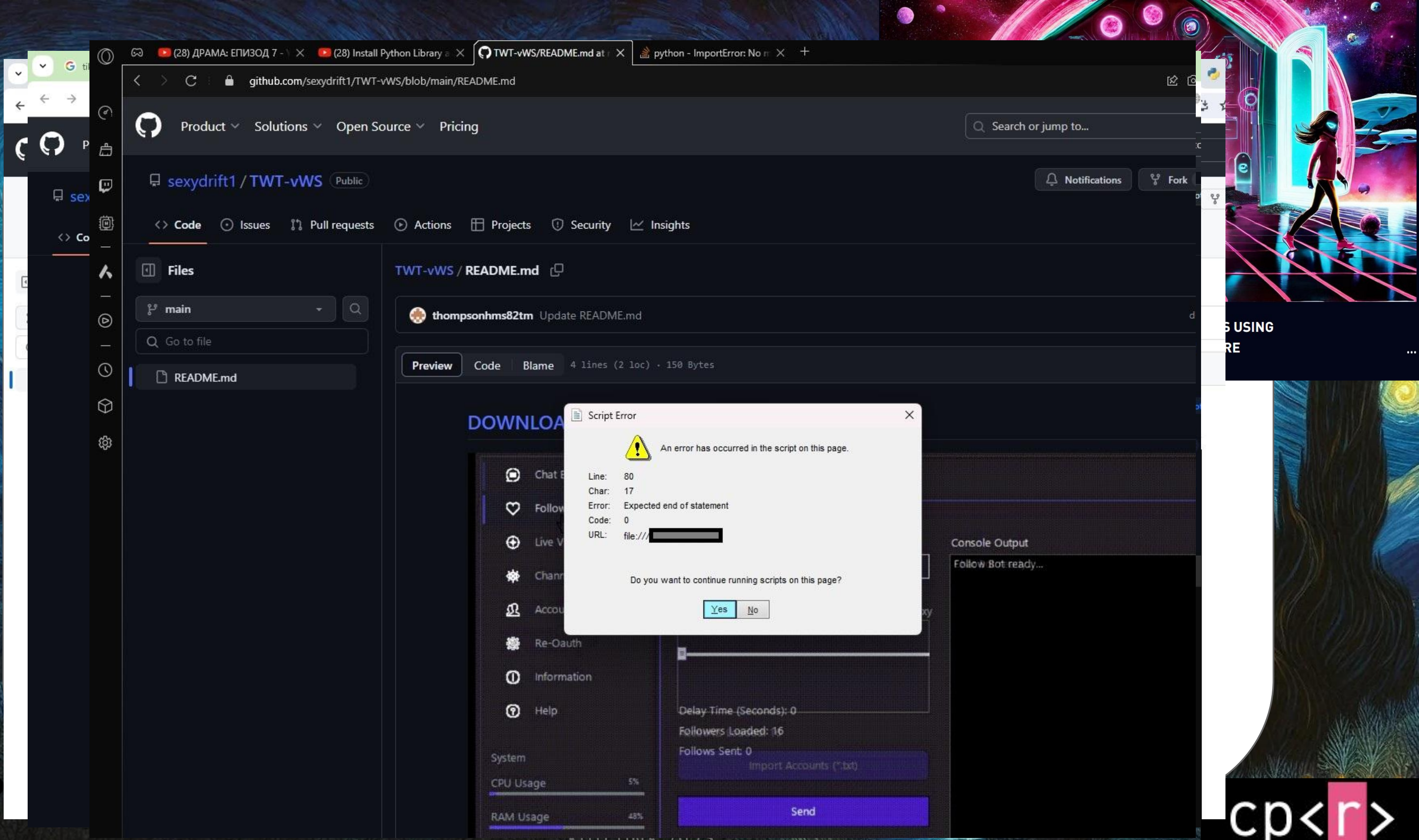
- First discovered Ghost Network
- Operates on **GitHub**
- Exists since **August 2022**
- **Public** since **July 2023**
- Makes malicious repos appear legitimate
- Ghost accounts actions:
  - Star/Watch/Fork repositories
  - Like/share releases
  - Create repos with malicious content
  - …

Past GitHub Attack Chains





Stargazers Ghost Network



Script Error

An error has occurred in the script on this page.

```
Line:   80
Char:   17
Error:  Expected end of statement
Code:   0
URL:    file:///[redacted]
```

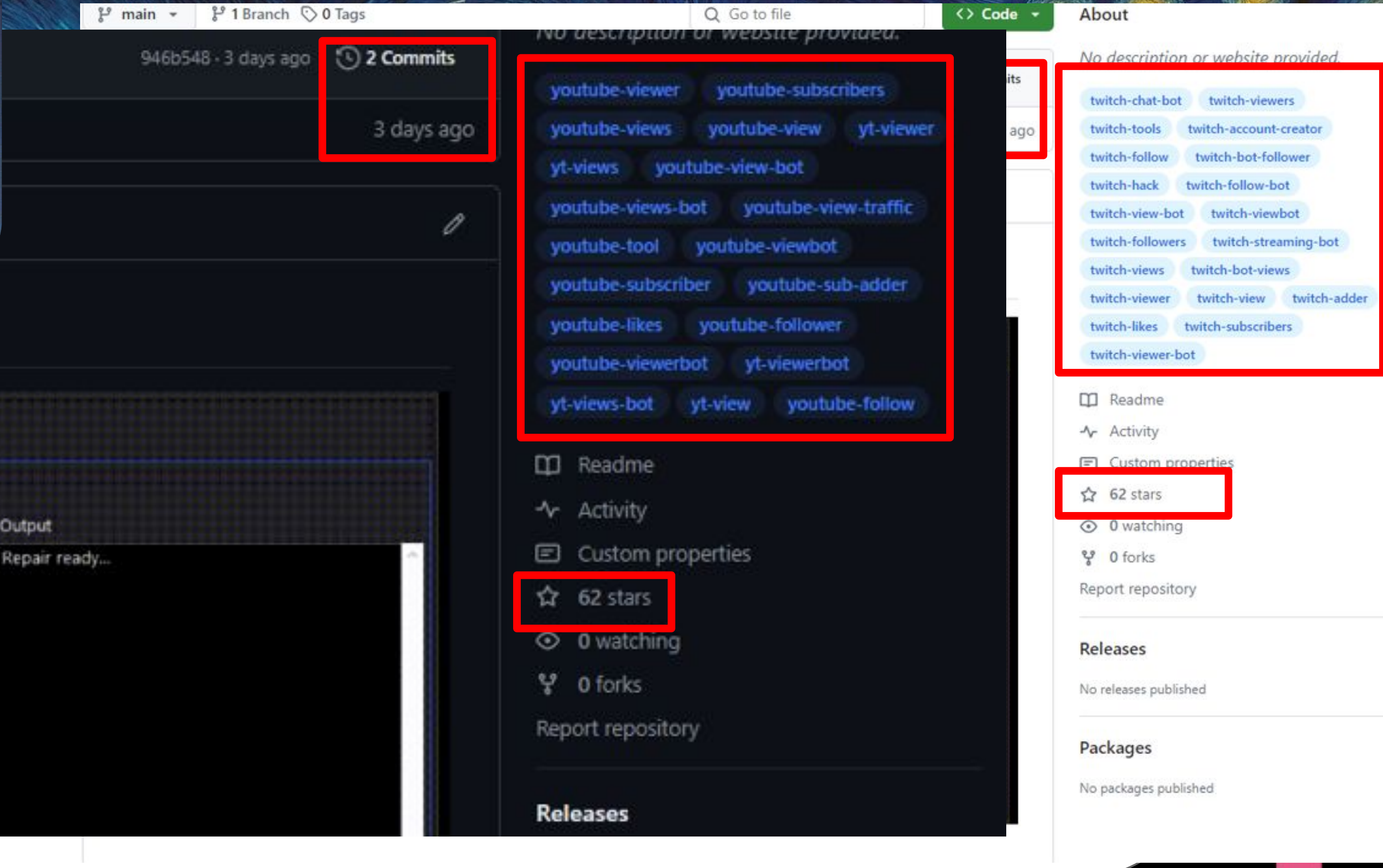
Do you want to continue running scripts on this page?

