Paweł Murdzek, Piotr Szewczyk
grupa Latexowe Rękawiczki
Raport
Osint-ctf dzień 2

**Konta szerzące hejt:**
wol58465
WolnyMurarz45
h4s666oc
57callitrichepa
96bletillastria
disoro137740
kr00xmox
99Adiantumvenus
39callapalustr
janpawel954
kowalski120801
88cyrtomiumfort
00Adiantumpedat
jaruuudon
55Cyrtomiumfalc
darmera42166
bagdhi230153
87blechnumspica
29Achilleaptarm
echinops32952
44BerulaErecta
dryoppo80208
bigun47637
deephakuna2
55Acoruscalamus
ropsis213303
Konta retweetują się nawzajem, nie tylko jedną jednostkę centralną - wzajemna adoracja.
**Uruchomienie narzędzi automatyzujących pracę:**
**maigret --file usernames.txt --pdf --html**
**cat usernames.txt | xargs python3 sherlock.py**

Target,Type
wol58465,Username
WolnyMurarz45,Username
h4s666oc,Username
57callitrichepa,Username
96bletillastria,Username
disoro137740,Username
kr00xmox,Username
99Adiantumvenus,Username
39callapalustr,Username
janpawel954,Username

kowalski120801,Username
88cyrtomiumfort,Username
00Adiantumpedat,Username
jaruuudon,Username
55Cyrtomiumfalc,Username
darmera42166,Username
bagdhi230153,Username
87blechnumspica,Username
29Achilleaptarm,Username
echinops32952,Username
44BerulaErecta,Username
dryoppo80208,Username
bigun47637,Username
deephakuna2,Username
55Acoruscalamus,Username
ropsis213303,Username

**SpiderFoot**

Username,Full URL,Tag
wol58465,https://x.com/wol58465,BotnetSuspect
WolnyMurarz45,https://x.com/WolnyMurarz45,BotnetSuspect
h4s666oc,https://x.com/h4s666oc,BotnetSuspect
57callitrichepa,https://x.com/57callitrichepa,BotnetSuspect
96bletillastria,https://x.com/96bletillastria,BotnetSuspect
disoro137740,https://x.com/disoro137740,BotnetSuspect
kr00xmox,https://x.com/kr00xmox,BotnetSuspect
99Adiantumvenus,https://x.com/99Adiantumvenus,BotnetSuspect
39callapalustr,https://x.com/39callapalustr,BotnetSuspect
janpawel954,https://x.com/janpawel954,BotnetSuspect
kowalski120801,https://x.com/kowalski120801,BotnetSuspect
88cyrtomiumfort,https://x.com/88cyrtomiumfort,BotnetSuspect
00Adiantumpedat,https://x.com/00Adiantumpedat,BotnetSuspect
jaruuudon,https://x.com/jaruuudon,BotnetSuspect
55Cyrtomiumfalc,https://x.com/55Cyrtomiumfalc,BotnetSuspect
darmera42166,https://x.com/darmera42166,BotnetSuspect
bagdhi230153,https://x.com/bagdhi230153,BotnetSuspect
87blechnumspica,https://x.com/87blechnumspica,BotnetSuspect
29Achilleaptarm,https://x.com/29Achilleaptarm,BotnetSuspect
echinops32952,https://x.com/echinops32952,BotnetSuspect
44BerulaErecta,https://x.com/44BerulaErecta,BotnetSuspect
dryoppo80208,https://x.com/dryoppo80208,BotnetSuspect
bigun47637,https://x.com/bigun47637,BotnetSuspect
deephakuna2,https://x.com/deephakuna2,BotnetSuspect
55Acoruscalamus,https://x.com/55Acoruscalamus,BotnetSuspect
ropsis213303,https://x.com/ropsis213303,BotnetSuspect

**maltego**

Spiderfoot nie znalazł nic, jednak wyszukiwanie po nickach za pomocą Sherlock znalazło obecność nicków na rosyjskich platformach:

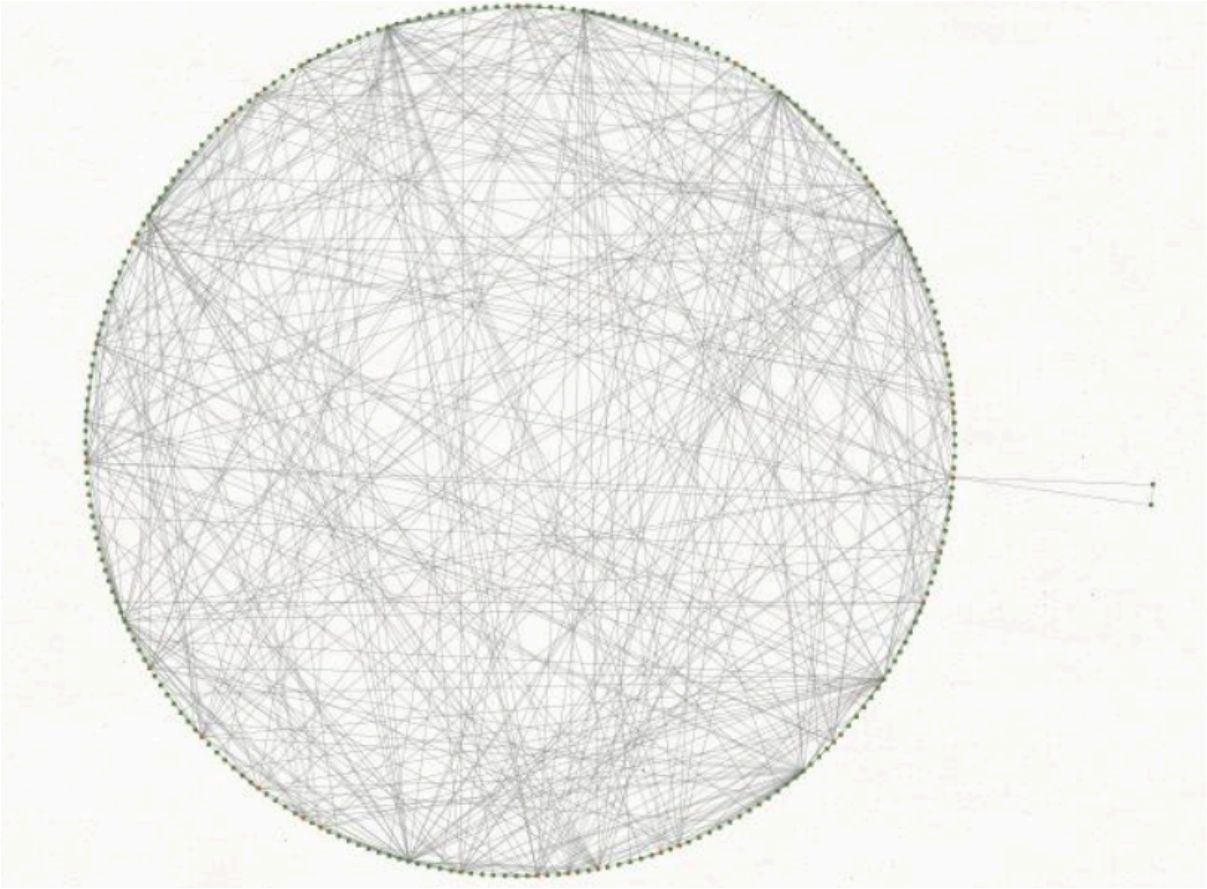
- **php.ru (Forum programistyczne) –** Występuje u m. in.: **00Adiantumpedat**, **39callapalustr**, **57callitrichepa**, **88cyrtomiumfort**.
- **svidbook.ru (Rosyjski serwis) –** Występuje u m. in.: **39callapalustr**, **88cyrtomiumfort**.
- **music.yandex (Yandex to rosyjski odpowiednik Google) –** Występuje u u m. in.: **88cyrtomiumfort**.

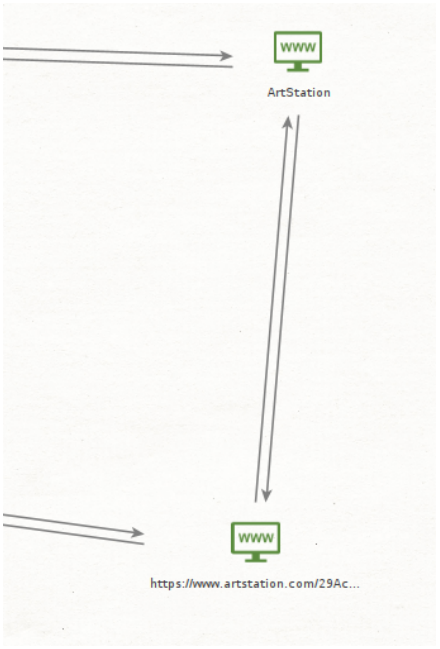
Większość z tych kont ma także konta na platformach:

- Coders Rank
- Envato Forum
- GNOME VCS (GitLab)
- HackenProof
- NationStates
- Patched
- SpeakerDeck

Co wskazuje na istnienie skryptu tworzącego konta (Ogrzewanie).

**Raport maltego wykazał anomalie:**
https://www.artstation.com/29Achilleaptarm
29Achilleaptarmica to jest jedyne konto, które wykracza poza standardową sieć pajęczą botów.




WWW
ArtStation
WWW
https://www.artstation.com/29Ac...

