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

Overview

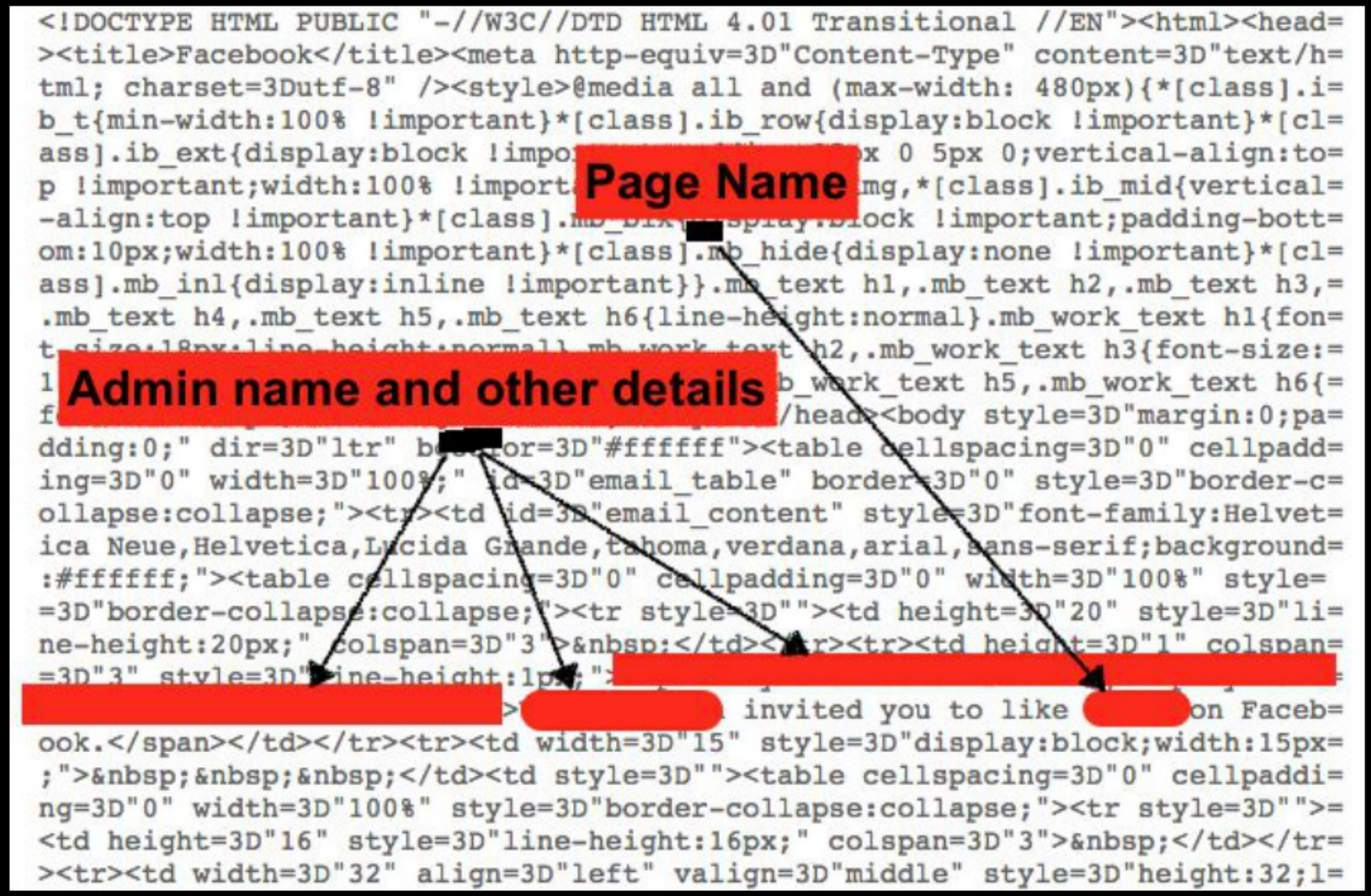
- Why are we talking about leaks
- Common partial data disclosure examples
- Full data disclosure examples
- What’s wrong with IT companies ecosystems
- What to do with it

