



Social OSINT fundamentals

v 0.0.1

SPEAKER: @soxoj

ABOUT ME

- Security engineer
- Antifraud systems developer
- OSINT enthusiast
- DEFCON7495 speaker



https://t.me/osint_mindset





Humans are naturally lazy.



Humans are naturally lazy.

CONCLUSION

They use the same nicknames, accounts, passwords, etc.



Search by nickname



- The most important search
- “Attack” surface determination
- Enough to find everything about person



(It's fiction)

Branding tools: not bros



Namech_k NOT BROS 🔍 ☰

Domains

Help keep Namechk free | [Donate PayPal](#)

.com	.net	.org	.co	.biz	.io	.at	.us	.me	.co.uk	.eu	.info
.xyz	.ca	.be	.am	.tv	.la	.life	.ch	.ms	.in	.club	.bar
.tech	.site	.online	.store	.space	.website	.fun	.host	.press	.digital	.today	.farm

Click an **available** or **premium** domain to purchase it. Click an **unavailable** domain to make an offer for it.

A green banner advertisement for GoDaddy .online domains. On the left, the text ".online" is displayed in a large, white, sans-serif font. Below it, in a smaller white font, is the text "I Choose a .online domain." On the right side of the banner, the GoDaddy logo (a stylized figure holding a lightning bolt) is shown next to the word "GoDaddy" in white. Below the logo, the text "Get .online domains" is written in a smaller white font. At the bottom right, there is a dark blue rectangular button with the text "BUY NOW" in white, uppercase letters.

Having difficulty finding a good name or brand? Try



Username

Namecheckers: bros

DC7495 ONLINE
Social OSINT fundamentals
dc7495.org



Welcome to WhatsMyName

This tool allows you to enumerate usernames across many websites

How to use:

1. Enter the username below, select any filters & click the search icon
2. Results will present as icons on the left, & in a searchable table on the right

Authors

WebBreacher, Munchko, L0r3m1p5um, lehuff, janbinx, bcoles,
Sector035, armydo, mccartney, salaheidinaz, camhoff, jocephus,
OSINT Combine



Search Username:



Filter by Category:



Found: 119 Processed: 254 / 255

[Show All](#)[Show Found](#)[Show Not Found](#)

Pastebin

Category: tech
Account Found

Disqus

Category: social
Account Found

Spotify

Category: music
Account Found

OpenStreetMap

Category: social
Account Found

Minecraft

Category: gaming
Account Found

GitHub

Category: coding
Account Found

Playlists.net

Category: music
Account Found

Blogspot

Category: blog
Account Found

Chess.com

Category: gaming
Account Found

Behance

Category: business
Account Found

themeforset

Category: art
Account Found

Audiojungle

Category: music
Account Found

Show entries

Search:

SITE	CATEGORY	LINK	FOUND?
500px	images	Open	☹️
7cup	social	Open	👍
9GAG	social	Open	👍
about.me	social	Open	👍
AngelList	tech	Open	☹️
aNobii	hobby	Open	☹️
appearoo	social	Open	☹️
ArmorGames	gaming	Open	👍
asciinema	coding	Open	👋

What's wrong with namecheckers?



- Not an OSINT tools in general (let's face it)
- False positives
- Poorly maintained
- No normal reports
- No important features such as screenshots/archiving, proxies auto select, extracting info, etc.

<https://telegra.ph/Whats-wrong-with-namecheckers-07-05> (RUS)

Actual list of the best namecheckers



OSINT namecheckers list

A list of tools to search accounts by username with pros and cons.

Scripts

Sherlock

- hunts down social media accounts by username across around 300 social networks
- has web-cli deployments 👍
- batch search 👍
- tor & proxy support 👍
- alexa top ranking 👍
- adding custom sites & rules
- csv reports
- false positives

Snoop

- sherlock fork, all its pros and cons so
- 67 sites in demo version, 1182 sites in full version 👍
- country ranking & filtering 👍
- html and csv reports

Maigret

- sherlock fork, all its pros and cons so
- 400+ sites 👍
- profile pages parsing and extracting personal info, links to other profiles, etc. 👍

<https://github.com/soxoj/osint-namecheckers-list>

Search by nickname: maigret



- 400+ sites for now, increasing rapidly
- Pages parsing and extracting personal info, links to other profiles, etc.
- Recursive search by new usernames found
- Censorship and captcha detection
- Very few false positives



<https://github.com/soxoj/maigret>

Accounts linking through SSO



Welcome back.



