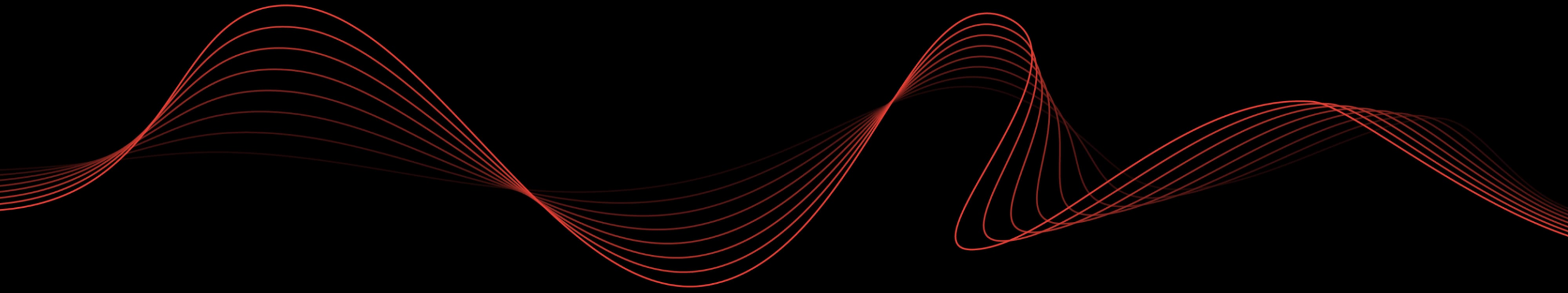
KAZHACKSTAN TURAN – 2023

«Offensive OSINT»

Aleksandr Goncharov



WHOAMI?

- **OSINT specialist at Innostage**
- **PHDays, OffZone, Codeby, OSINT Mindset speaker**
- **sOSINT specialist**

Notes

About

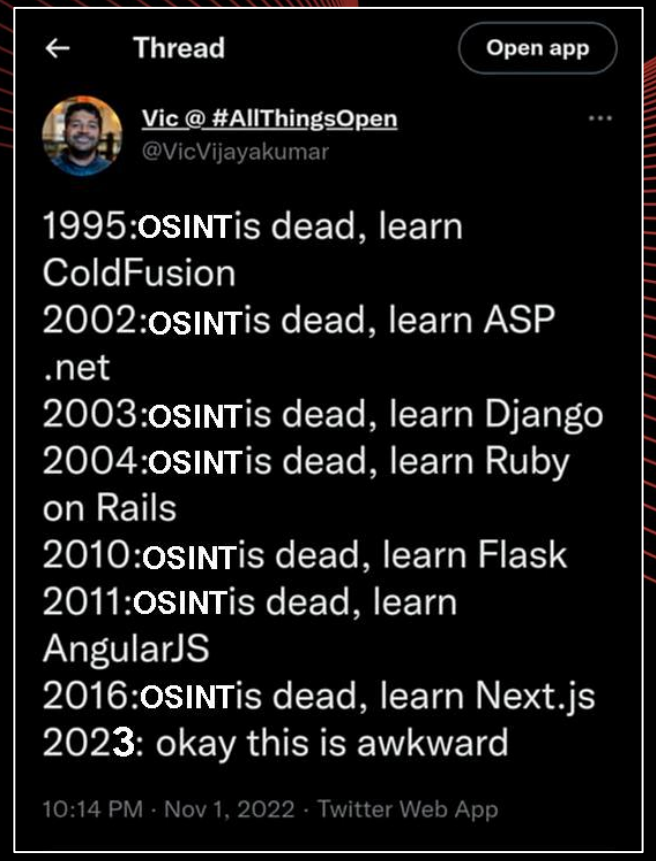
OffSec OSINT Pentest/RedTeam Tools

osint hacking infosec awesome-list pentesting pentest pentest-scripts information-gathering reconnaissance redteaming redteam pentesting-tools osint-tool redteam-tools