Yes No

CHECK POINT™

BOTCONF 2025

cp<r>
CHECK POINT RESEARCH



main · 1 Branch · 0 Tags · Go to file · Code

946b548 · 3 days ago · 2 Commits

3 days ago

ounts ON Use Proxy

Console Output

```
Account Repair ready...
```

No description or website provided.

youtube-viewer · youtube-subscribers · youtube-views · youtube-view · yt-viewer · yt-views · youtube-view-bot · youtube-views-bot · youtube-view-traffic · youtube-tool · youtube-viewbot · youtube-subscriber · youtube-sub-adder · youtube-likes · youtube-follower · youtube-viewerbot · yt-viewerbot · yt-views-bot · yt-view · youtube-follow

Readme

Activity

Custom properties

62 stars

0 watching

0 forks

Report repository

Releases

About

No description or website provided.

twitch-chat-bot · twitch-viewers · twitch-tools · twitch-account-creator · twitch-follow · twitch-bot-follower · twitch-hack · twitch-follow-bot · twitch-view-bot · twitch-viewbot · twitch-followers · twitch-streaming-bot · twitch-views · twitch-bot-views · twitch-viewer · twitch-view · twitch-adder · twitch-likes · twitch-subscribers · twitch-viewer-bot

Readme

Activity

Custom properties

62 stars

0 watching

0 forks

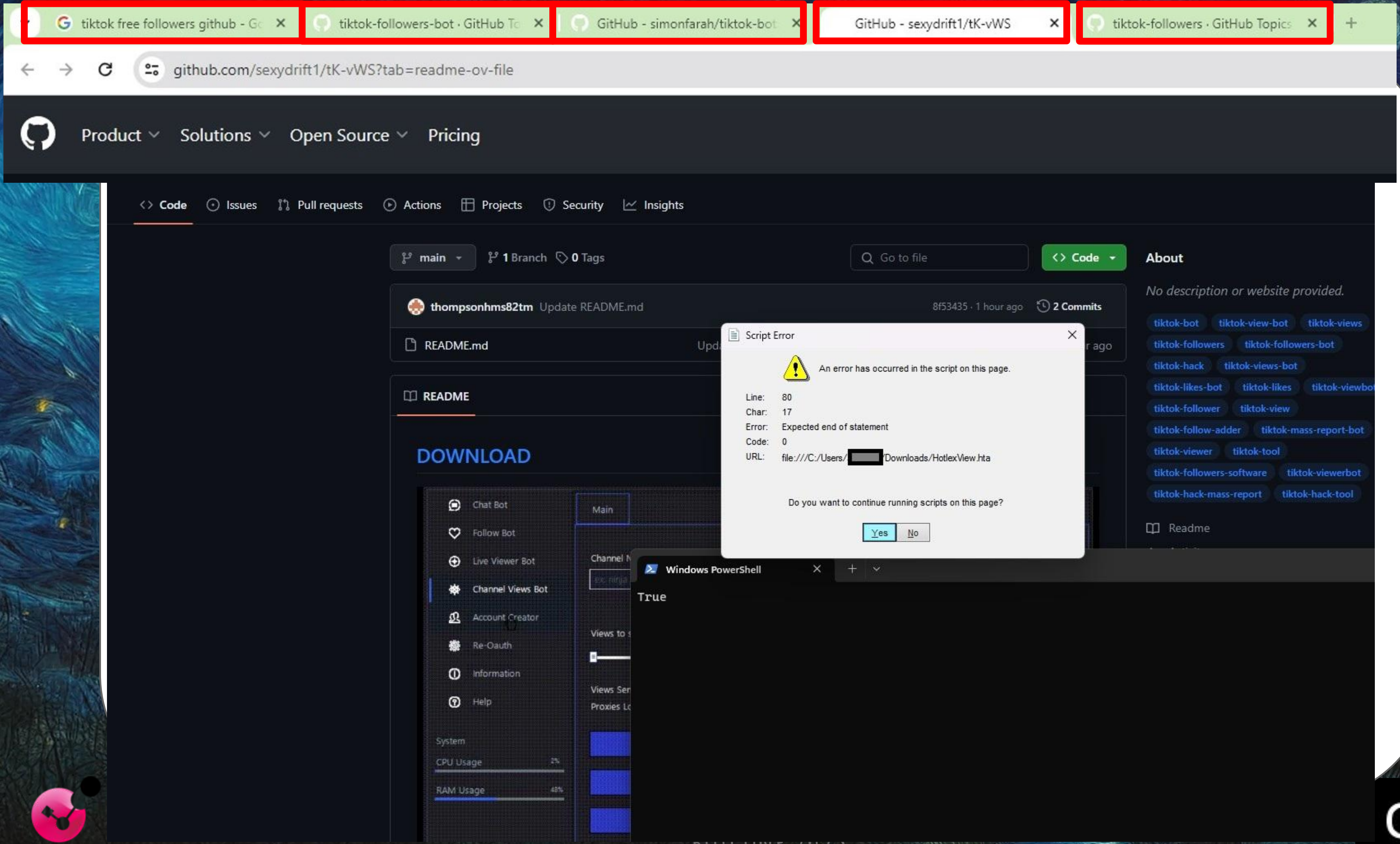
Report repository

Releases

No releases published

Packages

No packages published



Script Error

An error has occurred in the script on this page.

Line: 80
Char: 17
Error: Expected end of statement
Code: 0
URL: file:///C:/Users/[redacted]/Downloads/HotlexView.hta

Do you want to continue running scripts on this page?

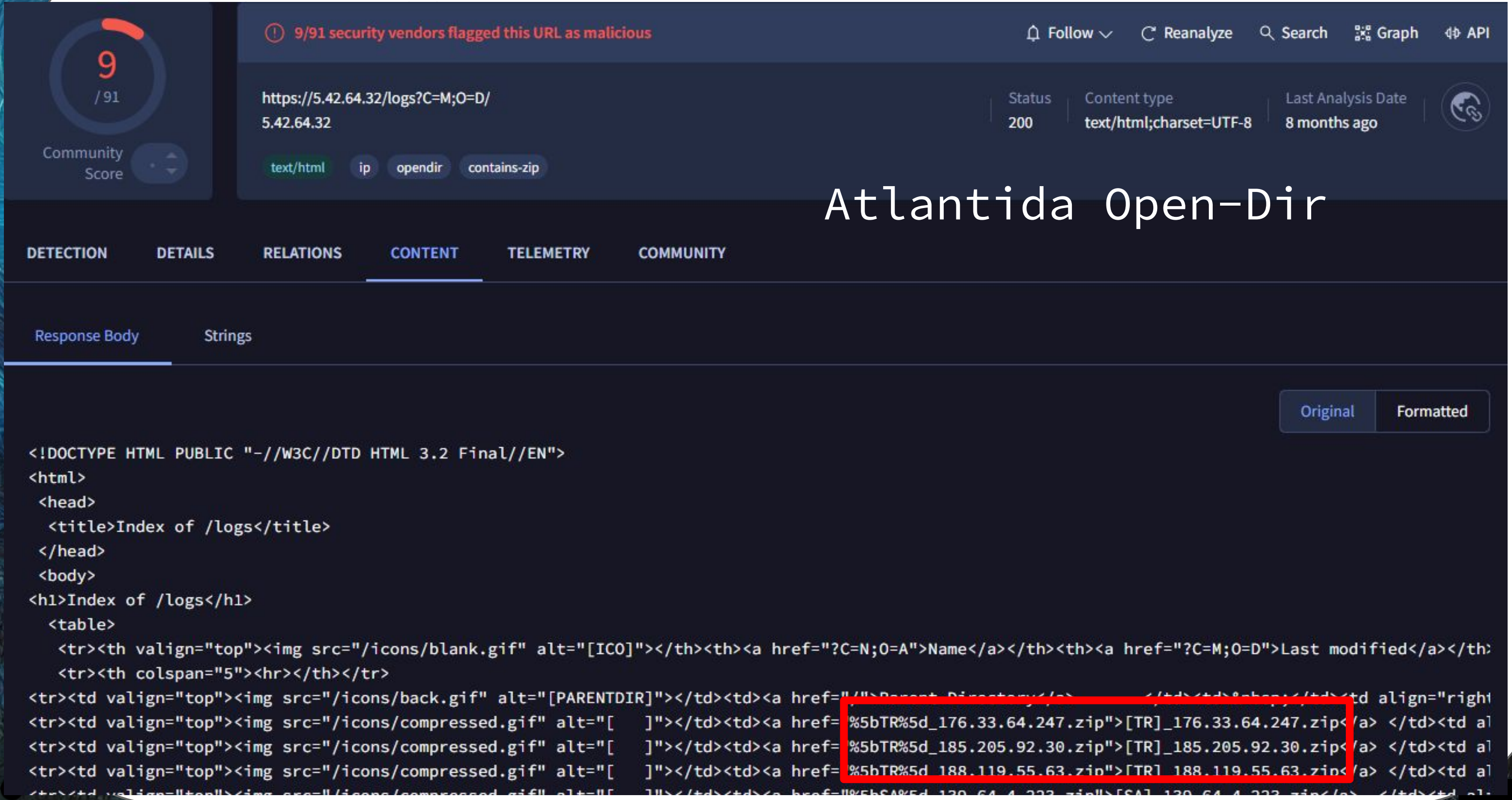
Yes No

```
True
```

Typical REPO

- Searchable **tags**
- **Phishy** README.md
- **Download link** in README.md
  - Link to external website
  - Release of other repo
  - Password protected archive
- High number of **stargazers**
- Usually recently updated