Sign in with Google



Sign in with Facebook



Sign in with Apple



Sign in with Twitter



Sign in with email

Войти



Имя пользователя



Пароль



Запомнить меня

[Забыли пароль?](#)

Войти

Или



Facebook



ВКонтакте

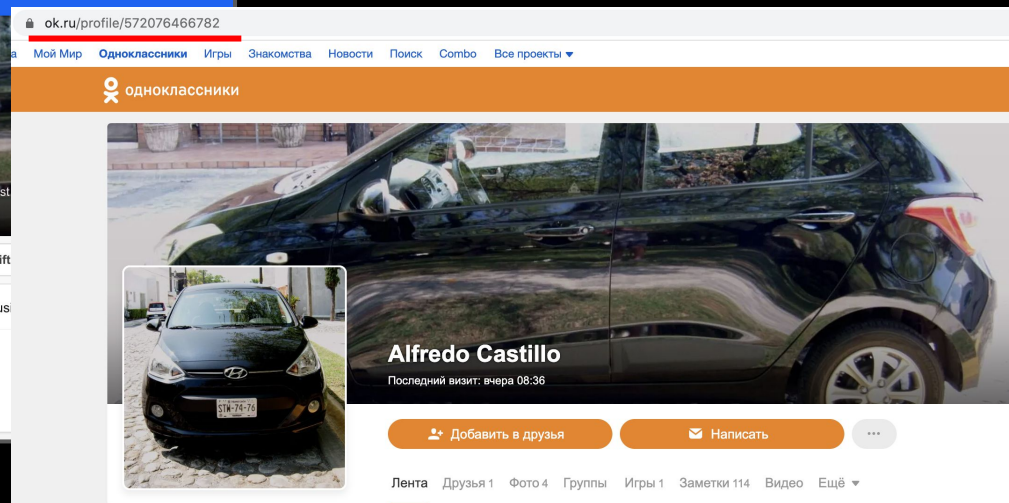
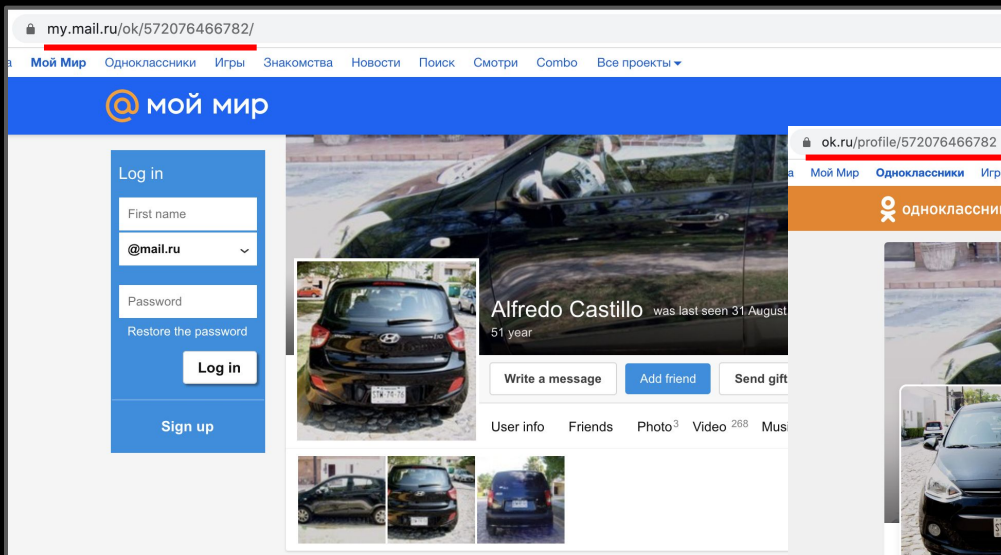