Readme
Activity
313 stars
8 watching
44 forks

Table of Contents

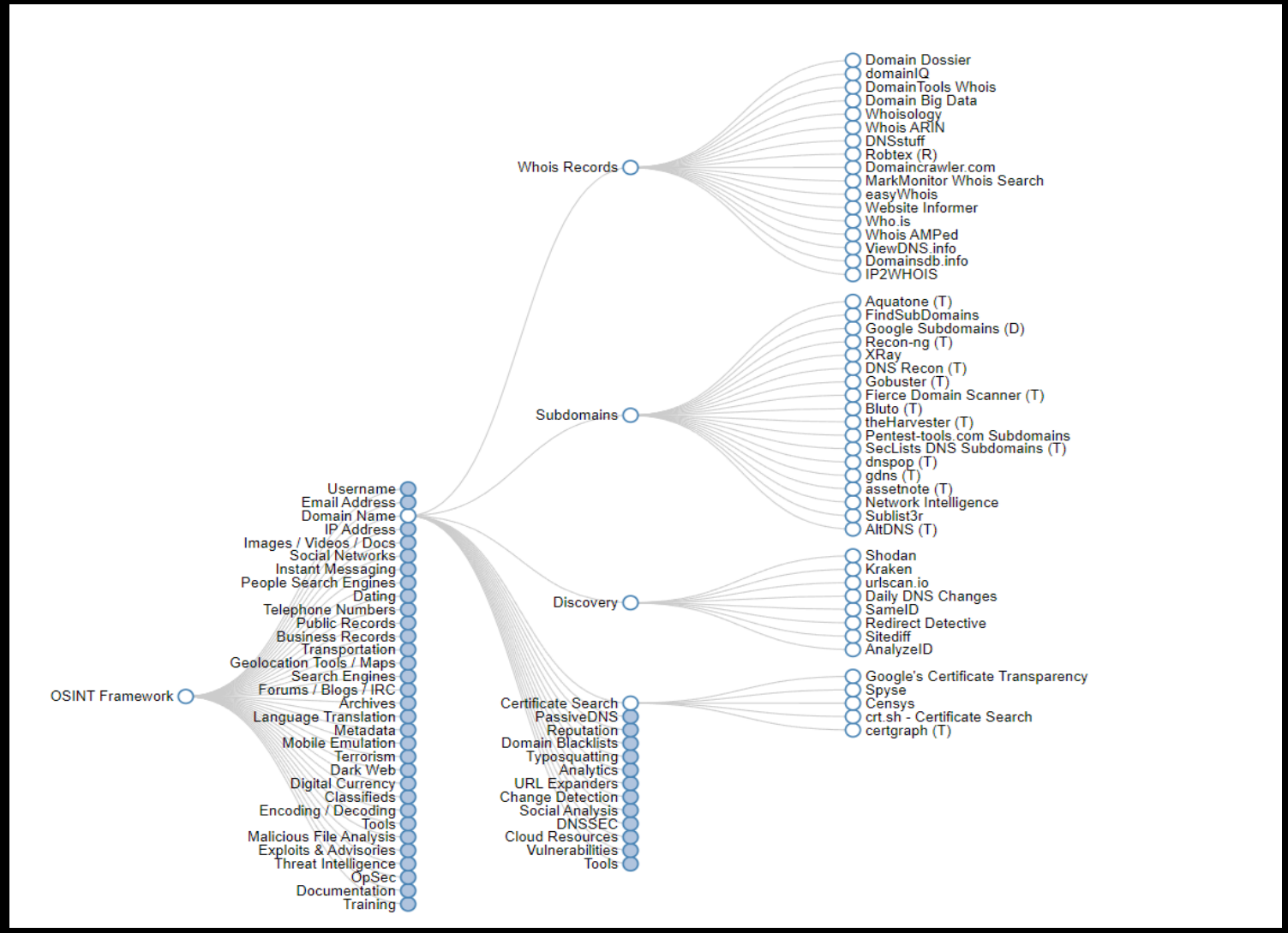
OSINT is dead?



Yet Another OSINT report?

