



Shadow OSINT: information leaks usage

v 0.0.2

SPEAKER: @soxoj

About me

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



<https://github.com/soxoj>

- Why are we talking about leaks
- Common partial data disclosure examples
- Full data disclosure examples
- What's wrong with IT companies ecosystems
- What to do with it

Let's talk about information leaks

- Also known as information disclosure
- “Exposure of Sensitive Information to an Unauthorized Actor” ([CWE-200](#))
- The CWE Top 25 (7th place)
- One of the most common vulnerabilities in the wild...
- ...and most often out of scope in bug bounty programs

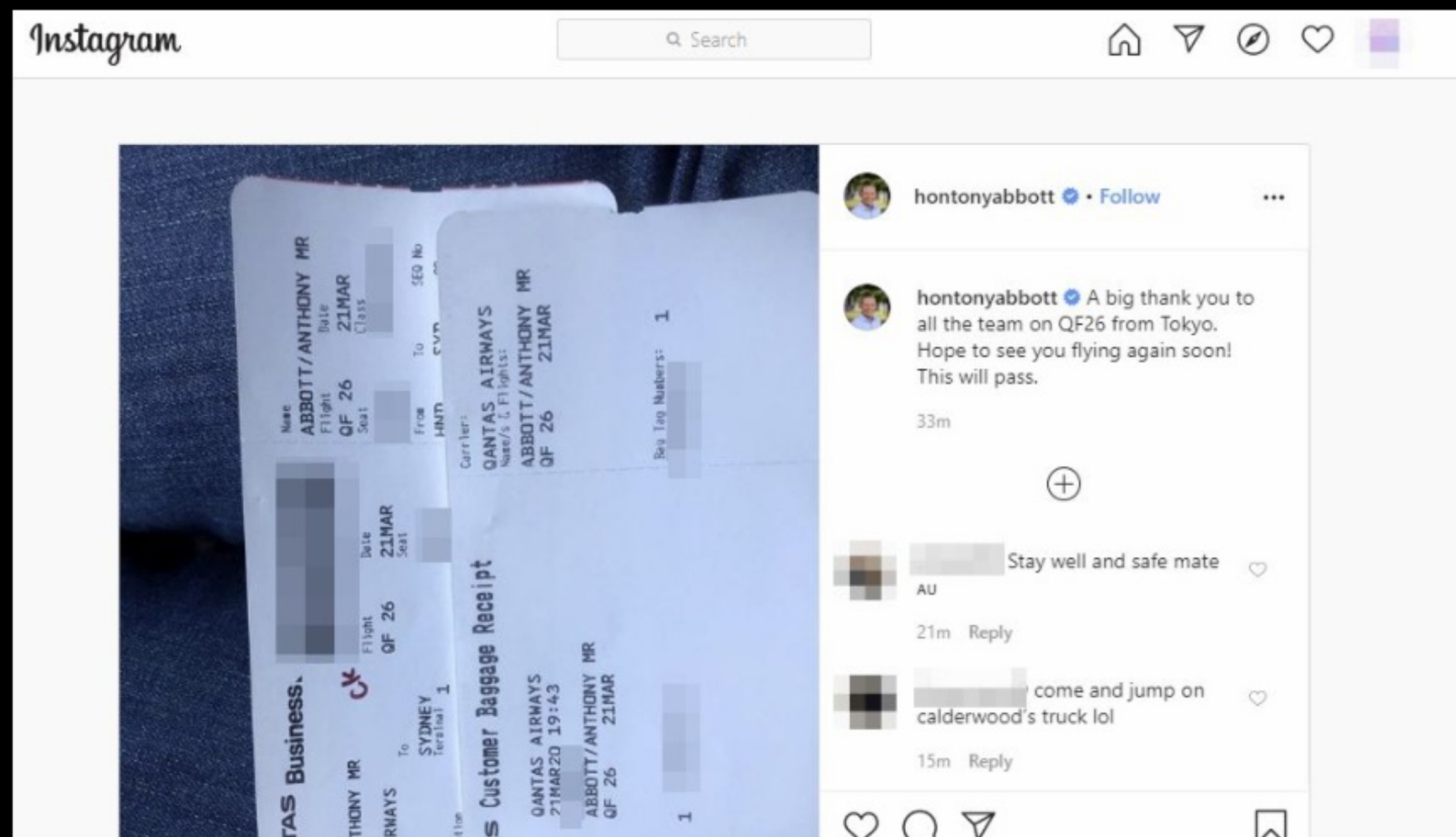
 RuCTFE 2020 / ructfe.org
Shadow OSINT
information leaks usage