Google



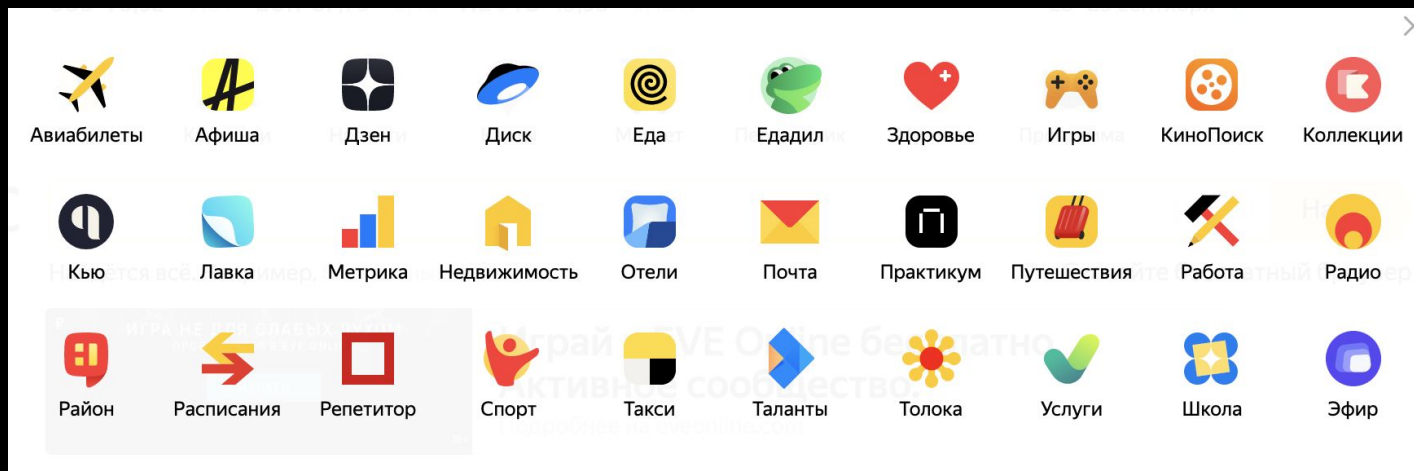
Accounts linking through SSO: example

DC7495 ONLINE
Social OSINT fundamentals
dc7495.org



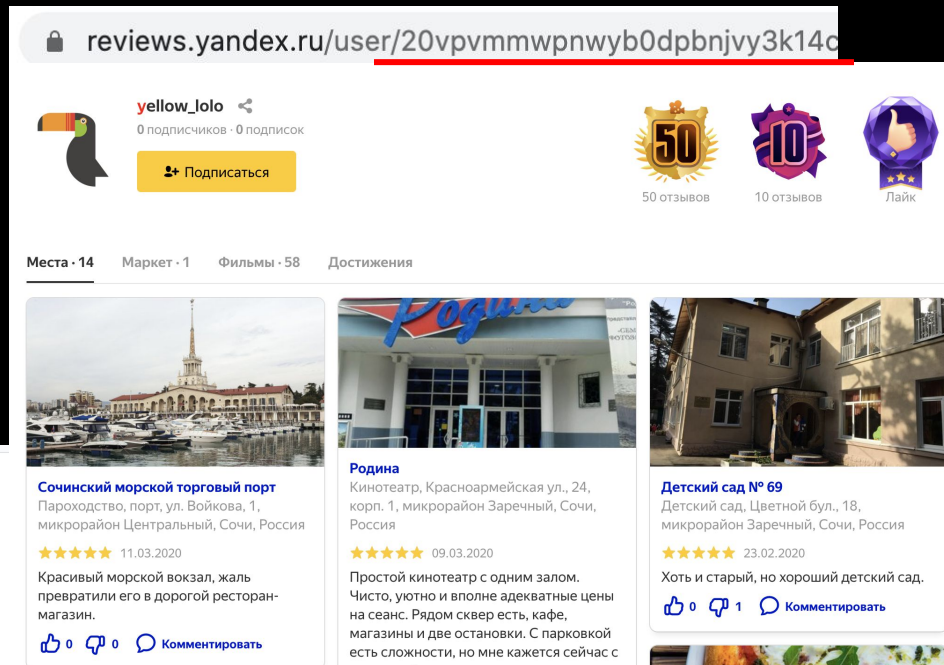
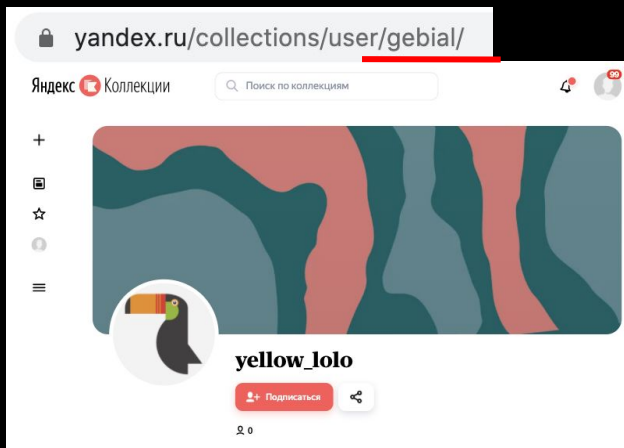
<https://my.mail.ru/ok/572076466782/> ⇔ <https://ok.ru/profile/572076466782/>