**https://whatsmyname.me/**
znalazło mi te linki, dużo kont jest usuniętych:
https://mastodon.social/api/v2/search?q=29Achilleaptarm&type=accounts

{"accounts":[{"id":"115445582288702594","username":"29Achilleaptarm","acct":"29Achilleaptarm@mas.to","display_name":"29Achilleaptarm","locked":false,"bot":false,"discoverable":true,"indexable":true,"group":false,"created_at":"2025-10-27T00:00:00.000Z","note":"","url":"https://mas.to/@29Achilleaptarm","uri":"https://mas.to/users/29Achilleaptarm","avatar":"https://files.mastodon.social/cache/accounts/avatars/115/445/582/288/702/594/original/f6abe5623d93cd1c.jpg","avatar_static":"https://files.mastodon.social/cache/accounts/avatars/115/445/582/288/702/594/original/f6abe5623d93cd1c.jpg","header":"https://mastodon.social/headers/original/missing.png","header_static":"https://mastodon.social/headers/original/missing.png","followers_count":0,"following_count":0,"statuses_count":1,"last_status_at":"2025-10-27","hide_collections":false,"emojis":[],"fields":[]}],"statuses":[],"hashtags":[]}

https://sourceforge.net/u/29Achilleaptarm/profile

https://speakerdeck.com/29Achilleaptarm/


https://www.udemy.com/user/29Achilleaptarm/

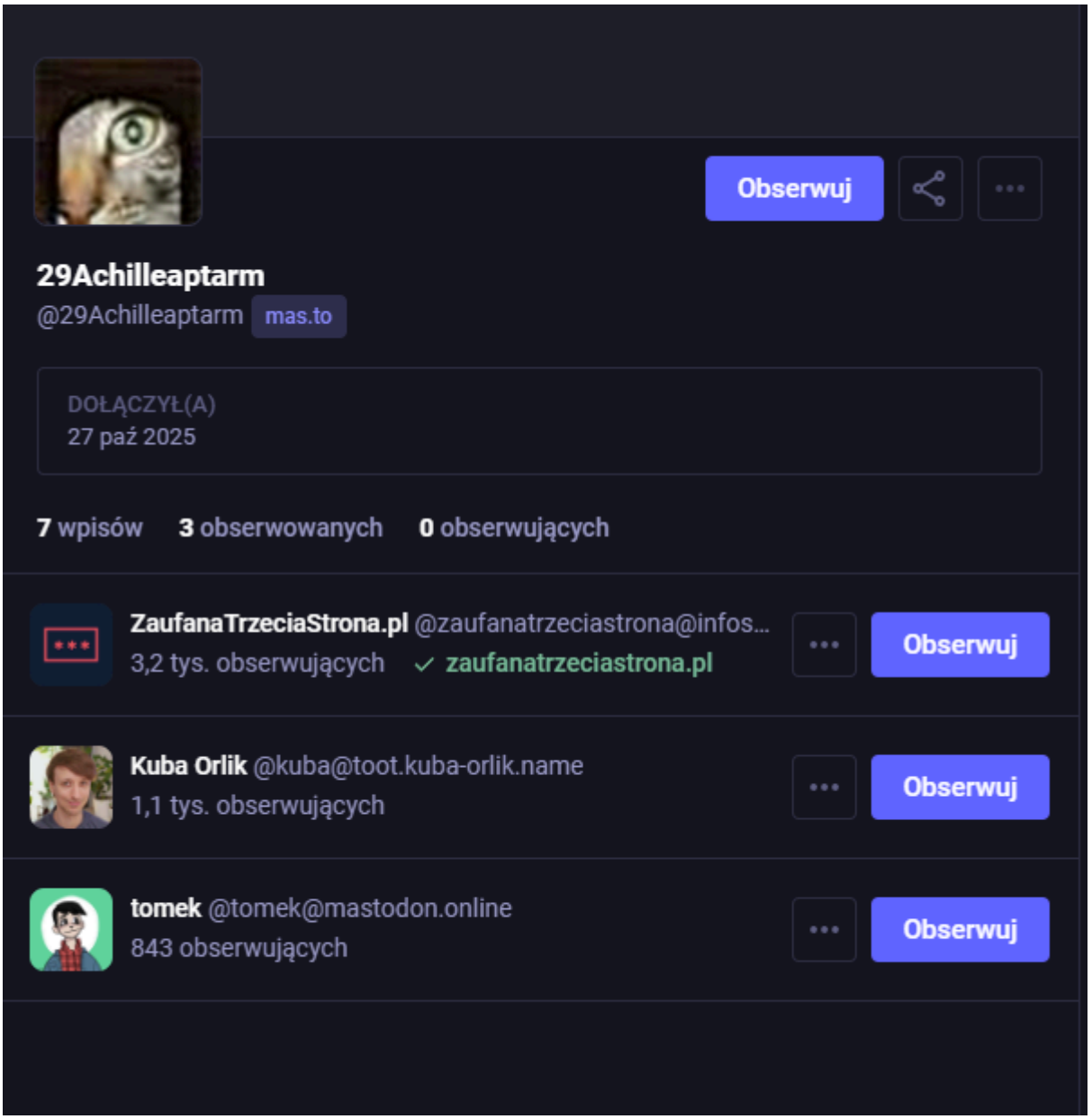
Na stronie speakerdeck.com znaleźliśmy zdjęcie profilowe z nickiem, ale jest to prawdopodobnie przypadkowy użytkownik