Admin name and other details

Page Name

Let's talk about information leaks (cont'd)

...or you can find former Prime Minister's passport number



```
"apisSectionBean":{"passport":  
  "GLOBAL_DEFAULT_1","gender":"M","dateOfBirth":"04/11/57","issuingCountry":"AU","documentNumber":"[REDACTED]","expiryDate":  
  "2020-03-21","isRedressNumberRequestable":false,"isKnownNumberRequestable":false},"nationalityAttributes":  
  {"value":"","mandatory":"N"},"fullName":"Anthony Abbott","businessPhones":[],"businessPhonesCount":0,"homePhonesCount":0,"mobil
```

<https://mango.pdf.zone/finding-former-australian-prime-minister-tony-abbotts-passport-number-on-instagram>

The role of leaks in OSINT

Recruiter of a well-known company:
“We are developing OSINT in Russia,
talking about vulnerabilities and letting
them be used”

Personal data leaks = illegal gold mine.

Мы - те, кто качает osint в России,
те, кто рассказывает людям про
уязвимости и даёт возможность
ими пользоваться.

13:46

 [.com](#)

13:46

ознакомься

13:46

Where personal data leak

- Registration & authorization
- Password recovery
- Account page
- Permissions granting, invites
- And any users interactions

VirusTotal simple example

Check for Virustotal user information by username

The image shows a VirusTotal community registration page on the left and a network inspector on the right. The registration page has fields for First name, Last name, Email, and Username. The Username field contains 'an' and a red error message below it says 'This username is unavailable'. A red box labeled 'Enter username' has arrows pointing to the Username field and the network inspector. The network inspector shows a response from 'an' with the following JSON data:

```
{
  "data": {
    "attributes": {
      "first_name": "Peter",
      "last_name": "Dink",
      "profile_phrase": "Security expert. Kaspersky",
      "reputation": 281651,
      "status": "active",
      "user_since": 1290149006
    },
    "id": "an",
    "links": {
      "self": "https://www.virustotal.com/ui/users/"
    },
    "type": "user"
  }
}
```

Not really a leak, all information is public. But why?

https://twitter.com/GONZOs_int/status/1334811159724253184

Common partial data disclosure

Reset Your Password

How do you want to get the code to reset your password?

- ☒  Send code via email
qw3511@[REDACTED]
|*****i@e[REDACTED].net
- ☐  Send code via SMS
+*****67
- ☐  Send code via SMS
+*****23

Verify your identity

Choose which method to verify your identity



Email code to

[REDACTED]@gmail.com

[REDACTED]@g.....l.com



Confirm your phone number
ending in -54

Enter the last 4 digits of your phone number



Password recovery almost always prompts pieces of personal data.

Common partial data disclosure (cont'd)

Восстановление пароля

Укажите данные, которые вы использовали при заключении договора

Я помню номер договора

Я помню телефон

Я помню e-mail

Восстановление пароля

Выберите номер договора:

☒ *****2610
Пенза, В***** ***, 45, п.3

Далее

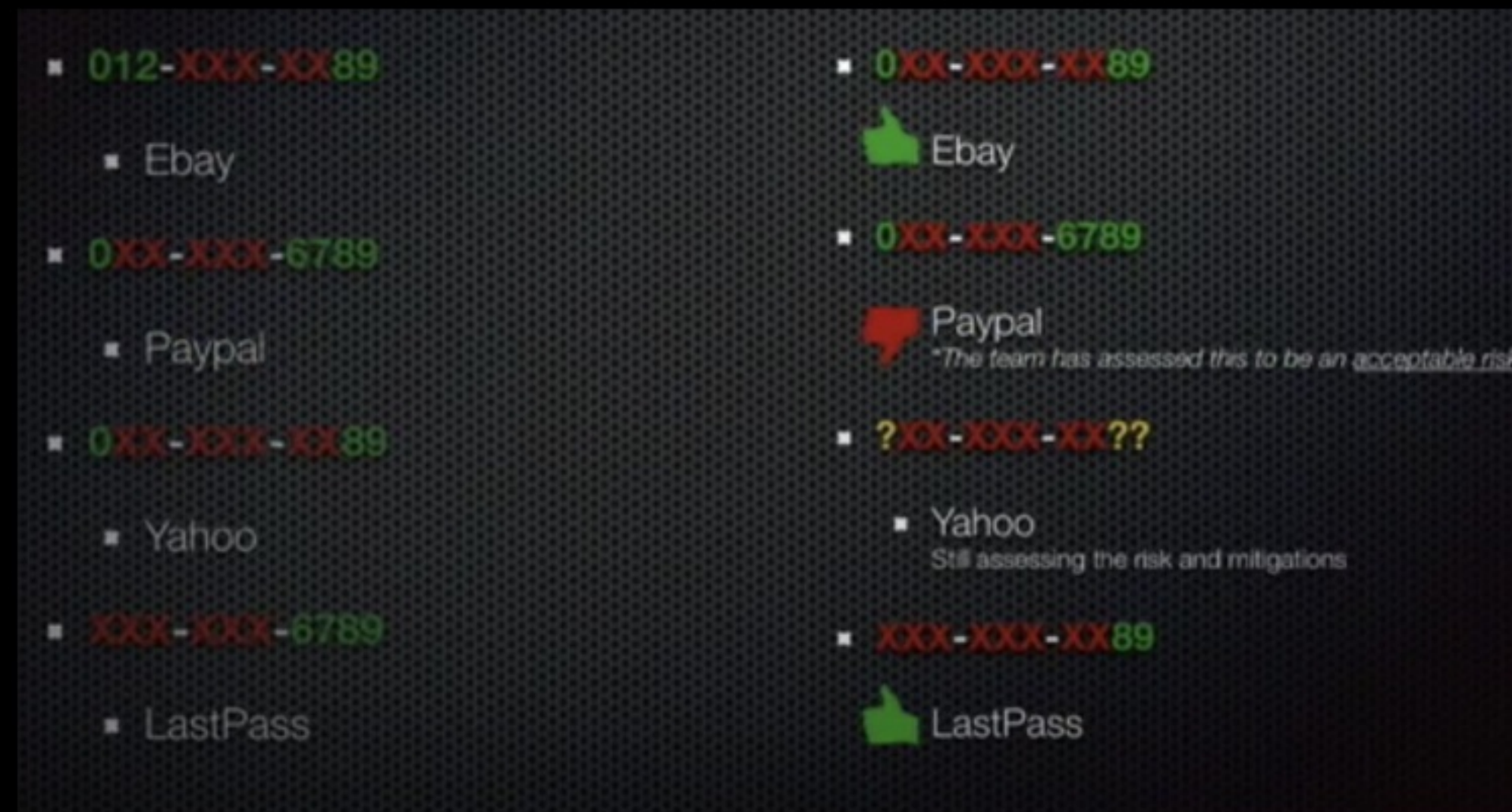
[Назад](#)

```
▼ {agreement: 580010, agreementId: 3899766, ...}
  address: ""
  agreement: 580010
  agreementId: 3899766
  code: ""
  ▼ contacts: [{contactId: 291195, contactType: 1, row: "mas*****@ma**.**", address: ""}, ...]
    ▼ 0: {contactId: 291195, contactType: 1, row: "mas*****@ma**.**", address: ""}
      address: ""
      contactId: 291195
      contactType: 1
      row: "mas*****@ma**.**"
    ► 1: {contactId: 5500462, contactType: 2, row: "8902****730", address: ""}
    ► 2: {contactId: 0, contactType: 3, row: "Пенза, В***** ***, 45, п.3", address: ""}
  message: ""
```

Common partial data disclosure (cont'd)

You can:

- Get pieces of personal data by primary service identifier
- Restore full information and verify it using other sources
- Collect all the pieces through the mass exploitation



<https://www.youtube.com/watch?v=1zssBR85vDA>

Common partial data disclosure (cont'd)

Examples of tools:

- <https://github.com/martinvigo/email2phonenumber>
- <https://github.com/megadose/holehe>

Multi-factor authentication can be a privacy issue.

Google alternate email address leak

```
{  
  "principal": [  
    {  
      "id": "users/1098022227107301",  
      "user": {  
        "gaiaId": "1098022227107301",  
        "email": "1098@gmail.com",  
        "lookupKeyEmail": "1098@mail.ru"  
      }  
    }  
  ]  
}
```

Status: Won't Fix (Intended Behavior)

One of the email addresses entered is the alternate email address of a Google Account. The alternate email address has been changed to that account's primary email address.