Accounts linking in related services



Accounts linking in related services: example

DC7495 ONLINE
Social OSINT fundamentals
dc7495.org



```
1 {  
2   "_url": "/collections/api/users/gebial",  
3   "id": "58f1df702a6f9300c29e3440",  
4   "public_id": "20vpvmmwpnwyb0dpbnjvy3k14c",  
5   "display_name": "yellow_lolo",  
6   "sex": "m",  
7   "phone_id": null,  
8   "is_forbid": false,  
9   "is_restricted": false,  
10  "is_verified": false,  
11  "is_km": false,  
12  "is_business": false,  
13  "is_subscribed": false,  
14  "is_passport": true,  
15  "url": "https://internal.collections.yandex.ru/collections/user/20vpvmmwpnwyb0dpbnjvy3k14c/"
```

Maigret, find'em all



```
$ python3 maigret --parse https://vk.com/rzrvrt - --ids --print-found --skip-errors
Extracted ID data from webpage: vk_id: 337779600, vk_username: rzrvrt, fullname: Миша Нежной
```

[*] Checking vk_id 337779600 on:

[+] My.Mail.ru@VK: https://my.mail.ru/vk/337779600

```
-uid: 2068355204
-username: 337779600
-email: 337779600@vk
-name: Разрыв Аорты
-isVip: False
-isCommunity: False
-isVideoChannel: False
```

[*] Checking username rzrvrt on:

[+] Pinterest: https://www.pinterest.com/rzrvrt/

[+] VK: https://vk.com/rzrvrt

```
-vk_id: 337779600
-vk_username: rzrvrt
-fullname: Миша Нежной
```

[+] Vimeo: https://vimeo.com/rzrvrt

```
-uid: 65024371
-name: Razryv Aorty
```

```
$ python3 maigret gebial --ids --print-found --skip-errors
```

[*] Checking username gebial on:

[+] YandexCollection: https://yandex.ru/collections/user/gebial/

```
-id: 58f1df702a6f9300c29e3440
-name: yellow_lolo
-yandex_public_id: 20vpvmmwprnwyb0dpbnjvy3k14c
```

[+] YandexMusic: https://music.yandex.ru/users/gebial/playlists

```
-yandex_uid: 19664080
-username: gebial
-name: yellow_lolo
```

[*] Checking yandex_public_id 20vpvmmwprnwyb0dpbnjvy3k14c on:

[+] Yandex: https://yandex.ru/user/20vpvmmwprnwyb0dpbnjvy3k14c

[+] YandexLocal: https://local.yandex.ru/users/20vpvmmwprnwyb0dpbnjvy3k14c

[+] YandexZnatoki: https://yandex.ru/q/profile/20vpvmmwprnwyb0dpbnjvy3k14c

Search site owner by adv. analytics IDs



Reverse Google Analytics ID

Use this tool to perform a reverse lookup of a Google Analytics ID. Make sure to enter it WITHOUT the "UA-" part. For example try: 4406282

Enter the Google Analytics ID without the 'UA-' part

Search

- ☐ DNSlytics ☐ HackerTarget ☐ Moonsearch ☐ DomainMetrics ☐ PublicWWW
- ☐ analyzeid

Select All

Important: Make sure that popups are allowed. If you don't see all new tabs opened after hitting search, go back to this tab and enable popups when your browser asks (Chrome: Right side in the URL bar).

Disclaimer: We are not responsible for any 3rd party services and their results.