Atlantida Open-Dir



9/91 security vendors flagged this URL as malicious

https://5.42.64.32/logs?C=M;O=D/
5.42.64.32

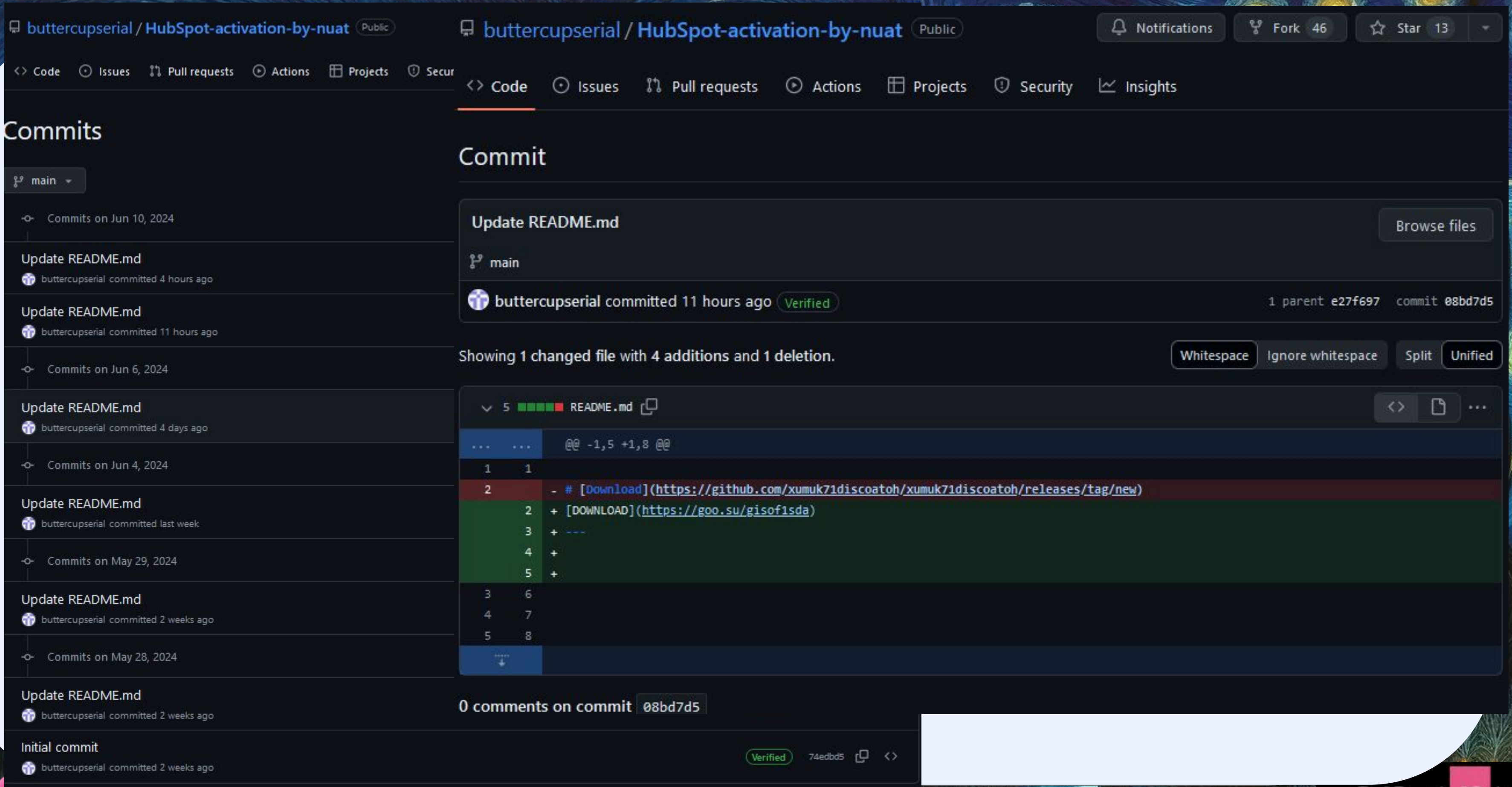
text/html   ip   opendir   contains-zip

Status: 200
Content type: text/html;charset=UTF-8
Last Analysis Date: 8 months ago

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /logs</title>
 </head>
 <body>
<h1>Index of /logs</h1>
  <table>
   <tr><th valign="top"><img src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;O=A">Name</a></th><th><a href="?C=M;O=D">Last modified</a></th
   <tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[PARENTDIR]"></td><td><a href="/">Parent Directory</a>       </td><td>&nbsp;</td><td align="right
<tr><td valign="top"><img src="/icons/compressed.gif" alt="[   ]"></td><td><a href="%5bTR%5d_176.33.64.247.zip">[TR]_176.33.64.247.zip</a> </td><td al
<tr><td valign="top"><img src="/icons/compressed.gif" alt="[   ]"></td><td><a href="%5bTR%5d_185.205.92.30.zip">[TR]_185.205.92.30.zip</a> </td><td al
<tr><td valign="top"><img src="/icons/compressed.gif" alt="[   ]"></td><td><a href="%5bTR%5d_188.119.55.63.zip">[TR]_188.119.55.63.zip</a> </td><td al
<tr><td valign="top"><img src="/icons/compressed.gif" alt="[   ]"></td><td><a href="%5bSA%5d_139.64.4.223.zip">[SA]_139.64.4.223.zip</a>  </td><td al
```

Operator: Stargazer Goblin

- Operates & Maintains **Stargazers Ghost Network**
- Public since **July 2023**
- Smaller scale since **August 2022**
- Campaigns focused mainly social media targets utilizing **Atlantida Stealer**



buttercupserial / HubSpot-activation-by-nuat Public

Commits

main

Commits on Jun 10, 2024

Update README.md
buttercupserial committed 4 hours ago

Update README.md
buttercupserial committed 11 hours ago

Commits on Jun 6, 2024

Update README.md
buttercupserial committed 4 days ago

Commits on Jun 4, 2024

Update README.md
buttercupserial committed last week

Commits on May 29, 2024

Update README.md
buttercupserial committed 2 weeks ago

Commits on May 28, 2024

Update README.md
buttercupserial committed 2 weeks ago

Initial commit
buttercupserial committed 2 weeks ago Verified 74edbd5

buttercupserial / HubSpot-activation-by-nuat Public

Commit

Update README.md

main

buttercupserial committed 11 hours ago Verified 1 parent e27f697 commit 08bd7d5

Showing 1 changed file with 4 additions and 1 deletion.

5 README.md