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

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

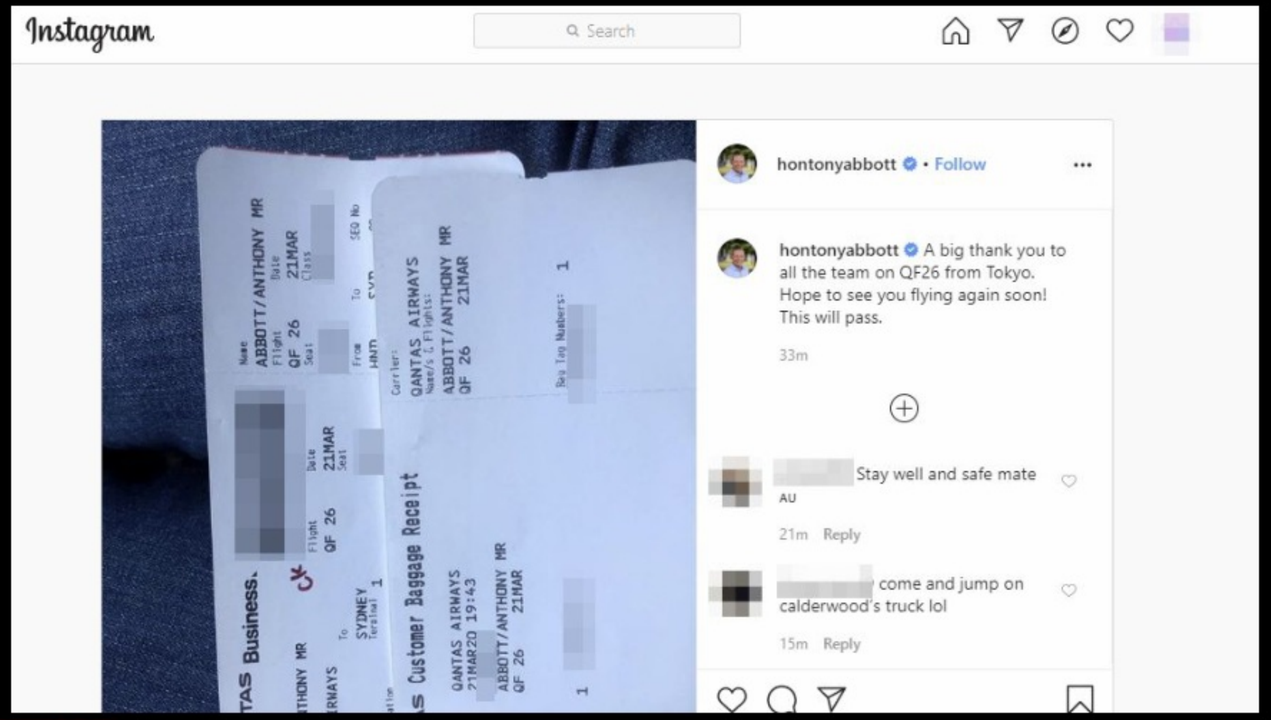
But you can get $2.5K for 2.5 minutes search for personal data in source code



https://seekurity.com/blog/2018/02/25/admin/general/the-2-5mins-or-2-5k-hawk-eye-bug-a-facebook-pages-admins-disclosure-vulnerability

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

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



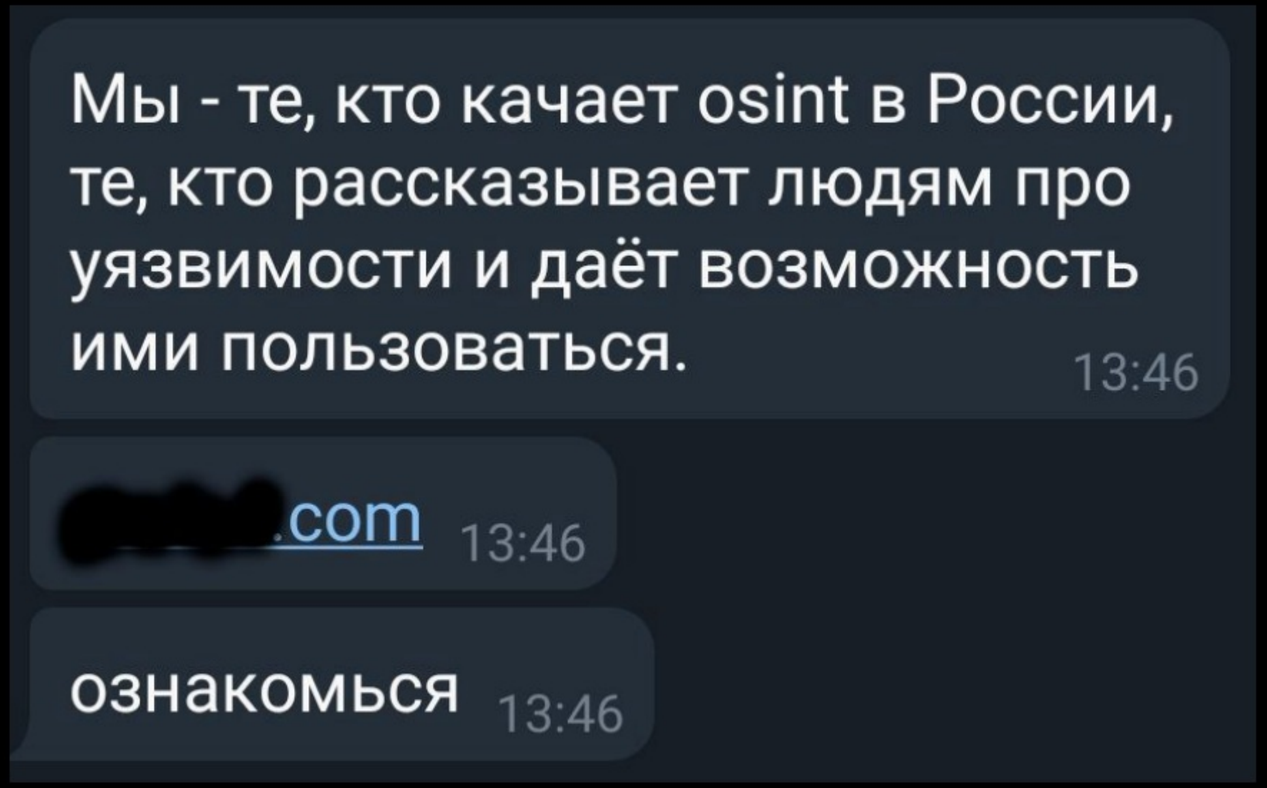
"apisSectionBean":{"passport":
OBAL_DEFAULT_1","gender":"M","dateOfBirth":"04/11/57","issuingCountry":"AU","documentNumber":"[redacted]","expiryDate":[redacted]
se,"isRedressNumberRequestable":false,"isKnownNumberRequestable":false},"nationalityAttributes":
lue":"","mandatory":"N"},"fullName":"Anthony 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”