<https://intelx.io/tools?tab=analytics>

Search site owner by adv. analytics IDs: example

DC7495 ONLINE
Social OSINT fundamentals
dc7495.org



Home -> Reverse Tools -> Reverse Analytics -> ua-28511072

Reverse Google® Analytics

Find domains sharing the same Analytics ID.

Enter domain name or Analytics ID. Example: qrtuls.com or ua-15589237

Reverse Analytics lookup for: ua-28511072

Found 4 domains using Analytics ID: ua-28511072.

#	Domain	Tools
1	<u>alum-sochi.ru</u>	<input type="button" value="Search"/> <input type="button" value="Typos"/> <input type="button" value="History"/> <input type="button" value="Whois"/>
First seen using this Analytics ID on 2018-05-19 , last checked on 2020-06-19 . DomainRank: 0.6/10 Name servers: ns1.hostiman.ru (used by 10,233 domains) ns2.hostiman.ru (used by 10,236 domains) ns3.hostiman.com (used by 9,823 domains) used by 9,815 domains Mail servers: mail.alum-sochi.ru (used by 1 domain) IPv4: 137.74.81.5 (used by 145 domains) Google Analytics ID: ua-28511072 (used by 4 domains)		
2	<u>ozge.ru</u>	<input type="button" value="Search"/> <input type="button" value="Typos"/> <input type="button" value="History"/> <input type="button" value="Whois"/>
First seen using this Analytics ID on 2019-03-09 , last checked on 2020-07-11 .		

host.io

About Documentation Rankings

Domains with Google Analytics ID UA-28511072

There are 3 domains having the Google Analytics ID UA-28511072.

ozge.ru	alum-sochi.ru	<u>xn-----ctbampbl8axd1ewb.xn--p1ai</u>
---------	---------------	---

domashnie-tsvety.ru
ozge.ru

Google Analytics 28511072
Unique tracking code of Google Analytics web-site statistics service 1

Domains	Moon Rank	Page Rank	Alexa	Dmoz	Yahoo
<u>ozge.ru</u>	<input type="text" value="0"/> / 10	<input type="text" value="0"/> / 10	—	<input type="button" value="✖"/>	<input type="button" value="✖"/>

Using breaches and common passwords to get linked emails



_IntelligenceX

test@test.com

 Found 194 Text Files, 4 Database Files, 1 PDF File, 1 Word File

[Collection 1/Collection #1_OLD CLOUD_BTC combos.tar.gz/Collection #1_OLD CLOUD_BTC combos/57.txt](#)

5722222@mail.ru;417905
larsen0112@hotmail.com;princess01
terkelsorensen@gmail.com;xxcjxx1999
mr.mantis@qwe.ru;223122
vaz-ru@mail.ru;9222304490
cafisher@suddenlink.net;fish6108
hz-speel@hahc.org.uk;m3di4n
tj3456@yahoo.com;Rtj222

[Collection 1/Collection #1_OLD CLOUD_BTC combos.tar.gz/Collection #1_OLD CLOUD_BTC combos/52.txt](#)

qgillis18@sjastudents.org;kitsue978
albert1988@gmail.com;Ae769209212
HOLLYWOODDIR@ATMC.NET;001249
lbell@mediaartistsgroup.com;berko4
partyinwis@aol.com;st0lting
mkostecka@gmail.com;K7702123858

Google

← Recovery email ?

Your recovery email is used to reach you in case we detect unusual activity in your account or you accidentally get locked out. [Learn more.](#)

Recovery email

@gmail.com

DONE





Humans are by nature social animals.



Accounts linking... to be identified



How to Link Your Social Media Accounts



All



Videos



News




Shopping

About 7,530,000,000 results (0.48 seconds)

Accounts linking... to be identified: example

DC7495 ONLINE
Social OSINT fundamentals
dc7495.org




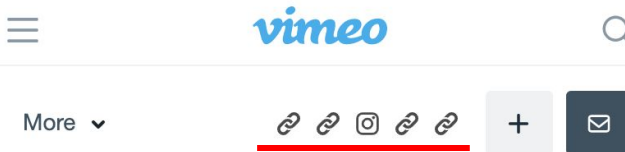
Alex Aimé
📍 Nevers / Brooklyn

[Follow](#)

Photographe Amateur Passionné par l'art J'ai creer son compte pour partager mes photos dans la France et le monde enti... [Read more](#)