```
@@ -1,5 +1,8 @@

- # [Download](https://github.com/xumuk71discoatoh/xumuk71discoatoh/releases/tag/new)
+ [DOWNLOAD](https://goo.su/gisof1sda)
+ ---
+
+



```

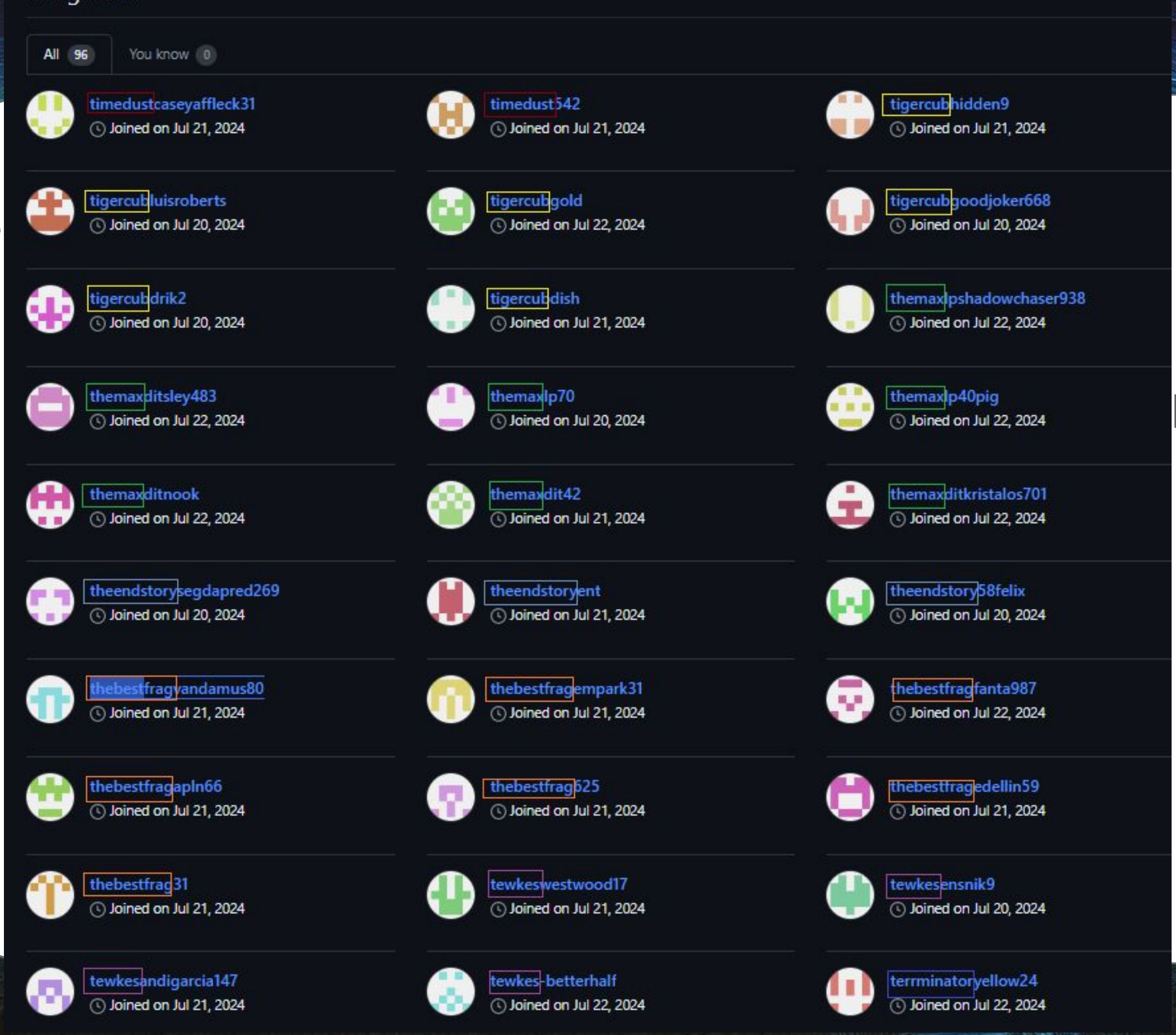
0 comments on commit 08bd7d5

G

-

-

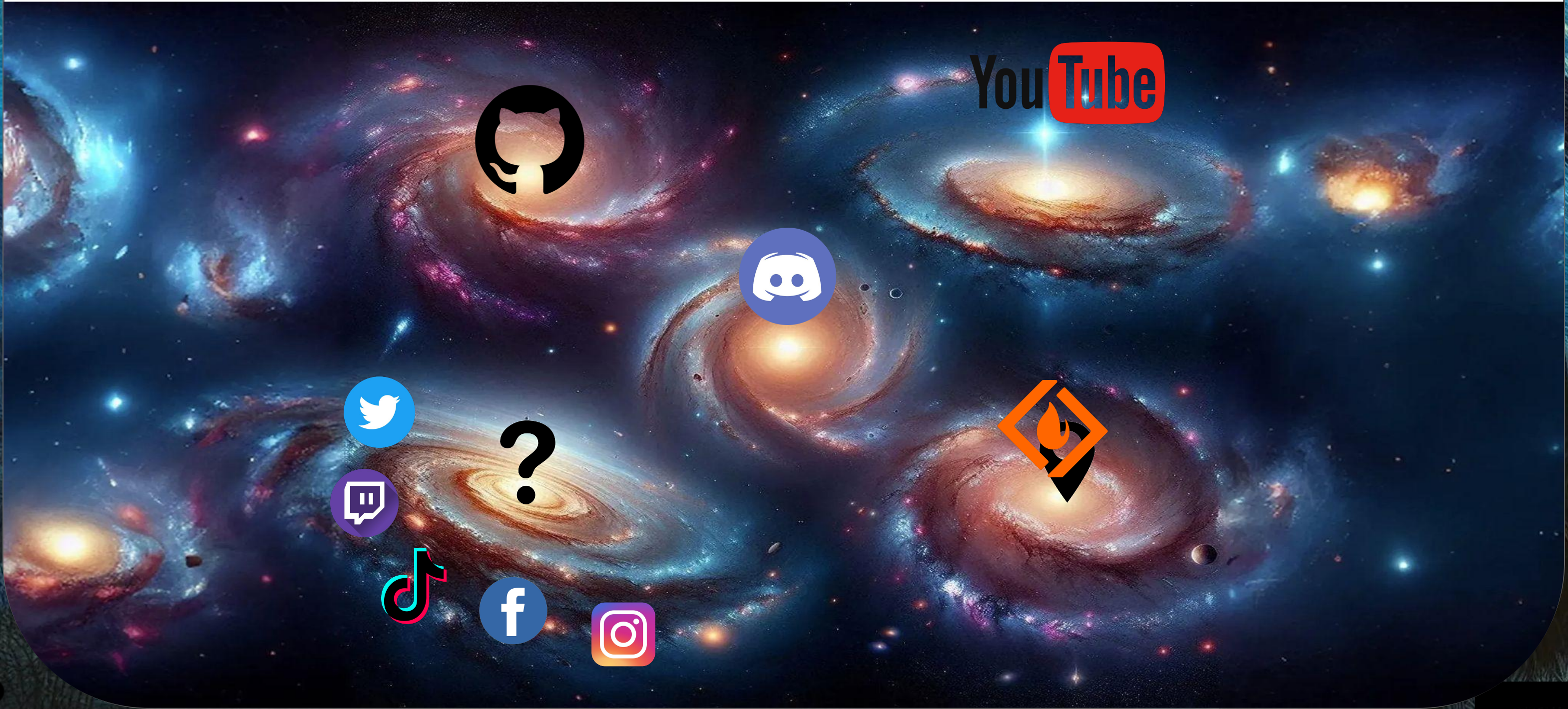
he

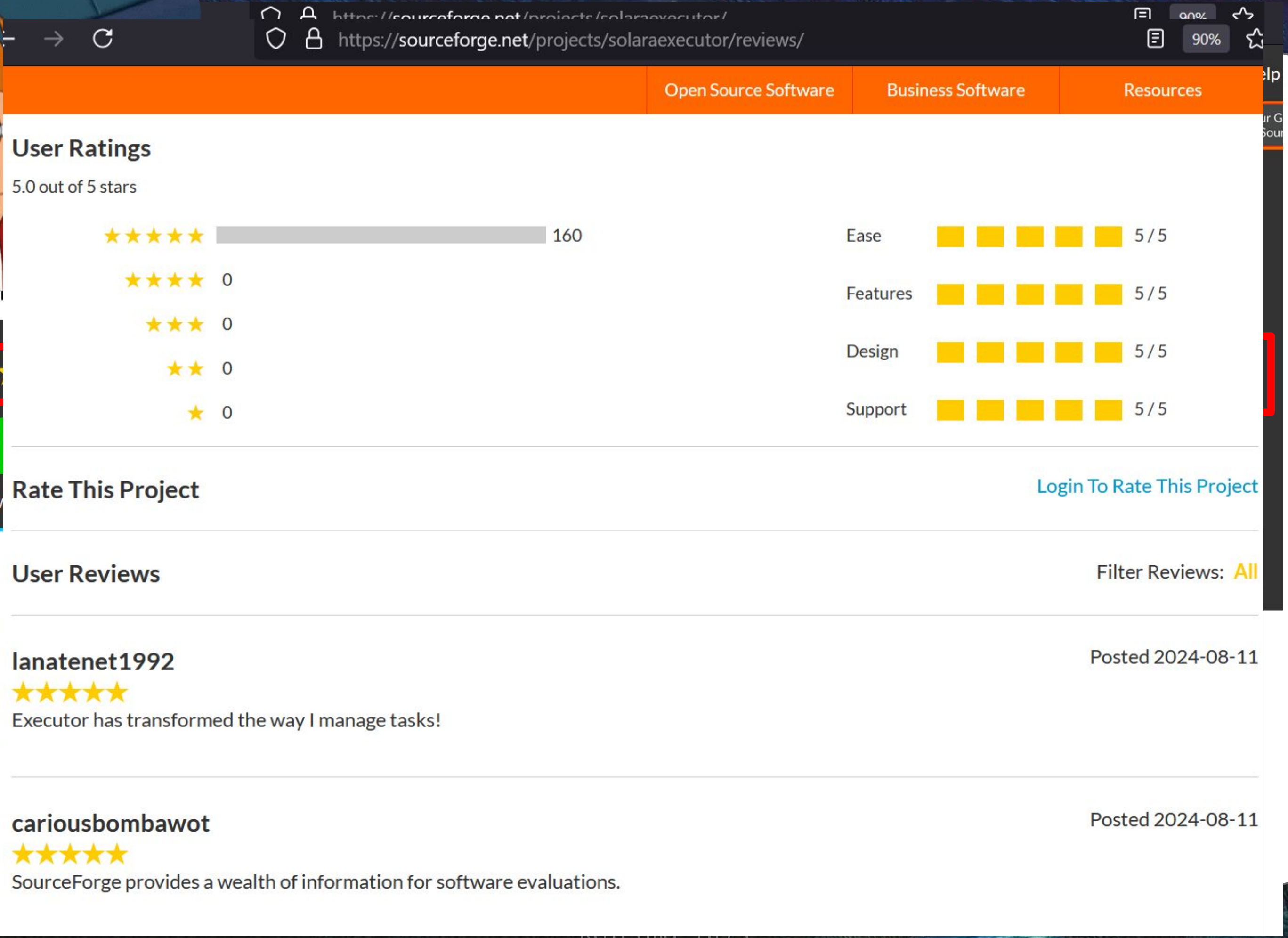


All 96 | You know 0

timedustcaseyaffleck31 Joined on Jul 21, 2024
timedust542 Joined on Jul 21, 2024
tigercubhidden9 Joined on Jul 21, 2024
tigercubluisroberts Joined on Jul 20, 2024
tigercubgold Joined on Jul 22, 2024
tigercubgoodjoker668 Joined on Jul 20, 2024
tigercubdrik2 Joined on Jul 20, 2024
tigercubdish Joined on Jul 21, 2024
themaxlpshadowchaser938 Joined on Jul 22, 2024
themaxditsley483 Joined on Jul 22, 2024
themaxlp70 Joined on Jul 20, 2024
themaxlp40pig Joined on Jul 22, 2024
themaxditnook Joined on Jul 22, 2024
themaxdit42 Joined on Jul 21, 2024
themaxditkristalos701 Joined on Jul 22, 2024
theendstorysegdapred269 Joined on Jul 20, 2024
theendstoryent Joined on Jul 21, 2024
theendstory58felix Joined on Jul 20, 2024
thebestfragvandamus80 Joined on Jul 21, 2024
thebestfragempark31 Joined on Jul 21, 2024
thebestfragfanta987 Joined on Jul 22, 2024
thebestfragapln66 Joined on Jul 21, 2024
thebestfrag625 Joined on Jul 21, 2024
thebestfragedellin59 Joined on Jul 21, 2024
thebestfrag31 Joined on Jul 21, 2024
tewkeswestwood17 Joined on Jul 21, 2024
tewkesensnik9 Joined on Jul 20, 2024
tewkesandigarcia147 Joined on Jul 21, 2024
tewkes-betterhalf Joined on Jul 22, 2024
terrminatoryellow24 Joined on Jul 22, 2024

Ghost Network Universe





https://sourceforge.net/projects/solaraexecutor/
https://sourceforge.net/projects/solaraexecutor/reviews/
90%
Open Source Software
Business Software
Resources

User Ratings

5.0 out of 5 stars

★★★★★	160
★★★★	0
★★★	0
★★	0
★	0

Ease	5 / 5
Features	5 / 5
Design	5 / 5
Support	5 / 5