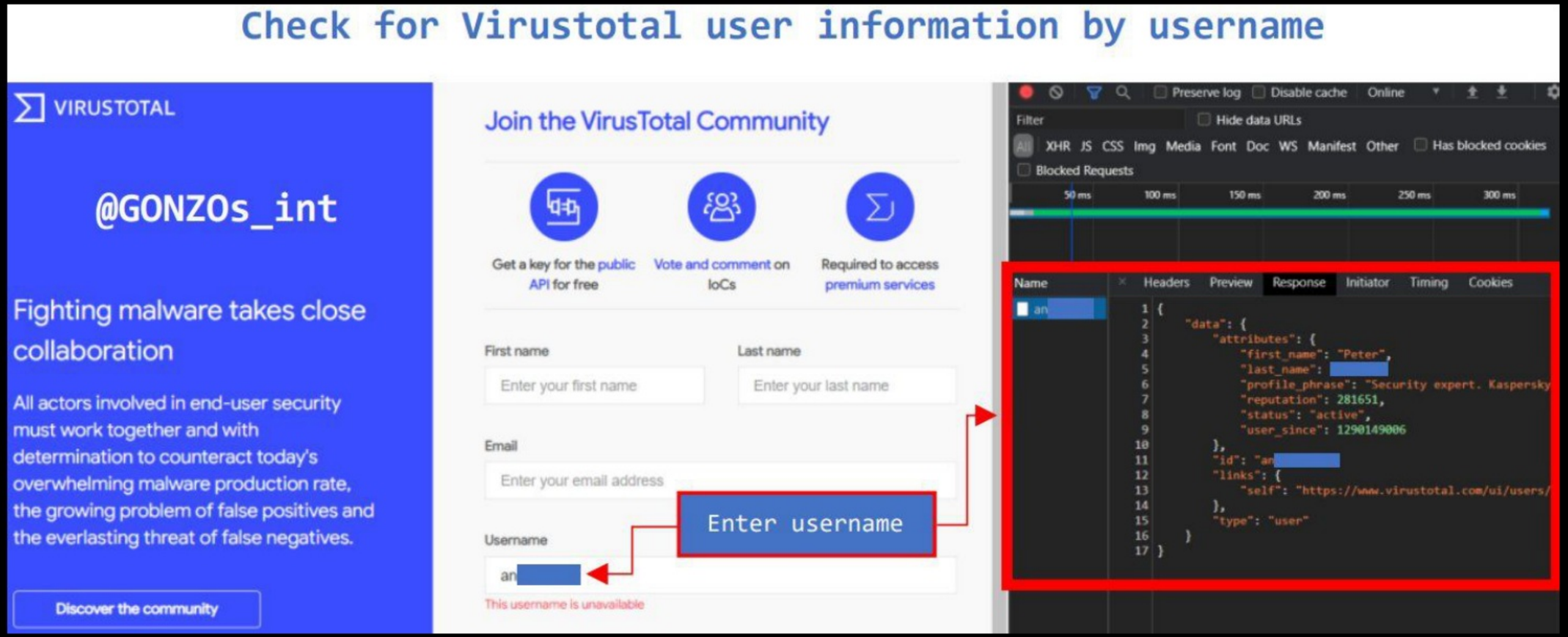
Personal data leaks = illegal gold mine.