Używając pythonowego narzędzia *maigret*, również natknęliśmy się na wyszukania użytkownika z w/w nickiem:

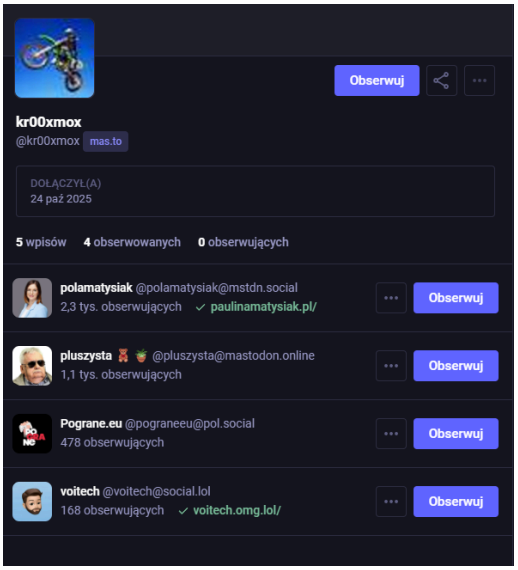
```
643
644 Searching |                                        | ▁▁ 162/2669 [6%] in 4s (~1
645 on 162:
646 [-] Codecanyon: Not found!
647
648 Searching |                                        | ▁▁ 162/2669 [6%] in 4s (~1
649 on 162:
650 [+] Kaggle: https://www.kaggle.com/29Achilleaptarm
651
652 Searching |                                        | ▁▁ 162/2669 [6%] in 4s (~1
653 on 162:
654 [-] linktr.ee: Not found!
655
656 Searching |                                        | ▁▁ 162/2669 [6%] in 4s (~1
657 on 162:
658 [-] OK: Illegal Username Format For This Site!
659
```

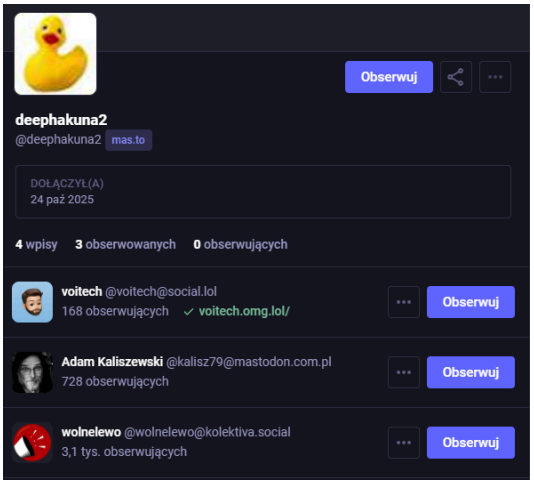
**Strona mastodon przekierowała nas na stronę:**
https://mas.to/@29Achilleaptarm

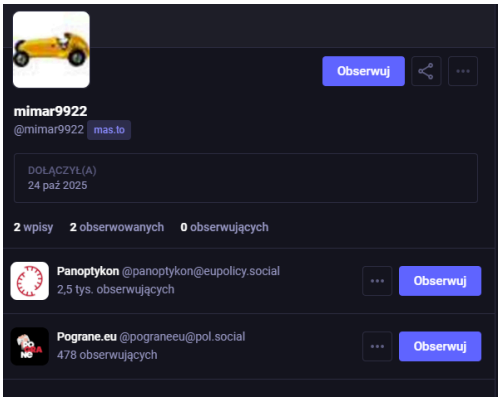
Konto śledzi na matodonie 3 inne konta, wszystkie z polski:



Inne konta też funkcjonują na platformie, obserują tylko albo 0 albo 3-4 profile z polski:




Pacjent zero to konto **mimar9922** https://mas.to/@mimar9922/
Konto jest już zbanowane na twitterze jako bot
*"discoverable": false,*
*"indexable": false*
w profilu wskazują na to, że jest on prywatny - możliwe że zarządca najpierw go testował w ukryciu.