Rate This Project

Login To Rate This Project

User Reviews

Filter Reviews: All

lanatenet1992 Posted 2024-08-11

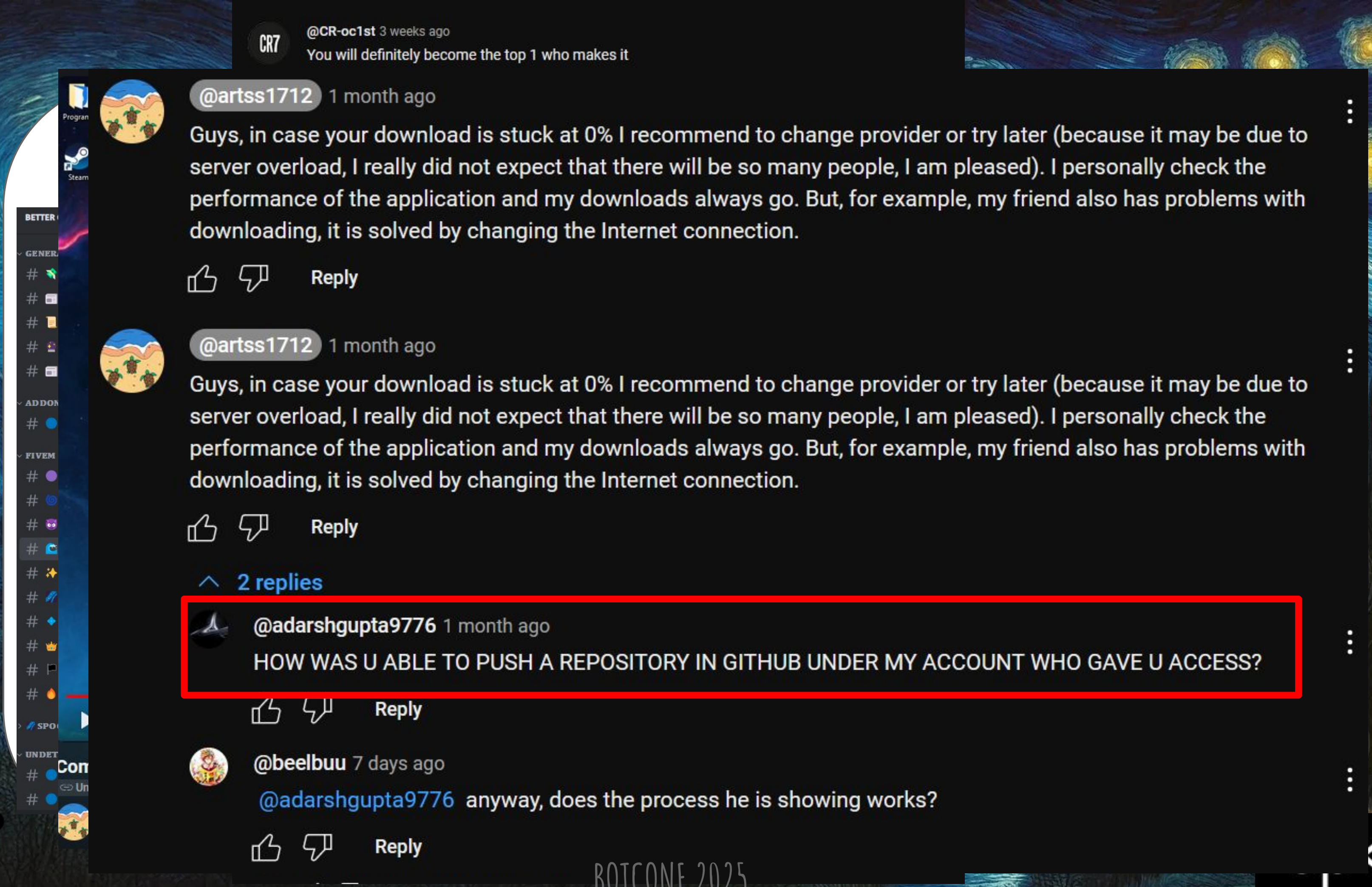
★★★★★

Executor has transformed the way I manage tasks!

cariousbombawot Posted 2024-08-11

★★★★★

SourceForge provides a wealth of information for software evaluations.



@CR-oc1st 3 weeks ago

You will definitely become the top 1 who makes it

@artss1712 1 month ago

Guys, in case your download is stuck at 0% I recommend to change provider or try later (because it may be due to server overload, I really did not expect that there will be so many people, I am pleased). I personally check the performance of the application and my downloads always go. But, for example, my friend also has problems with downloading, it is solved by changing the Internet connection.

@artss1712 1 month ago

Guys, in case your download is stuck at 0% I recommend to change provider or try later (because it may be due to server overload, I really did not expect that there will be so many people, I am pleased). I personally check the performance of the application and my downloads always go. But, for example, my friend also has problems with downloading, it is solved by changing the Internet connection.

2 replies

@adarshgupta9776 1 month ago

HOW WAS U ABLE TO PUSH A REPOSITORY IN GITHUB UNDER MY ACCOUNT WHO GAVE U ACCESS?

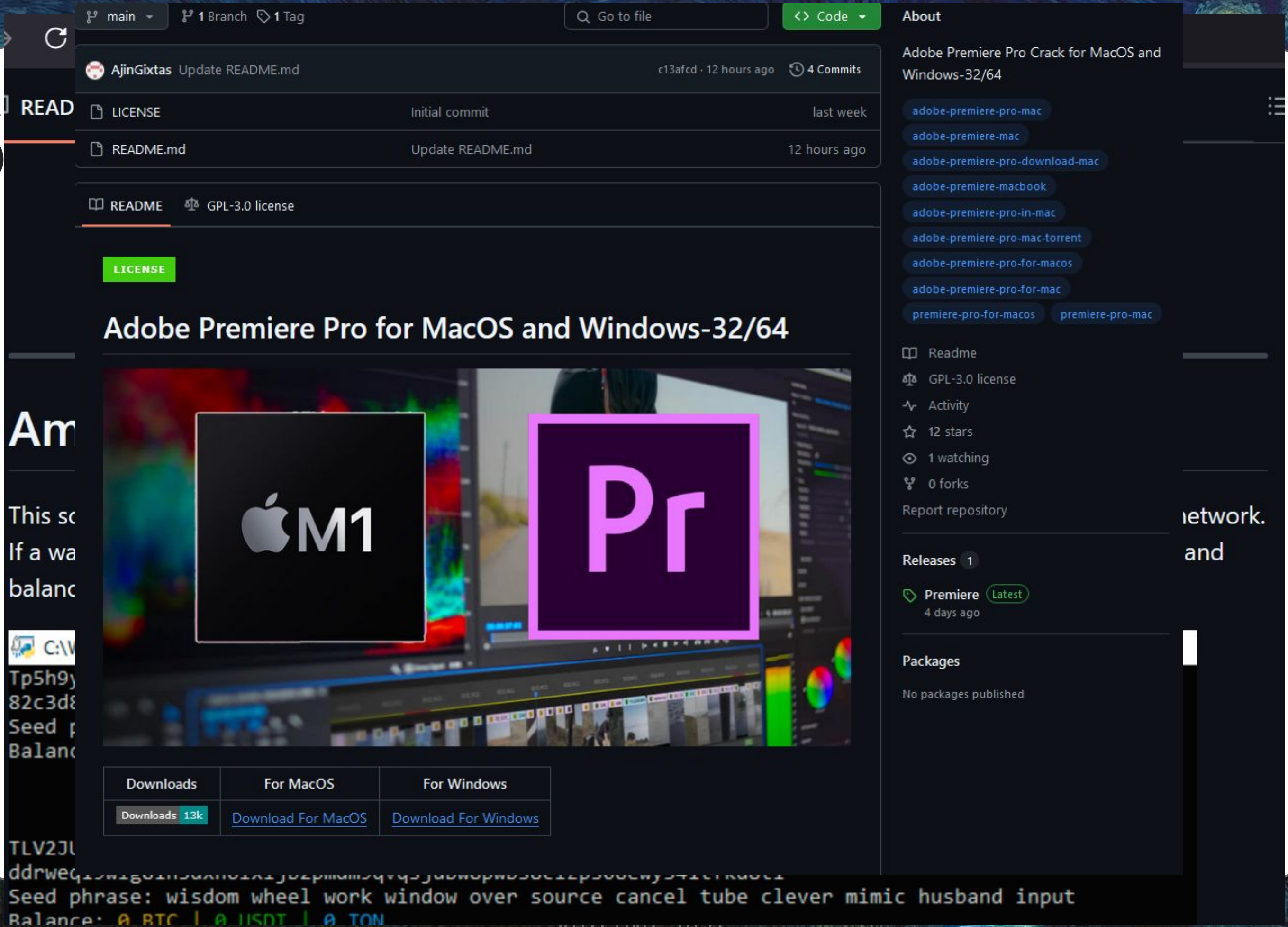
@beelbuu 7 days ago

@adarshgupta9776 anyway, does the process he is showing works?

MALWARE DISTRIBUTED VIA NETWORKS

- Atlantida
- Rhadamanthys
- Lumma
- Medusa
- RedLine
- RisePro
- Python Stealers
- …

IS



main | 1 Branch | 1 Tag | Go to file | Code

AjinGixtas Update README.md c13afcd · 12 hours ago 4 Commits

LICENSE	Initial commit	last week
README.md	Update README.md	12 hours ago

README | GPL-3.0 license

LICENSE

Adobe Premiere Pro for MacOS and Windows-32/64