Where personal data leak

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

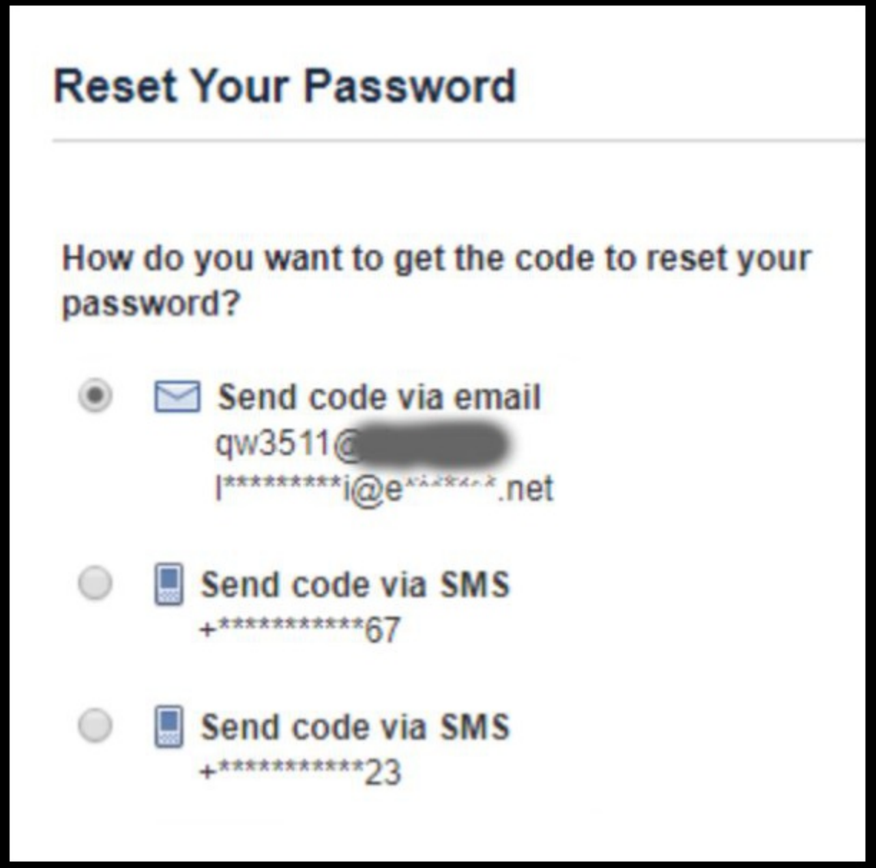
VirusTotal simple example

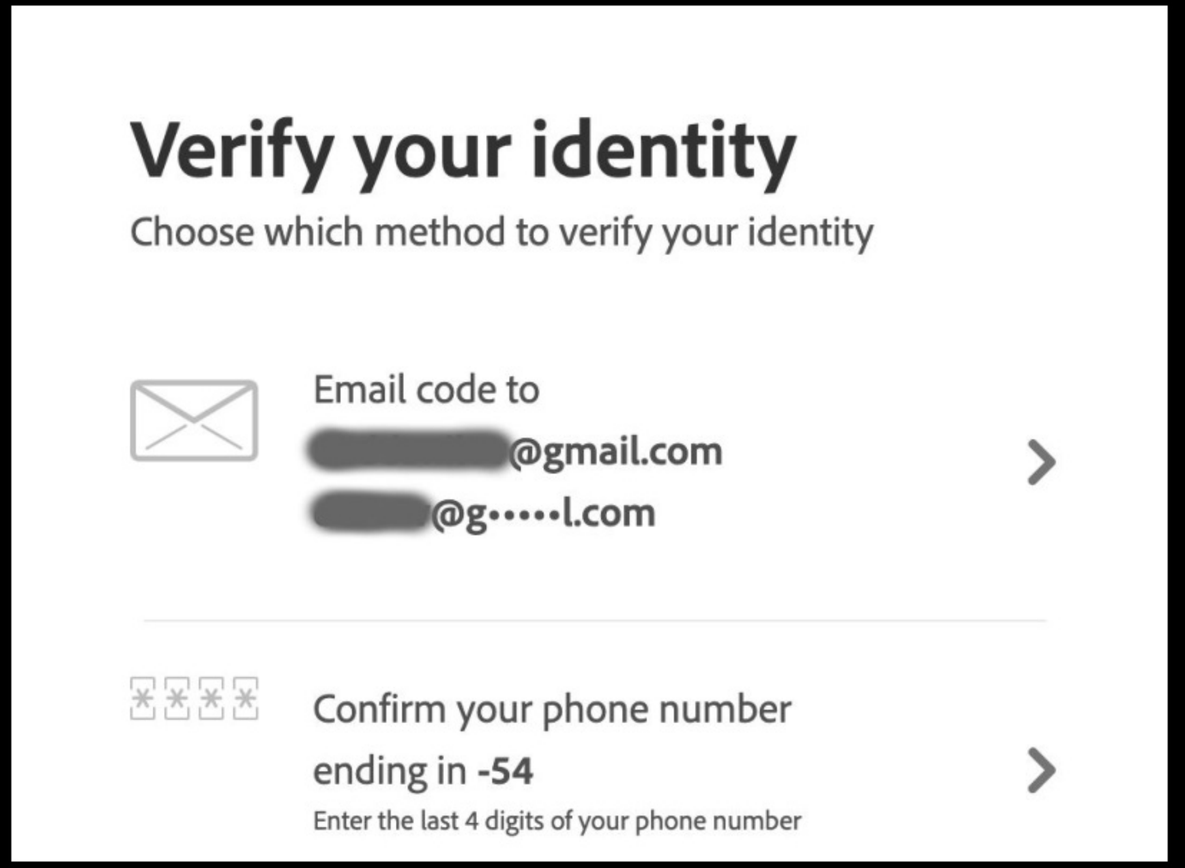


Not really a leak, all information is public. But why?