- **Let’s take a look what other sources offers**

OSINT Framework / awesome-osint



Top Sheets……


TOP OPEN SOURCE INTELLIGENCE TOOLS USED IN CYBERSECURITY
1 OSINT Framework
2 CheckUserNames
3 HavelbeenPwned
4 SecurityTrails API
5 Censys
6 Wappalyzer
7 Google Dorks
8 Maltego
9 Recon-Ng
10 theHarvester
11 Shodan
12 Jigsaw
13 SpiderFoot
14 Creepy
15 Nmap
16 WebShag
17 OpenVAS
18 Fierce
19 Unicornscan
20 Foca
21 ZoomEye
22 OWASP AMASS
23 IVRE
24 Metagoofil
25 Exiftool
SecurityTrails


15 Top OSINT Tools
@securitytrybe
1. Nmap
2. OSINT Framework
3. CheckUserNames
4. Jigsaw
5. Maltego
6. Censys
7. BeenVerified
8. OpenVAS
9. Sypse
10. IVRE
11. Fierce
12. ZoomEye
13. Recon-ng
14. Shodan
15. TheHavester
SECRET
Securrity Trybe

Red Team understanding of OSINT

- Creating Significant Traffic != OSINT
- Simulation of regular user traffic = OSINT

What we looking for

Network assets

- IP
- Domain
- Subdomains
- Services
- Version

Employee information

- Full name
- Email
- Logins
- Creds/Secrets
- Numbers
- Personal data

Company info

- Addresses
- Internal docs
- Internal Information

Network assets

Wildcard scope

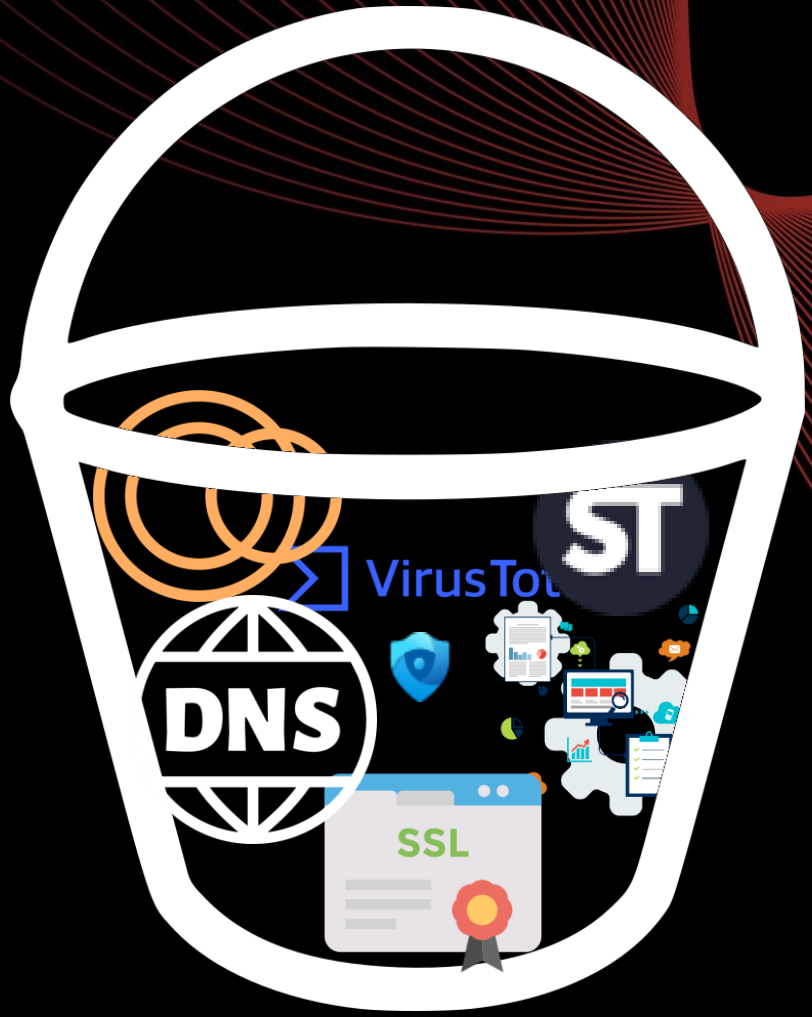
192.68.68.0/24
*.hackdomaim.com

Just a name

Horns & Hooves

Where subdomains are born?