Downloads	For MacOS	For Windows
Downloads 13k	Download For MacOS	Download For Windows

About

Adobe Premiere Pro Crack for MacOS and Windows-32/64

adobe-premiere-pro-mac
adobe-premiere-mac
adobe-premiere-pro-download-mac
adobe-premiere-macbook
adobe-premiere-pro-in-mac
adobe-premiere-pro-mac-torrent
adobe-premiere-pro-for-macos
adobe-premiere-pro-for-mac
premiere-pro-for-macos premiere-pro-mac

Readme
GPL-3.0 license
Activity
12 stars
1 watching
0 forks
Report repository

Releases 1

Premiere Latest
4 days ago

Packages

No packages published

READ

Am

This sc ... network.
If a wa ... and
balanc

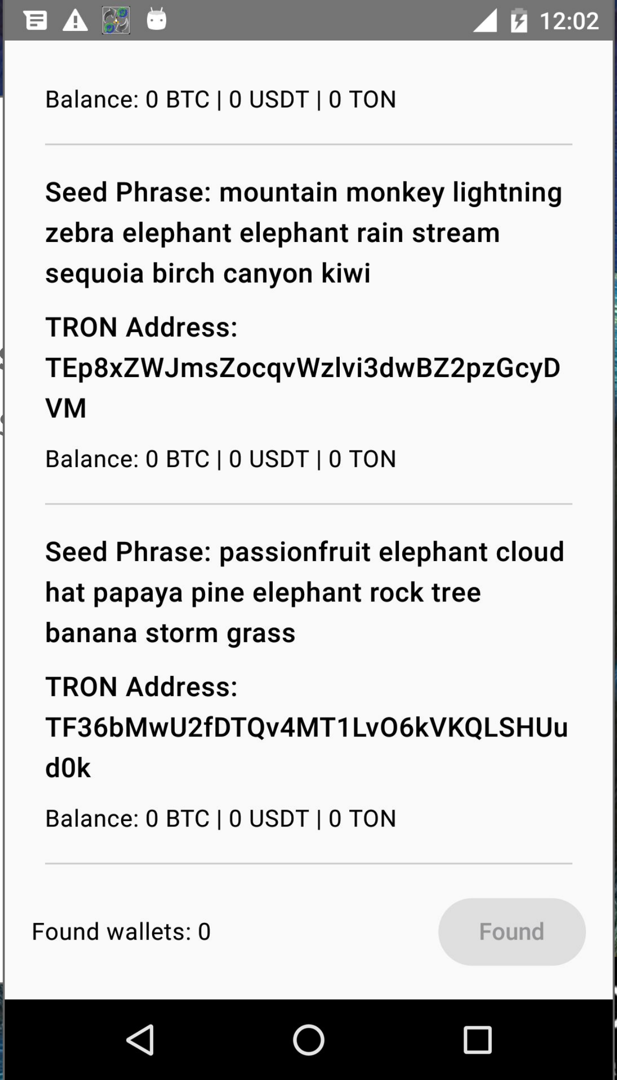
```
C:\
Tp5h9y
82c3d8
Seed p
Balanc
TLV2JU
ddrweq
Seed phrase: wisdom wheel work window over source cancel tube clever mimic husband input
Balance: 0 BTC | 0 USDT | 0 TON
```

CHECK POINT

cp<r> CHECK POINT RESEARCH

DUAL OS - ANDROID INFECTIONS

- In **2 days - 24 Android infection**
- Actor possibly of **Russian** origin
- File Stealer
- Victims:
  - **US - 13**
  - **RU/UA/NL - 2**
  - **DE/PL/CZ/IN/TR - 1**



Balance: 0 BTC | 0 USDT | 0 TON

Seed Phrase: mountain monkey lightning zebra elephant elephant rain stream sequoia birch canyon kiwi

TRON Address: TEp8xZWJmsZocqvWzlvi3dwBZ2pzGcyDVM

Balance: 0 BTC | 0 USDT | 0 TON

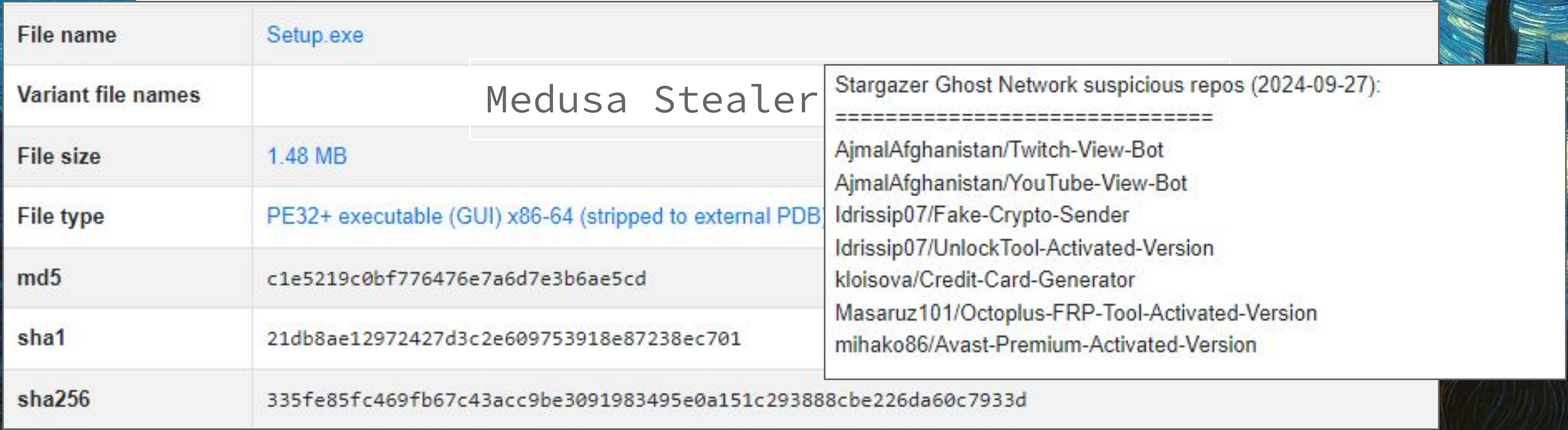
Seed Phrase: passionfruit elephant cloud hat papaya pine elephant rock tree banana storm grass

TRON Address: TF36bMwU2fDTQv4MT1LvO6kVKQLSHUud0k

Balance: 0 BTC | 0 USDT | 0 TON

Found wallets: 0

Monitoring Stargazers Ghost Network



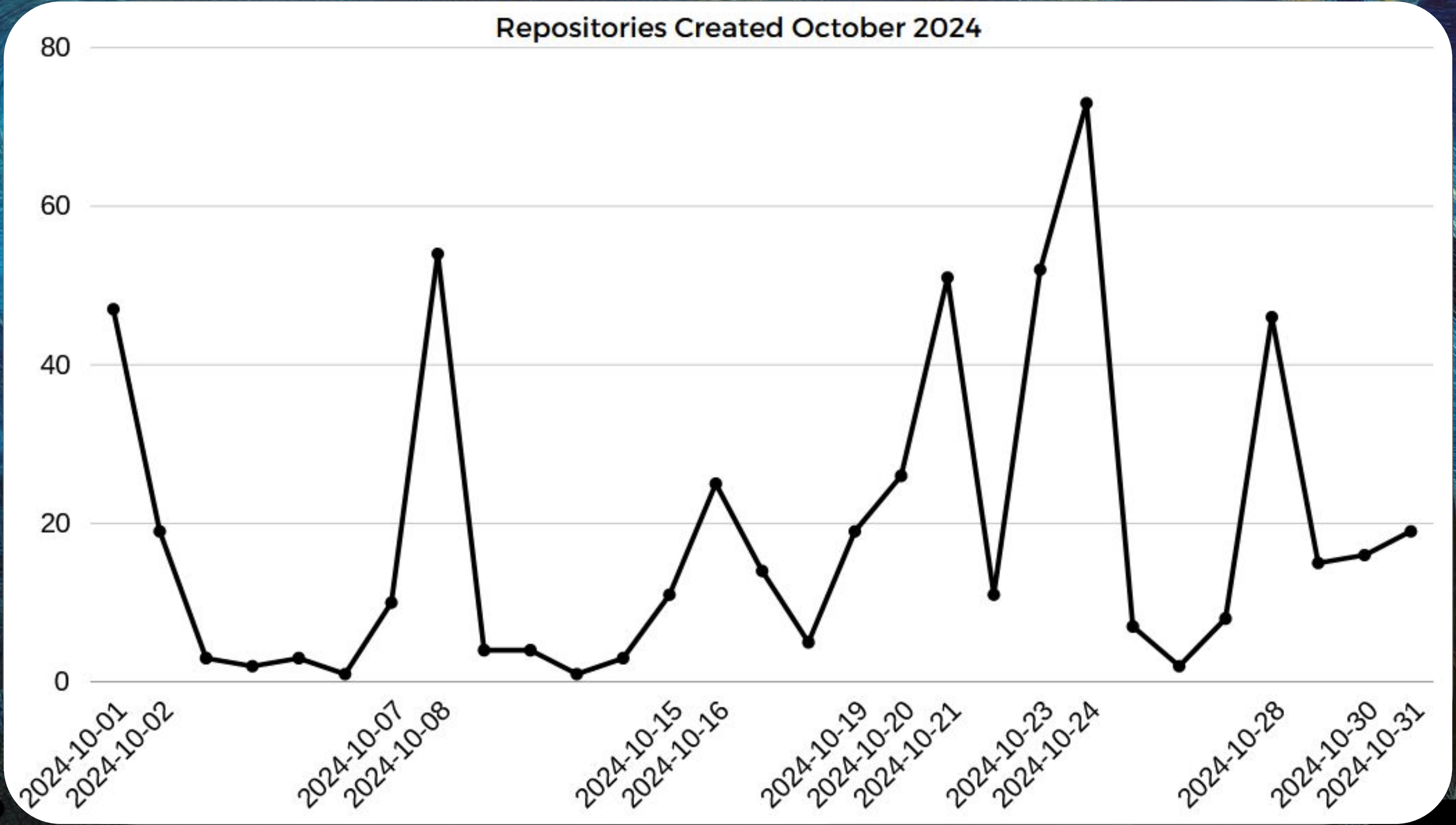
File name	Setup.exe
Variant file names	
File size	1.48 MB
File type	PE32+ executable (GUI) x86-64 (stripped to external PDB)
md5	c1e5219c0bf776476e7a6d7e3b6ae5cd
sha1	21db8ae12972427d3c2e609753918e87238ec701
sha256	335fe85fc469fb67c43acc9be3091983495e0a151c293888cbe226da60c7933d