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

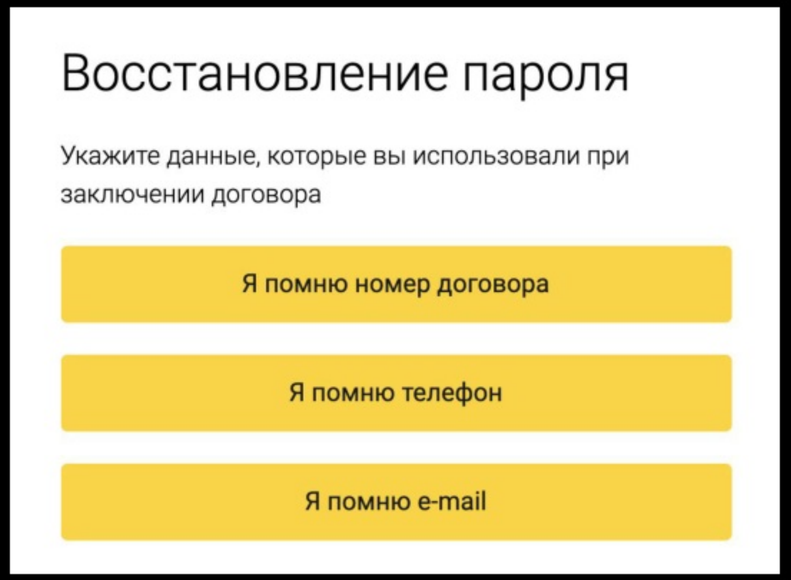
Common partial data disclosure

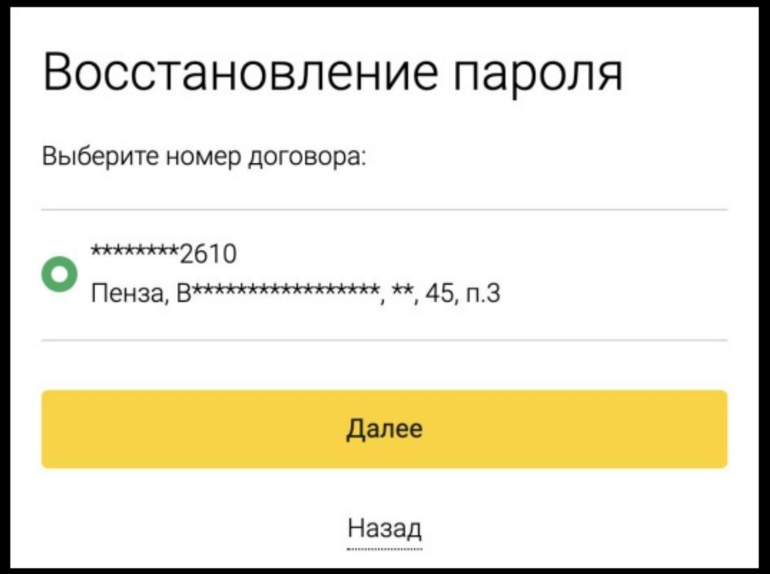




Password recovery almost always prompts pieces of personal data.

Common partial data disclosure (cont'd)