363 **Followers** 10 **Following** 13.7K Photo Likes 634.0K Photo impressions ⓘ

[!\[\]\(e5e4ed11b5418bbc3931e5d0c2c8031c_img.jpg\)](#) [!\[\]\(a775cc7674cd110b159cc5ec24961f6c_img.jpg\)](#) [!\[\]\(aab349efd208998288b825e248e914cb_img.jpg\)](#) [!\[\]\(c6b31ff4852ce9d7149f6fbe306dcd9b_img.jpg\)](#)



AlexAimePhotography
📍 France | 14 Videos | 0 Followers | 4 Likes

Maximum of connectedness

DC7495 ONLINE
Social OSINT fundamentals
dc7495.org



lawrencsystems

Thomas Lawrence

Tech Enthusiast, Entrepreneur, Open
Source Advocate, YouTube(r) ,
PodCaster & Hot Sauce Addict!
Southgate MI

Teams



dc313



6 devices



24FF D8D3 8FE1 22FC



tomlawrencetech  tweet



flipsidecreations  gist



flipsidecreations  post



lawrencsystems.com  https



lawrencsystems*keybase.io

Chat with lawrencsystems

Your conversation will be end-to-end encrypted.

Maigret, your turn



[*] Checking username alexaimephotographycars on:

[+] 500px: <https://500px.com/p/alexaimephotographycars>
- uid: dXJpOm5vZGU6VXNlcjoyNjQwMzQxNQ==
- legacy_id: 26403415
- username: alexaimephotographycars
- name: Alex Aimé
- website: www.flickr.com/photos/alexaimephotography/
- facebook_uid: www.instagram.com/street.reality.photography/
- instagram_username: alexaimephotography
- twitter_username: Alexaimephotogr

[*] Checking username alexaimephotography on:

[+] DeviantART: <https://alexaimephotography.deviantart.com>
- country: France
- registered_for_seconds: 54636259
- gender: male
- username: Alexaimephotography
- twitter_username: alexaimephotogr
- website: www.instagram.com/alexaimephotography/
- links:
 - <https://www.instagram.com/alexaimephotography/>

[+] EyeEm: <https://www.eyeem.com/u/alexaimephotography>

[+] Facebook: <https://www.facebook.com/alexaimephotography>

[+] Instagram: <https://www.instagram.com/alexaimephotography>
- uid: 6828488620
- username: alexaimephotography

[+] Picuki: <https://www.picuki.com/profile/alexaimephotography>

[+] Pinterest: <https://www.pinterest.com/alexaimephotography/>

[+] Reddit: <https://www.reddit.com/user/alexaimephotography>

[+] Tumblr: <https://alexaimephotography.tumblr.com/>

[+] VK: <https://vk.com/alexaimephotography>

[+] Vimeo: <https://vimeo.com/alexaimephotography>
- uid: 75857717

Input: alexaimephotographycars



500px found, extracted links and nicknames:
alexaimephotography, Alexaimephotogr,
street.reality.photography



DeviantART, Instagram, Vimeo, etc.
+ 10 sites, + 3 new nicknames



Humans don't pay attention to details



Humans don't pay attention to details

CONCLUSION

They forget to check what they are disclosing about themselves with their files, photos, source code, etc.





```
$ ./gitcolombo.py -u https://github.com/LubyRuffy/cheatsheet
Cloning into 'cheatsheet'...
remote: Enumerating objects: 2184, done.
remote: Total 2184 (delta 0), reused 0 (delta 0), pack-reused 2184
Receiving objects: 100% (2184/2184), 262.14 KiB | 922.00 KiB/s, done.
Resolving deltas: 100% (1412/1412), done.
```

```
-----
INFO: Resolving GitHub usernames, please wait...
Analyze of the git repo(s) "cheatsheet"
Verbose persons info:
-----
```

```
Name:          lubyruffy
Email:         zhaowu@baimaohui.net
Appears as author: 676 times
Appears as committer: 676 times
```

```
Matching info:
-----
```

```
lubyruffy is the owner of emails:
ghost@gitbook.com
zhaowu@baimaohui.net
lubyruffy@gmail.com
```

```
gitbook-bot and Ghost are the same person
```

<https://github.com/soxoj/gitcolombo>

Track 2 files into repository. ...