CLOSE

<https://twitter.com/subfnSecurity/status/1255741950914727942>

Google alternate email address leak (cont'd)

You can:

- Get real account of anonymous person
- Confirm that two email addresses are owned by the same person
- Get account ID aka GAIA ID and find out info from other Google services



email-a@example.com



email-b@gmail.com

Google alternate email address leak (cont'd)

Examples of tools:

- <https://tools.epieos.com/google-account.php>
- https://t.me/getgmail_bot

Google primary email address leak

Open Google profile Dashboard =>

https://www.google.com/settings/dashboard?uq=<GAIA_ID>

=> Login =>

https://accounts.google.com/AddSession?continue=https://www.google.com/settings/dashboard#Email=<EMAIL_ADDRESS>

In fact, it was possible to get email for account ID.

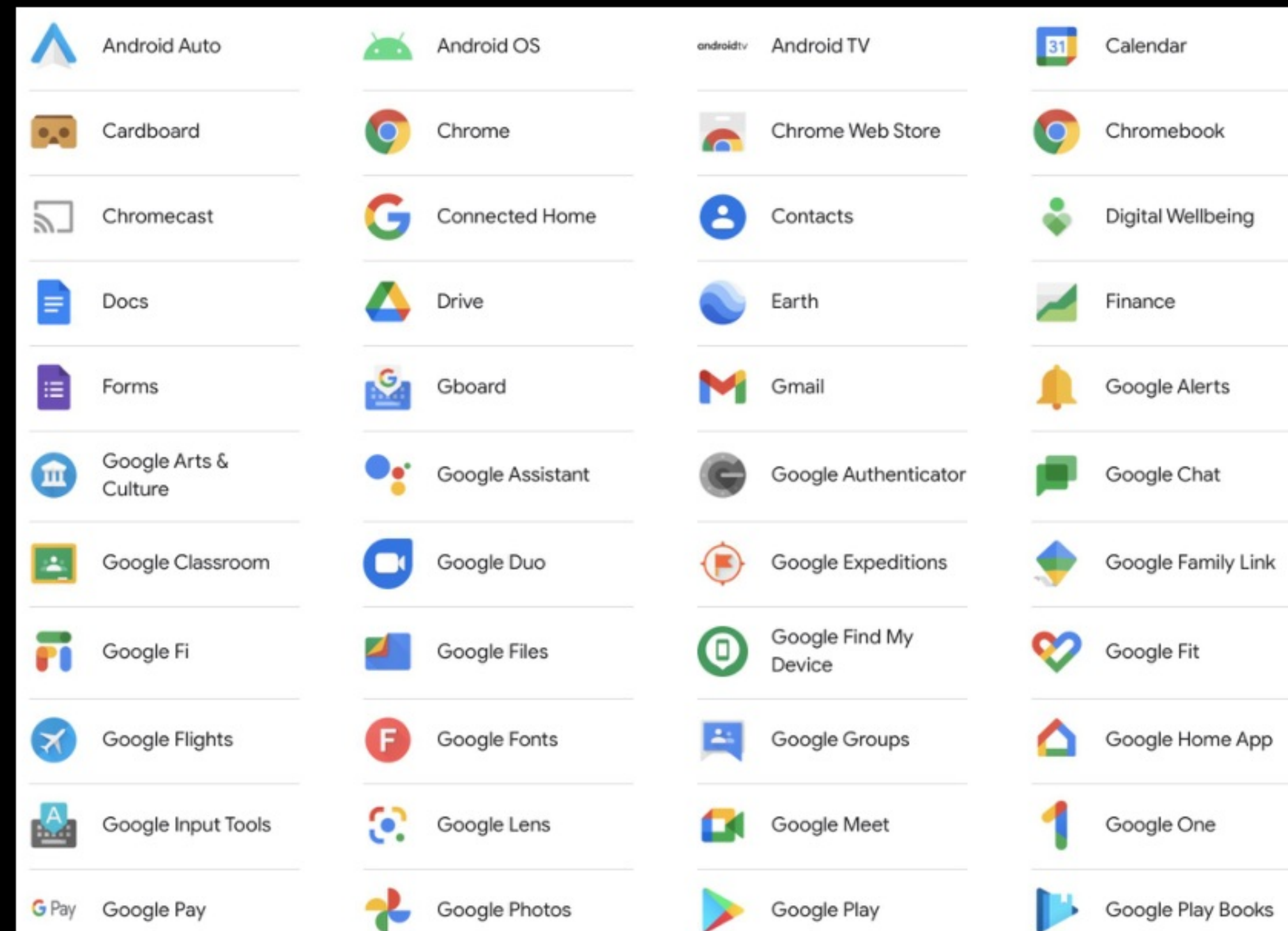
What about GAIA ID using?