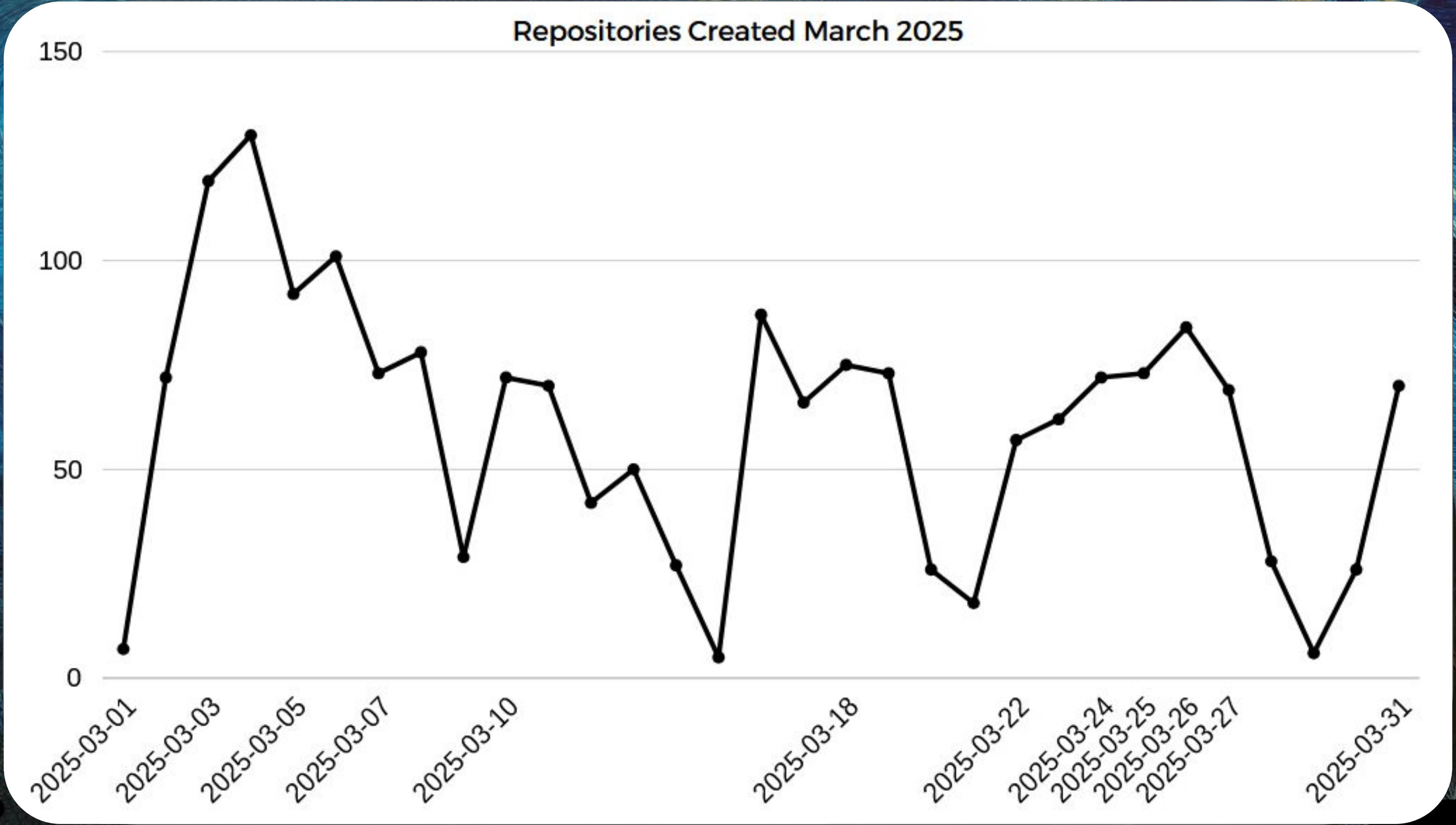
Medusa Stealer

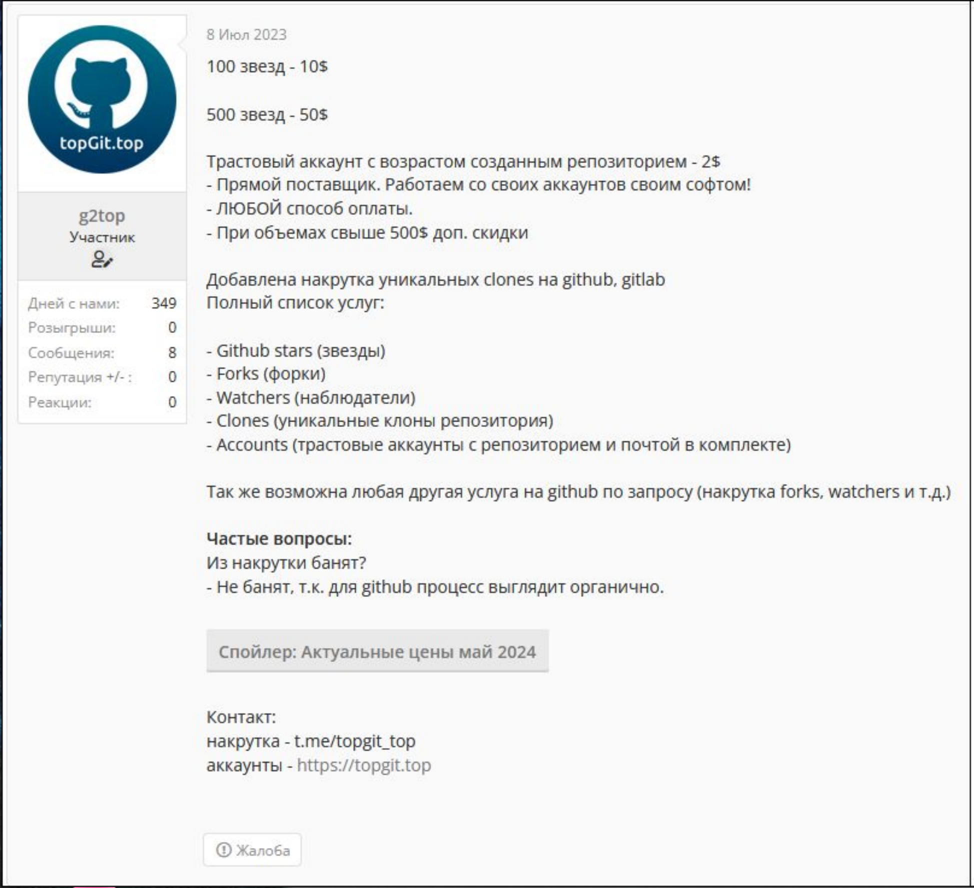
```
Stargazer Ghost Network suspicious repos (2024-09-27):
================================
AjmalAfghanistan/Twitch-View-Bot
AjmalAfghanistan/YouTube-View-Bot
Idrissip07/Fake-Crypto-Sender
Idrissip07/UnlockTool-Activated-Version
kloisova/Credit-Card-Generator
Masaruz101/Octoplus-FRP-Tool-Activated-Version
mihako86/Avast-Premium-Activated-Version
```

SIZE(STARGAZERS_GHOST_NETWORK)

- Constant changing number
  - Increases when:
    - Creating new accounts
    - Obtaining credentials of compromised accounts
  - Decreases when:
    - Legitimate user changes credentials
    - GitHub bans accounts


Repositories Created October 2024
80
60
40
20
0
2024-10-01
2024-10-02
2024-10-07
2024-10-08
2024-10-15
2024-10-16
2024-10-19
2024-10-20
2024-10-21
2024-10-23
2024-10-24
2024-10-28
2024-10-30
2024-10-31


Repositories Created March 2025
150
100
50
0
2025-03-01
2025-03-03
2025-03-05
2025-03-07
2025-03-10
2025-03-18
2025-03-22
2025-03-24
2025-03-25
2025-03-26
2025-03-27
2025-03-31



Дней с нами:	349
Розыгрыши:	0
Сообщения:	8
Репутация +/- :	0
Реакции:	0

8 Июл 2023

100 звезд - 10$

500 звезд - 50$

Трастовый аккаунт с возрастом созданным репозиторием - 2$
- Прямой поставщик. Работаем со своих аккаунтов своим софтом!
- ЛЮБОЙ способ оплаты.
- При объемах свыше 500$ доп. скидки

Добавлена накрутка уникальных clones на github, gitlab
Полный список услуг:

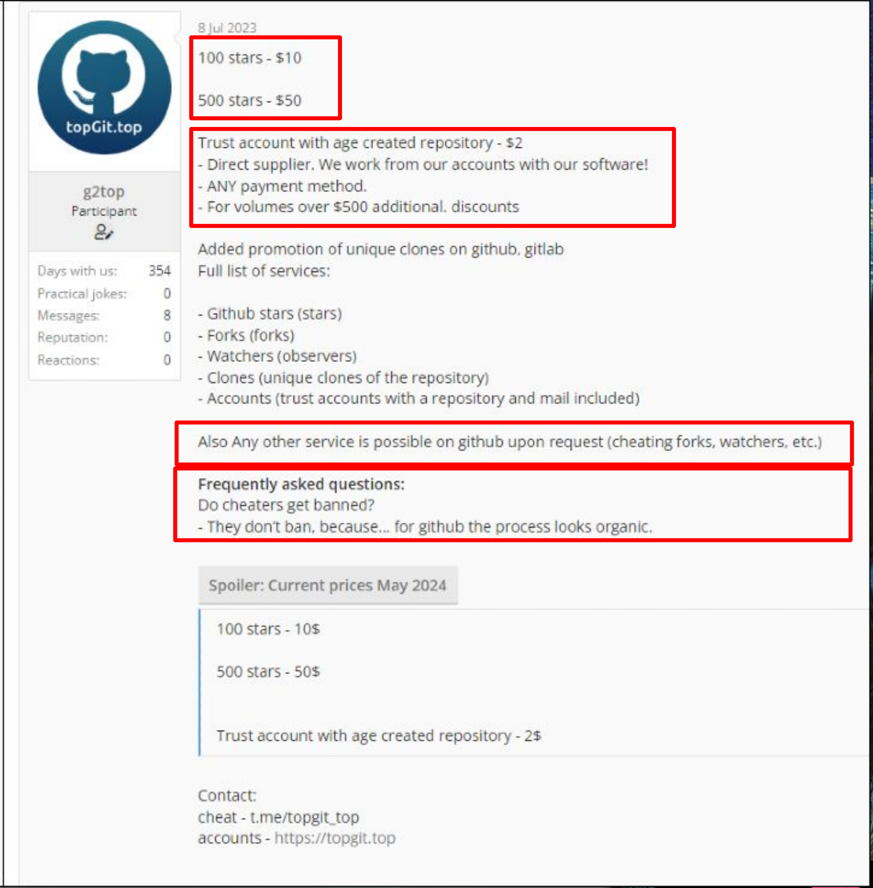
- Github stars (звезды)
- Forks (форки)
- Watchers (наблюдатели)
- Clones (уникальные клоны репозитория)
- Accounts (трастовые аккаунты с репозиторием и почтой в комплекте)

Так же возможна любая другая услуга на github по запросу (накрутка forks, watchers и т.д.)

Частые вопросы:
Из накрутки банят?
- Не банят, т.к. для github процесс выглядит органично.

Спойлер: Актуальные цены май 2024