- DNS
- Certificates
- Web Scraping/Dorks
- Public repositories



Most useful subdomain search tools

- Sudomy
- amass
- BBOT
- SpiderFoot/theHarvester

- Running without API = waste of time

Most useful TI systems for searching subdomains

- TI.defender.microsoft.com (ex RiskIQ)
- securitytrails.com
- pulsedive.com
- alienvault.com
- threatbook.io

Difference

```
$ sudomy -d example.com

earthengine.google.com
meet.google.com
classroom.google.com
passwords.google.com
cloud.google.com
jibe.google.com
books.google.com
messages.google.com
adsense.google.com
sites.google.com
images.google.com
```

```
$ ti.defender.microsoft.com -d
example.com

earthengine.google.com
meet.google.com
classroom.google.com
passwords.google.com
cloud.google.com
jibe.google.com
books.google.com
messages.google.com
adsense.google.com
sites.google.com
images.google.com
database.google.com
store.google.com
jira.google.com
```

Think, Mark!

In/De-crementing

- atm40.test.com -> atm41
- s5.atm.test.domain.com -> s6
- 2020s.domain.com -> 2021s
- vpn2.domain.com - > vpn1

Software domains

- Skype | *meet.* dialin.* schedule.**
- Outlook |*owa.* autodiscover.**
- Kaspersky Secure Mail Gateway | *ksmg.**
- etc...

- GitHub Dorks

Permutations

- alterx
- dnsgen
- altdns
- goaltdns
- gotator

```
echo www.example.com | alterx

   ___    ____           _  __
  / _ | / / /____ ____| |/_/
 / __ |/ / __/ -_) __/>  <
/_/ |_/_/\__/\__/_/ /_/|_|

        projectdiscovery.io

prod-www.example.com
www.lib.example.com
www.prod.example.com
dev-www.example.com
lib-www.example.com
lib.www.example.com
www-stage.example.com
stage-www.example.com
wp-www.example.com
prod.www.example.com
www.dev.example.com
www.stage.example.com
www-dev.example.com
www-prod.example.com
www-wp.example.com
dev.www.example.com
stage.www.example.com
wp.www.example.com
www.wp.example.com
www-lib.example.com
[INF] Generated 20 permutations in 0.0021s
```

*** Approximately 3-10% generated alterx domains are detected on retesting**

AI come’s to help

```
$ subgpt -i input.txt -o output.txt -c /path/to/cookies.json

call-prompts-staging.example.com
dclb02-dca1.prod.example.com
activedirectory-sjc1.example.com
iadm-staging.example.com
elevatenetwork-c.example.com
```

SubGPT

No IP/domain?

No IP/domain?

- Ripe DB
- bpb.tools
- Resolutions check
- Hosts certificate

organisation: ORG-IL855-RIPE

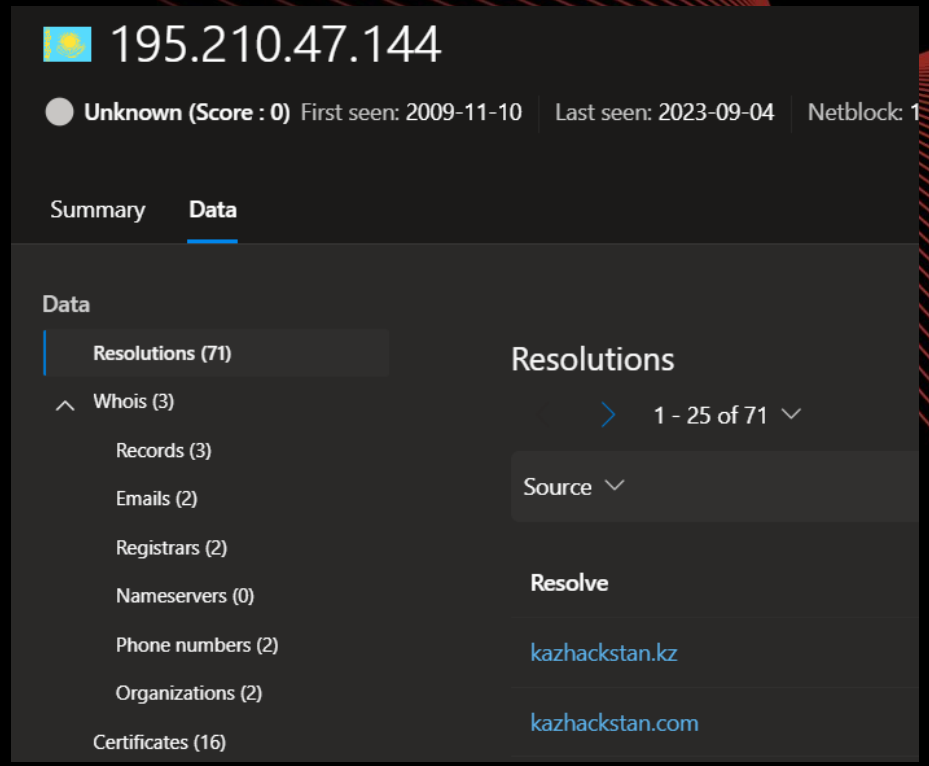
e-mail=info@**innostage**-group.ru, org-name=**Innostage** LLC