Fixed: \$1337 reward

<https://www.tomanthony.co.uk/blog/google-exploit-steal-login-email-addresses/>

The Google ecosystem

*One Account to rule them all,
One Account to find them,
One Account to bring them all
and in the darkness bind them*



Google Account information retrieval using GAIA ID

You can get:

- Owner's name
- Last time the profile was edited
- Activated Google services list
- Possible YouTube channel
- Possible other usernames
- Public photos
- Phones models and firmwares, installed softwares
- Google Maps reviews, possible physical location
- Events from Google Calendar
- ...

Google Account information retrieval using GAIA ID (cont'd)

Examples of tools:

- <https://github.com/mxrch/GHunt>

```
C:\Users\mxrch\Desktop\labs\google\id>python hunt.py [REDACTED]@live.fr

Name: [REDACTED]
Location: Sélestat-Erstein, France

Last profile edit : 2019/04/22 23:49:54 (UTC)

Email : [REDACTED]@live.fr
Google ID : 10668544[REDACTED]

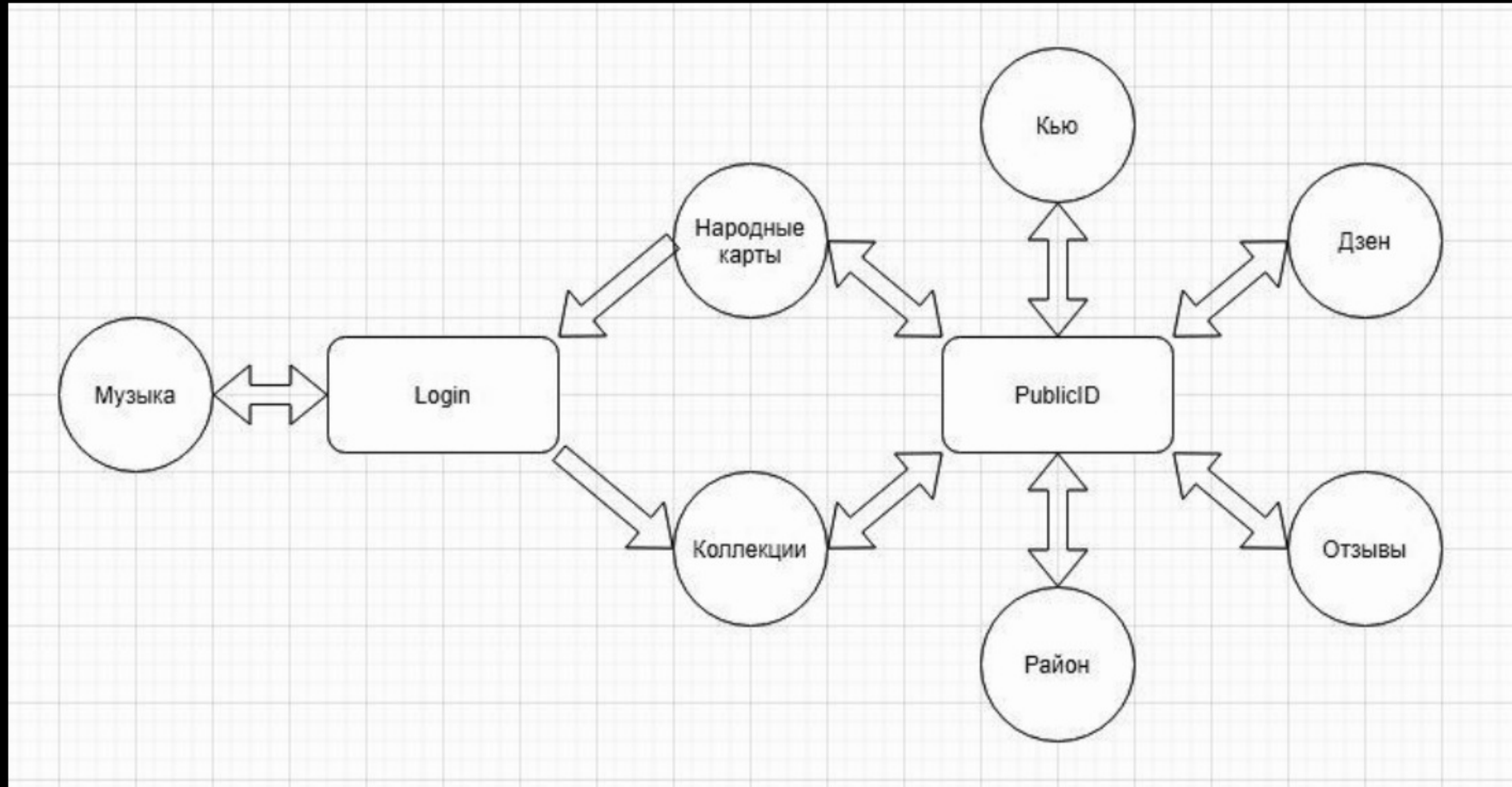
Hangouts Bot : No

Activated Google services :
- Youtube
- Photos
- Maps

Youtube channel (confidence => 90.0%) :
- [REDACTED] https://youtube.com/channel/[REDACTED]

Google Photos : https://get.google.com/albumarchive/10668544[REDACTED]
=> 2 albums, 2 photos
```