Контакт:
накрутка - t.me/topgit_top
аккаунты - https://topgit.top



Days with us:	354
Practical jokes:	0
Messages:	8
Reputation:	0
Reactions:	0

8 Jul 2023

100 stars - $10

500 stars - $50

Trust account with age created repository - $2
- Direct supplier. We work from our accounts with our software!
- ANY payment method.
- For volumes over $500 additional. discounts

Added promotion of unique clones on github, gitlab
Full list of services:

- Github stars (stars)
- Forks (forks)
- Watchers (observers)
- Clones (unique clones of the repository)
- Accounts (trust accounts with a repository and mail included)

Also Any other service is possible on github upon request (cheating forks, watchers, etc.)

Frequently asked questions:
Do cheaters get banned?
- They don't ban, because... for github the process looks organic.

Spoiler: Current prices May 2024

100 stars - 10$

500 stars - 50$

Trust account with age created repository - 2$

Contact:
cheat - t.me/topgit_top
accounts - https://topgit.top

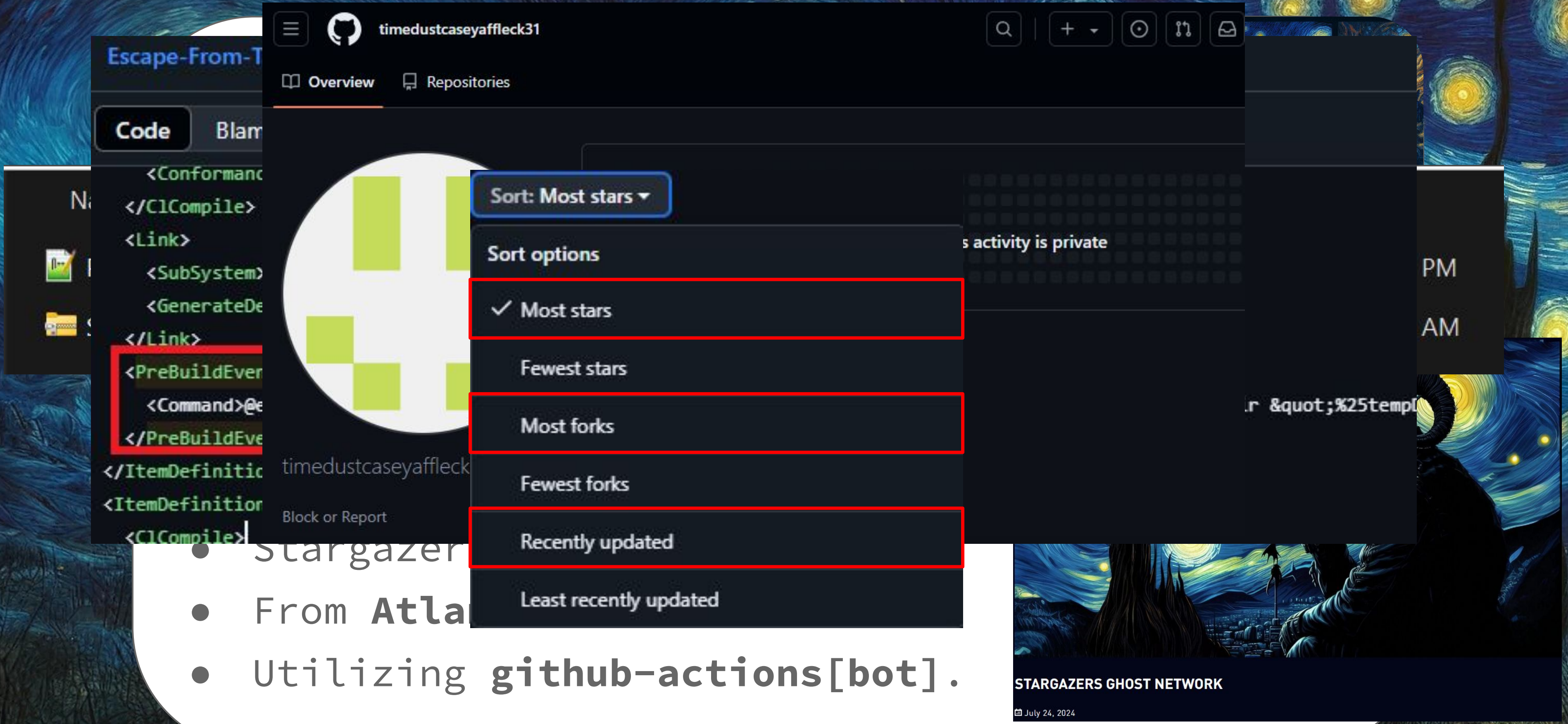
GENERATED PROFIT

October 2024, Profit ~**14.7K USD**

- **113786** stars -> ~**11.4K** USD
- **551** repositories -> ~**1.1K** USD
- **14964** forks -> ~**2.2K** USD

March 2025, Profit ~**17.8K USD**

- **54356** stars -> ~**12K** USD
- **1859** repositories -> ~**3.7K** USD
- **13834** forks -> ~**2K** USD



```
    <Conformanc
  </ClCompile>
  <Link>
    <SubSystem>
    <GenerateDe
  </Link>
  <PreBuildEven
    <Command>@e
  </PreBuildEve
</ItemDefinitic
<ItemDefinition
  <ClCompile>
```

```
r &quot;%25templ
```

- Stargazer
- From **Atla**
- Utilizing **github-actions[bot]**.

CONCLUSION

- Ghost Networks break social actions trust by misusing various platforms engagement tools.
- Stargazers Ghost Network, is highly profitable and Threat actors achieve great infection rates.

Questions?

Contact

@Tera0017