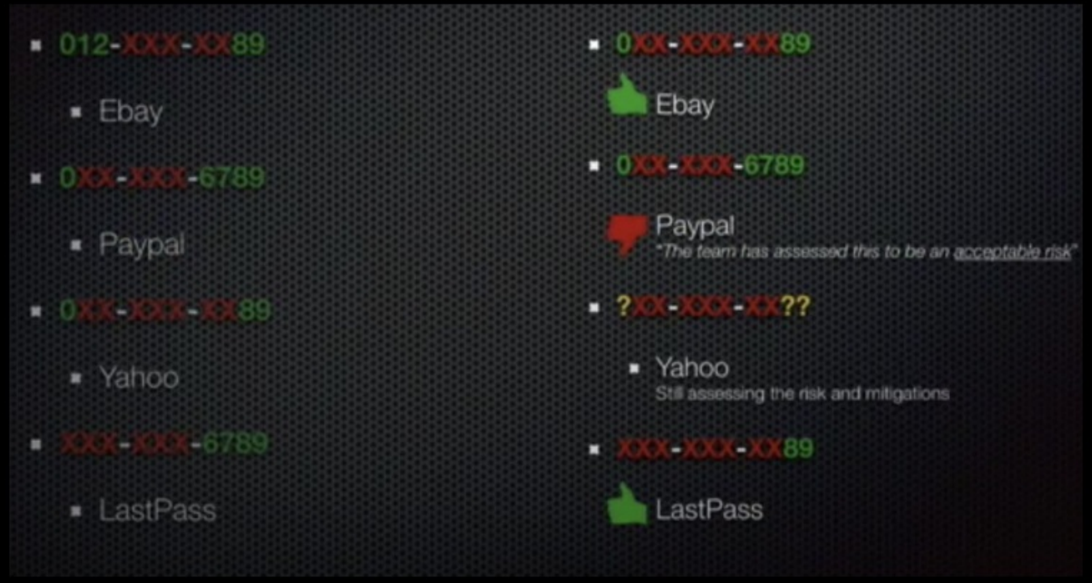




Common partial data disclosure (cont'd)

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/109802222710730[redacted]",
      "user": {
        "gaiaId": "109802222710730[redacted]",
        "email": "[redacted]98@gmail.com",
        "lookupKeyEmail": "[redacted]13@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.

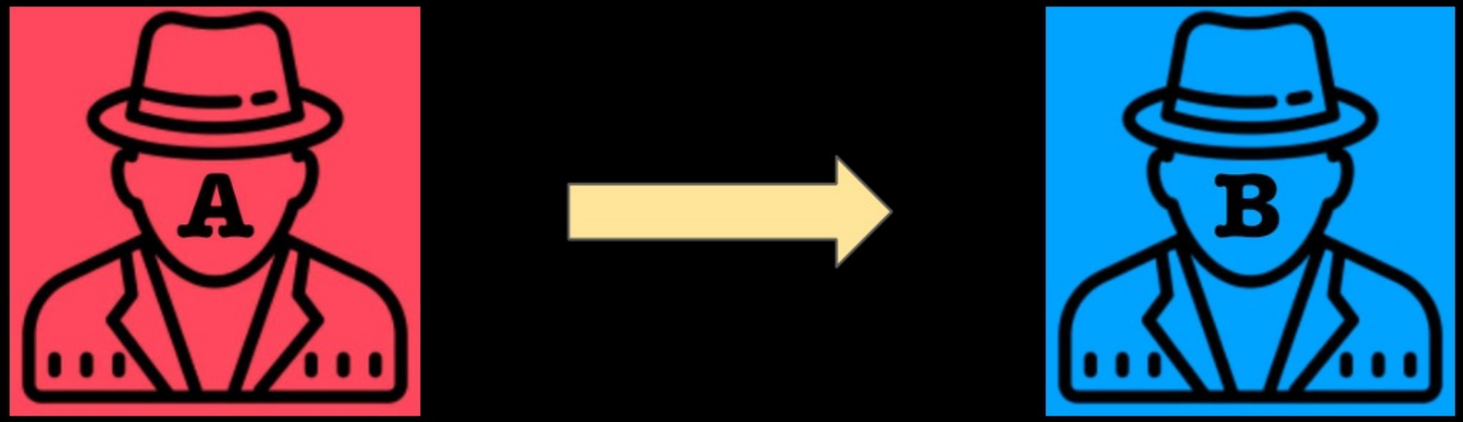
CLOSE

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

- Android Auto
- Android OS
- Android TV
- Calendar
- Cardboard
- Chrome
- Chrome Web Store
- Chromebook
- Chromecast
- Connected Home
- Contacts
- Digital Wellbeing
- Docs
- Drive
- Earth
- Finance
- Forms
- Gboard
- Gmail
- Google Alerts
- Google Arts & Culture
- Google Assistant
- Google Authenticator
- Google Chat
- Google Classroom
- Google Duo
- Google Expeditions
- Google Family Link
- Google Fi
- Google Files
- Google Find My Device
- Google Fit
- Google Flights
- Google Fonts
- Google Groups
- Google Home App
- Google Input Tools
- Google Lens
- Google Meet
- Google One
- Google Pay
- Google Photos
- Google Play
- Google Play Books

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
- ...