The Yandex ecosystem



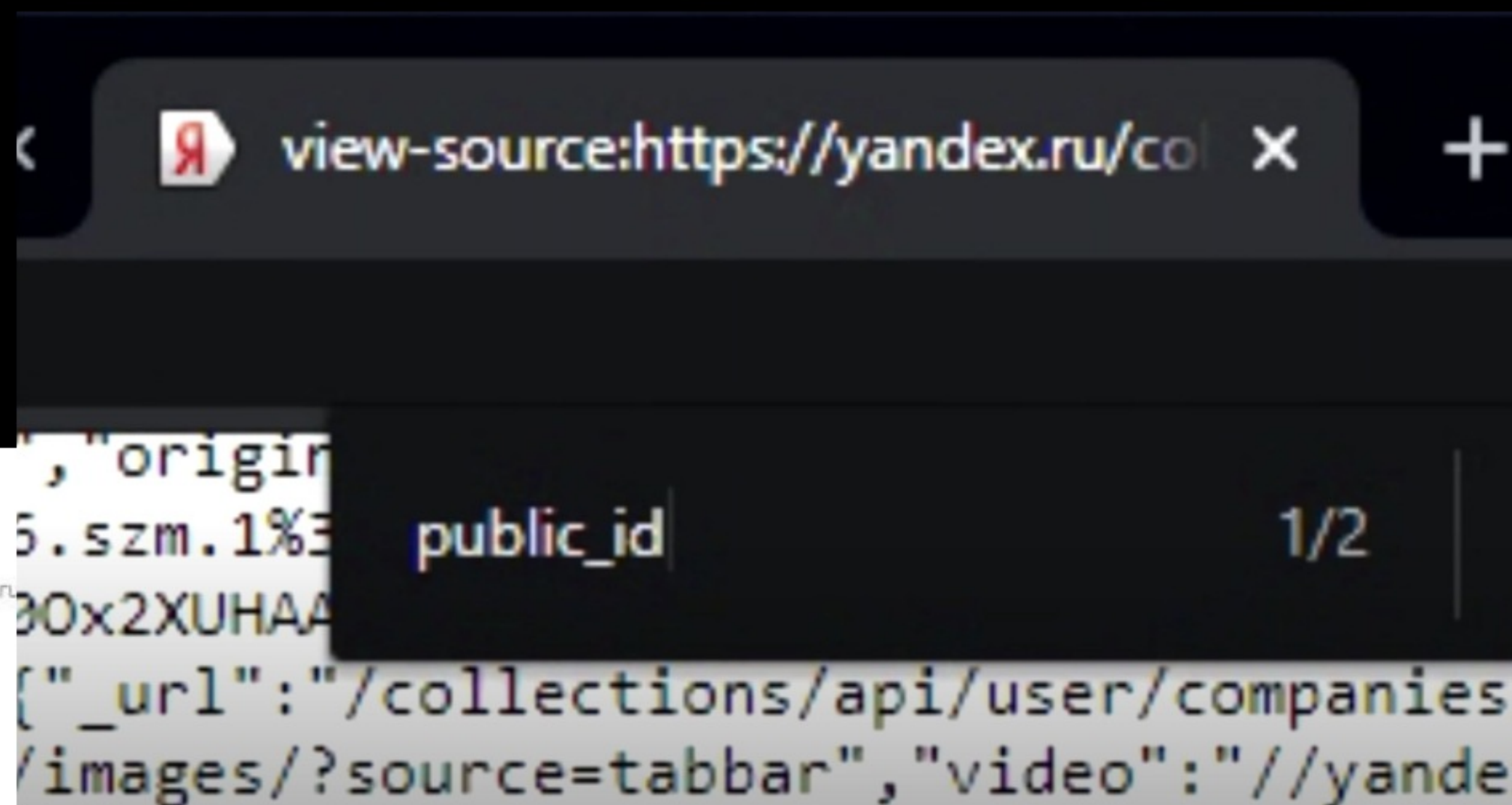
https://t.me/HowToFind_RU/127

The Yandex ecosystem (cont'd)

Re: Information disclosure Яндекс.Дзен

 security-report@yandex-team.ru  security-report@yandex-team.ru
1 получатель

Добрый день,
Прошу прощения за долгий ответ.
Поздравляем, за уязвимость, о которой вы сообщили, вам присужден приз — 7500 рублей. Обратите внимание, что это сумма до вычета налога.



Yandex.Zen author ID disclosure - \$100 reward

<https://www.youtube.com/watch?v=0calRx1jgRY>

Куплено
благодаря
Skladchik.com

Phone vendor's #1 ecosystem

Что Вы хотите изменить?

☐ Номер телефона: 155*****89

☐ Адрес эл. почты: ya***@****ail.com

☐ Безопасный номер телефона: 155*****89

☐ Безопасный адрес эл. почты: le***@**.com

[Назад](#) [Далее](#)

Phone number, primary & secondary emails, devices you used, Wi-Fi hotspots SSIDs

* Модель устройства

Выберите

Номер IMEI

Выберите

- HUAWEI nova 2S
- MEDIAPAD 10 LINK+
- MEDIAPAD 7 YOUTH
- 华为畅享7 Plus
- 荣耀V9 play
- 荣耀畅玩4X
- 荣耀畅玩7X

* Часто используемая точка доступа Wi-Fi

Выберите точку доступа Wi-Fi, которую используете часто.

Выберите

- 04**39
- 1-4**104
- 107***0398
- 117**5-4
- FAST***8DC8
- 020gy*****com_5G

Phone vendor's #2 ecosystem

Reset recovery phone

[redacted] 12****

Recovery phone: 199*****20

Recovery email: 25*****2@q*.com

We received your application. We'll send you a reply to your new recovery phone within 3-5 working days.