Leaf Certificate

920e43b5ff234242c4fd0dec9f676939e1586a0f79ca9e7eee46c730732c4a47

CN=kazhackstan.kz

C=US, O=Let's Encrypt, CN=R3



How to verify?

Passive

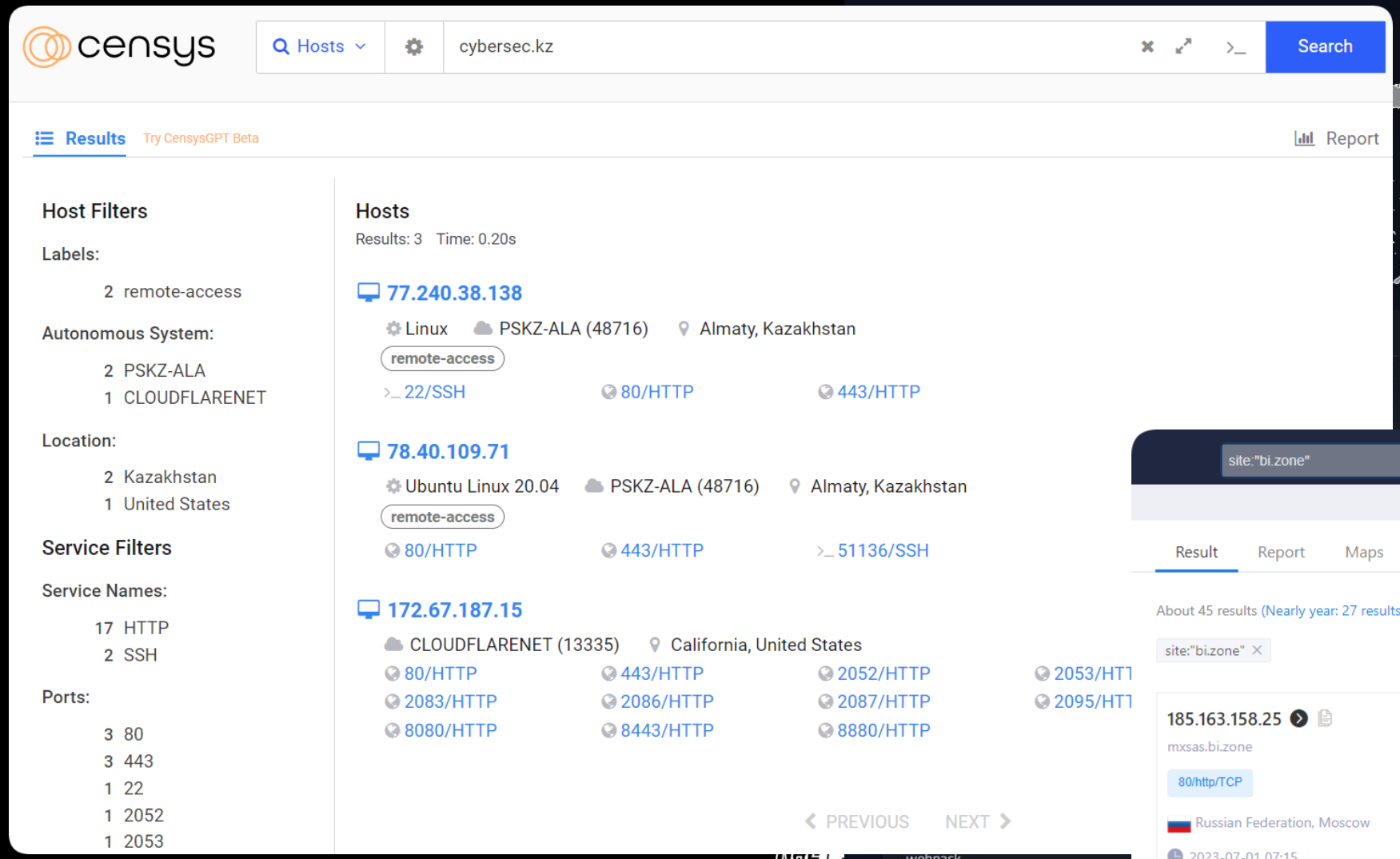
- VirusTotal API
- SecurityTrails API
- ViewDNS API