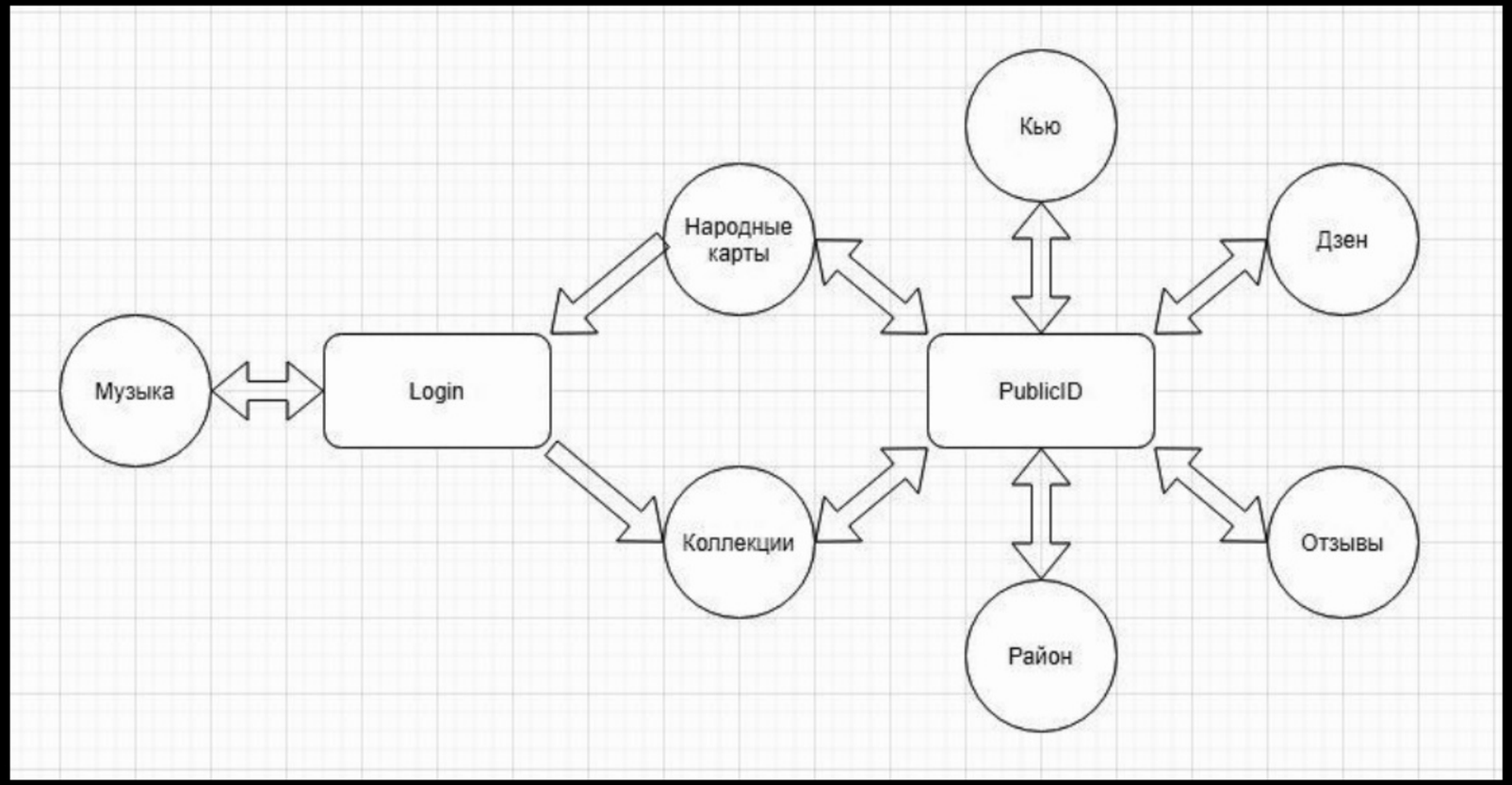
Google Account information retrieval using GAIA ID (cont'd)

Examples of tools:

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

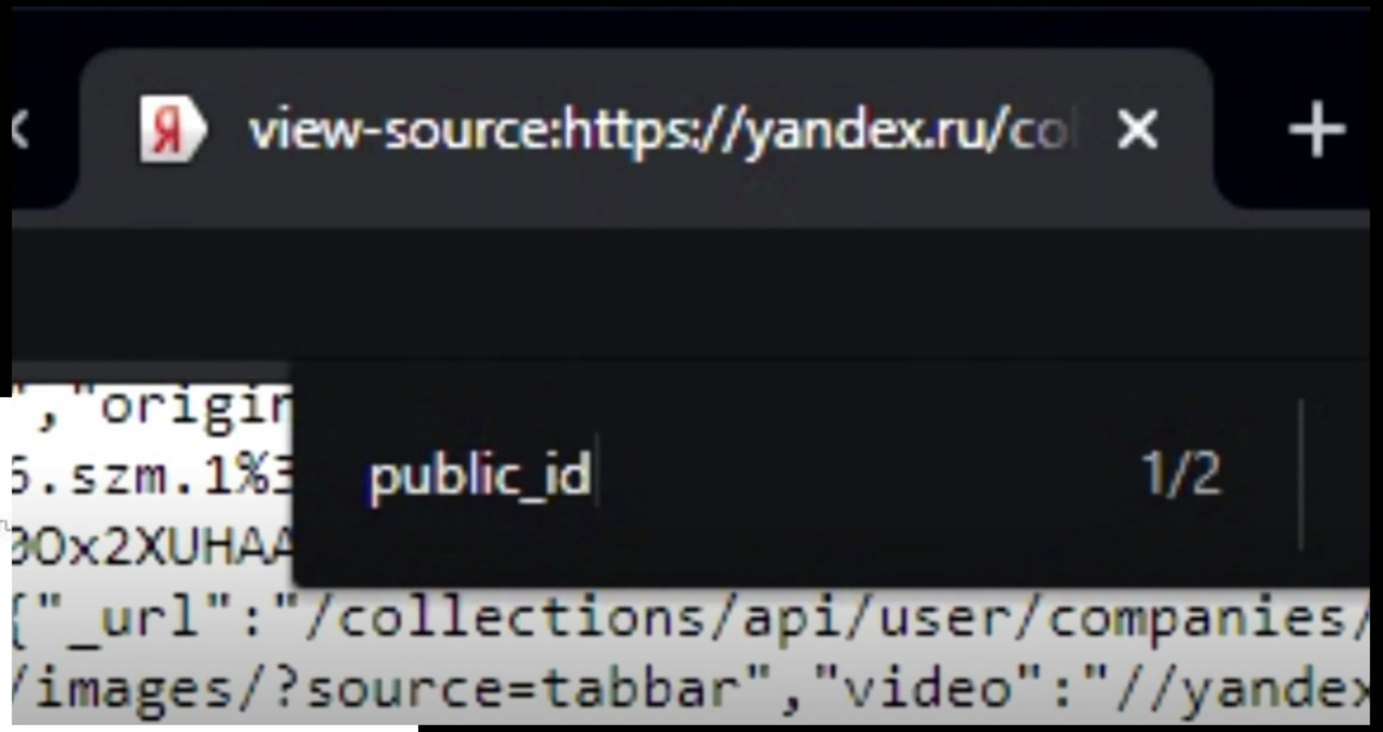
```
C:\Users\mxrch\Desktop\labs\google\id>python hunt.py [redacted]@live.fr

[redacted]

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

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

Email : [redacted]@live.fr
Google ID : 106685440[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/106685[redacted]
=> 2 albums, 2 photos
```

The Yandex ecosystem



https://t.me/HowToFind_RU/127

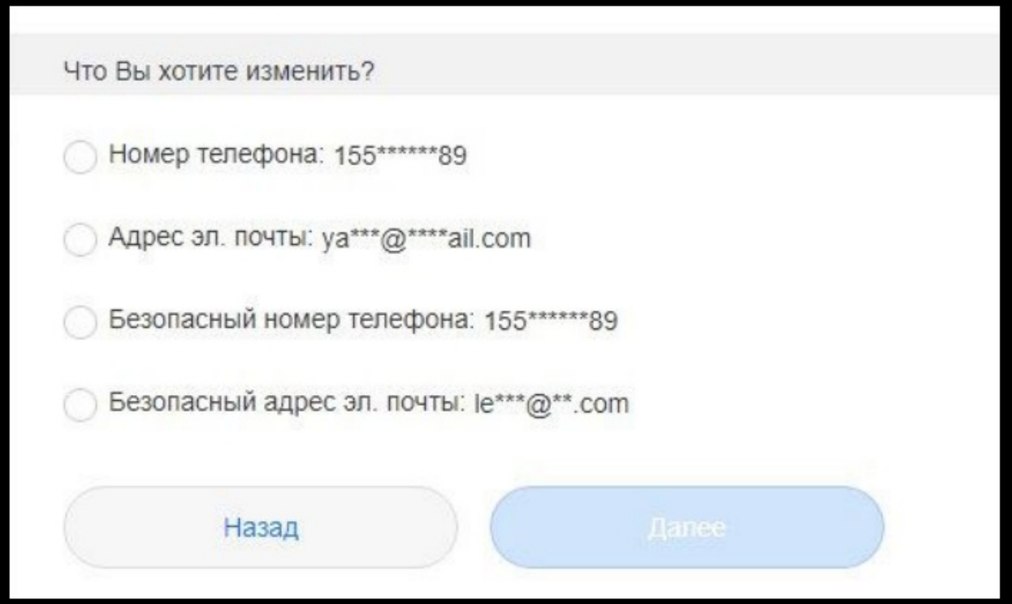
The Yandex ecosystem (cont'd)



Yandex.Zen author ID disclosure - $100 reward

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

Phone vendor's #1 ecosystem



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

Phone vendor's #2 ecosystem

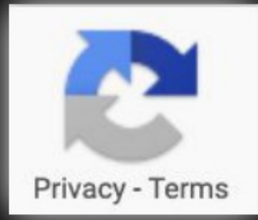
Main site password recovery
+
Other product API leak
=
Full personal info disclosure

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?