Provide as much info as possible. The more information we have, the easier it will be to recover your identity.

Main site password recovery

+

Other product API leak

=

Full personal info disclosure

```
"data": {
  "profiles": {
    "123814": {
      "userId": 123814,
      "userName": "[redacted]@gmail.com",
      "icon": "",
      "userAddresses": null,
      "nickname": "李子",
      "create_time": 1295285173000,
      "infoupdate_time": 1295285173000,
      "userExtra": {
        "userId": "",
        "sex": "",
        "birthday": "",
        "modify_time": ""
      },
      "userSettings": null,
      "avatarUrl": [
```

Proposals to developers

Don't leak sensitive info, please.

But if you are leaking:

- Do monitoring and alerting
- Use rate limiting and captcha
- Prevent mass exploitation

Proposals to researches

Report a leak as a vulnerability.

But if it is only “Informative”:

- Put it in your arsenal
- Create tool to automate its use

Useful links

1. <https://www.bugcrowd.com/resources/webinars/hidden-in-plain-site-disclosing-information-via-your-apis/>
2. <https://www.youtube.com/watch?v=0BsOEMA9d5s>
3. <https://www.martinvigo.com/email2phonenumber/>
4. https://t.me/osint_mindset/8
5. <https://github.com/soxoj/socid-extractor>



The End

<https://t.me/soxoj>

<https://dc7495.org>

https://t.me/osint_mindset

<https://t.me/HowToFind>

THANKS. ANY QUESTIONS?