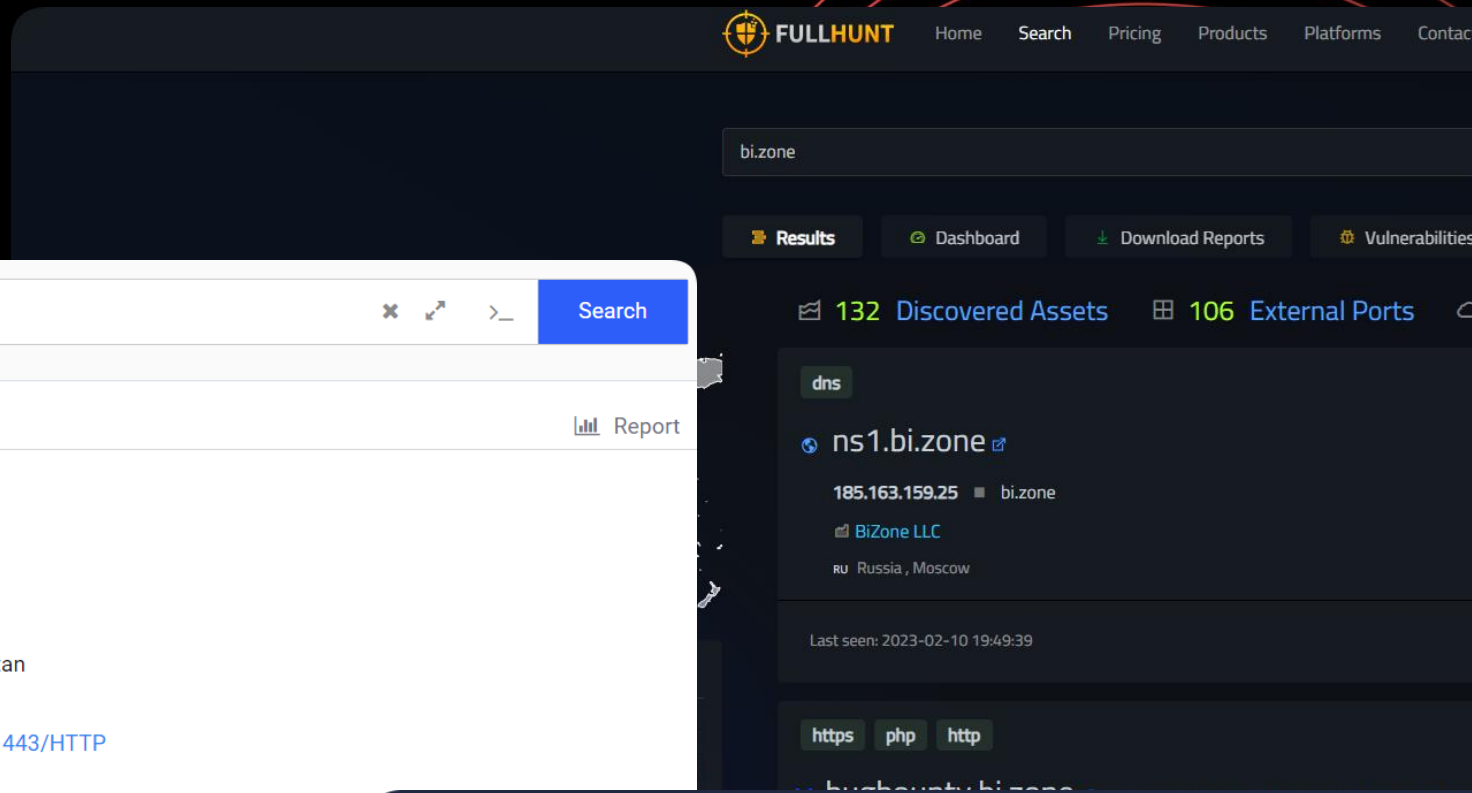
Active

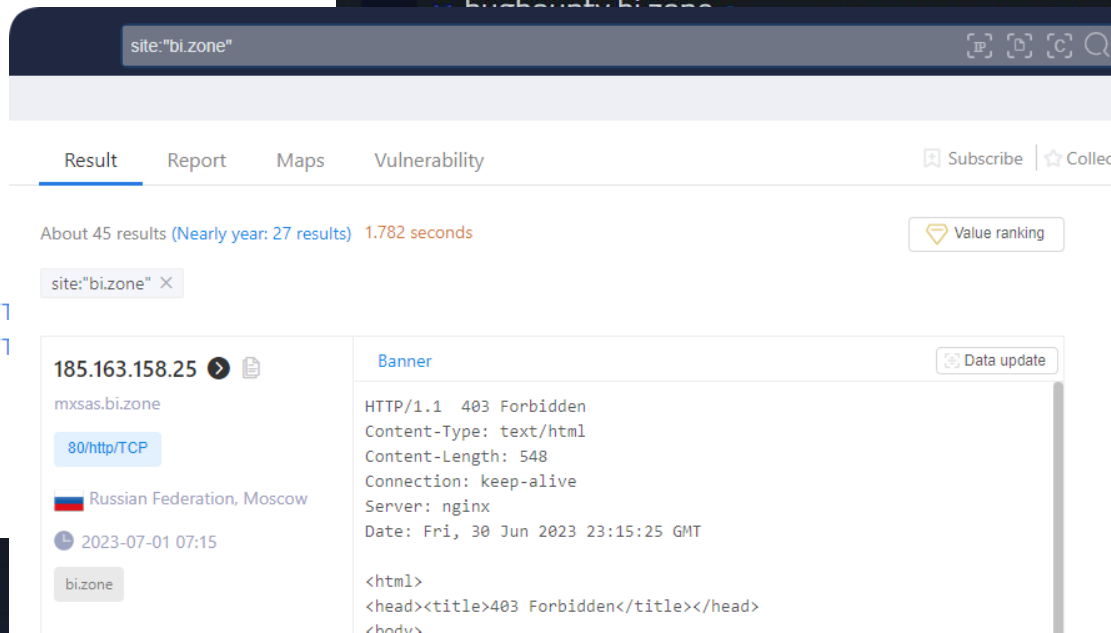
- Anything proxy, API, etc...

BUT only if the NS records point to the DNS server of the hosting/DNS provider

Search engines







Search engines

- Censys
- Shodan
- ZoomEye
- Greynoise.io
- Onyphe
- Fofa
- Binaryedge
- FullHunt
- Netlas
- Quake360
- Criminalip
- Synapsint
- Natlas
- Leakix