LubyRuffy committed on 23 Dec 2019

Commits on May 22, 2019

update bash



zhaowu committed on 22 May 2019 ✓

Check for info hidden in public pages



Информация о файле

Имя: **CropNumbers.rar**

Владелец: **MaltsevAnton**

Размер: **264,6 МБ**

Изменён: **21.11.2014 20:59**

Просмотры: **3775**

Скачан: **1679 раз**

Owner of uploaded to Yandex.Disk file



```
$ python3 maigret --parse https://yadi.sk/d/EAFnQ947criHW --ids
Extracted ID data from webpage: yandex_uid: 6107910, name: MaltsevAnton
```

Common pipeline



- Port scan
- Site crawling
- Search files with dork through Google

...

- Extract valuable data from content
- Extract file metadata
- Extract secrets (high entropy strings: tokens, passwords)

...

- ?

How to use found info?



README.md

OSINT tools

Various OSINT tools and scripts, total 133 repos.

Categories

- [Account](#)
 - [Azure](#), [BitBucket](#), [Facebook](#), [GitHub](#), [GitLab](#), [Gmail](#), [Instagram](#), [LinkedIn](#), [QQ](#), [Snapchat](#), [Spotify](#), [Telegram](#), [TikTok](#), [Twitter](#), [VK](#), [WhatsApp](#), [Yandex](#), [YouTube](#)
- [Audio](#)
- [Document](#)
- [Domain](#)
- [Email](#)



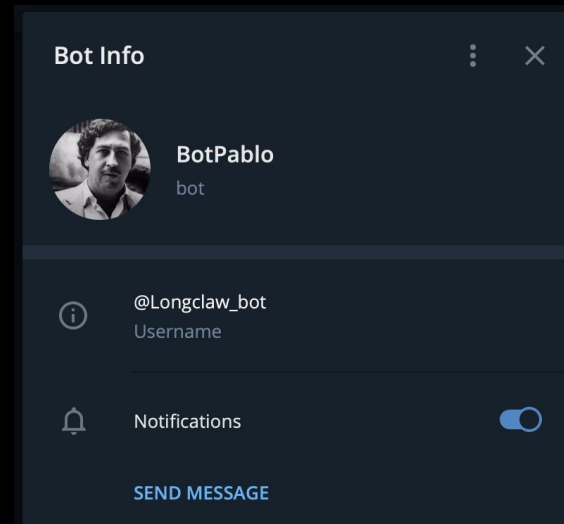
http://t.me/HowToFind_bot

<https://github.com/HowToFind-bot/osint-tools>

Using tokens to go deeper



```
$ python3 dumper.py --token 315271734:AAHy8Z2AoCFp_V-MZKIVe0d0cbs1JScZ6sY
ID: 315271734
Name: BotPablo
Username: @Longclaw_bot - https://t.me/Longclaw_bot
Dumping history from 200 to 0...
[1][295638585][2017-03-07 12:12:50+00:00] /start
=====
NEW USER DETECTED: 295638585
First name: Siddharth
Last name: Kumar
Username: @Cham3l3on - https://t.me/Cham3l3on
Saving photo 1269758054466955179...
Saving photo 1269758054466955177...
[2][295638585][2017-03-07 12:13:13+00:00] /help
[3][295638585][2017-03-07 13:09:43+00:00] hello
[4][295638585][2017-03-07 13:11:44+00:00] sup?
[5][295638585][2017-03-07 13:14:31+00:00] nm
[6][295638585][2017-03-07 13:16:00+00:00] lol
[7][315271734][2017-03-07 13:18:10+00:00] Hey!
[8][295638585][2017-03-07 13:36:04+00:00] Hey
[9][295638585][2017-03-07 13:36:28+00:00] sup
[10][295638585][2017-03-07 13:36:46+00:00] ..
[11][295638585][2017-03-07 13:38:04+00:00] hey
[12][295638585][2017-03-07 13:42:52+00:00] oii
[13][315271734][2017-03-07 13:44:32+00:00] How are you?
[14][285437854][2017-03-07 13:52:03+00:00] /start
```



<https://github.com/soxoj/telegram-bot-dumper>





The End



<https://t.me/soxoj>

https://t.me/osint_mindset

THANKS. ANY QUESTIONS?