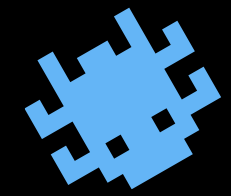
Search engines – Scanned ports

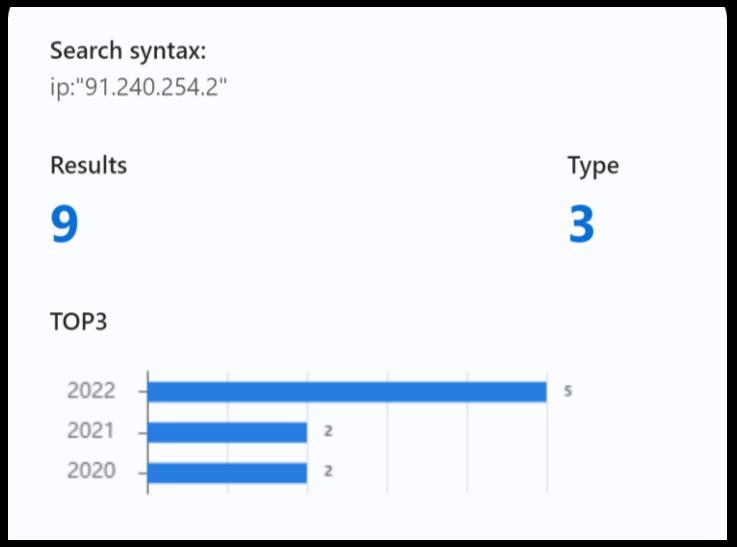
- Censys - ~3,592 (Official)
- Shodan - ~1400 (Shodan Twitter)
- ZoomEye – No info
- Binaryedge - No info
- Netlas - No info
- fofa.info - No info

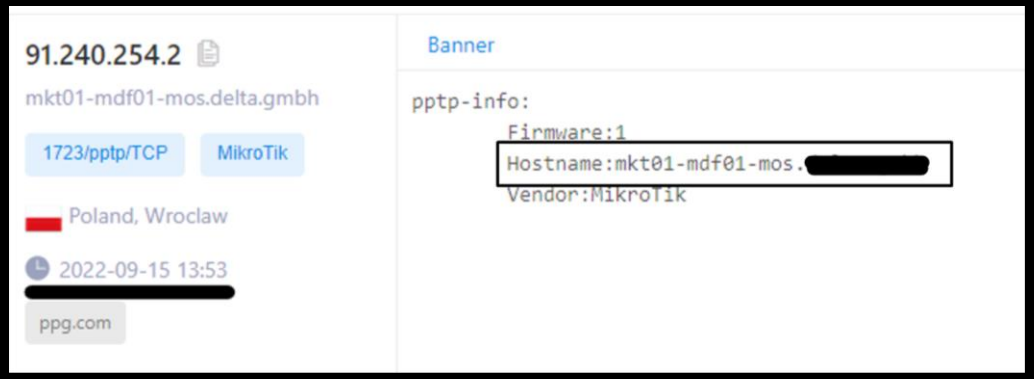
Search engines

- Has the most up-to-date data available: **Censys**
- Has the largest amount of data: **BinaryEdge / ZoomEye**
- Best for finding vulnerabilities: **Netlas**

Old But Gold




Search syntax:
ip:"91.240.254.2"
Results
9
Type
3
TOP3
2022
2021
2020
5
2
2


91.240.254.2
mkt01-mdf01-mos.delta.gmbh
1723/pptp/TCP
MikroTik
Poland, Wroclaw
2022-09-15 13:53
[redacted]
ppg.com
Banner
pptp-info:
Firmware:1
Hostname:mkt01-mdf01-mos.[redacted]
Vendor:MikroTik

Any parameter can be a source of info

Leaf Certificate

0f354ff74de72e1d04926832689885b86928f67a052a4a813d59b3343f8e6364

C=RU, ST=Moscow, L=Moscow, O=OOO Telekom Integraciya, CN=*.it-innosystem.ru

C=BE, O=GlobalSign nv-sa, CN=GlobalSign RSA OV SSL CA 2018

25/smtp

Device	
Product	Postfix smtpd
Version	
Service	smtp
ProtType	TCP
OS	
Updated	2021-08-14 23:18

Banner

```
220 kpc-relay-pa2.kaspersky-labs.com ESMTP Postfix
501 Syntax: EHLO hostname
```

URLs

- Potentially vulnerable parameters
- Sensitive information
- Directory information
- Subdomains
- And a lot of other things.

URLs - Tools

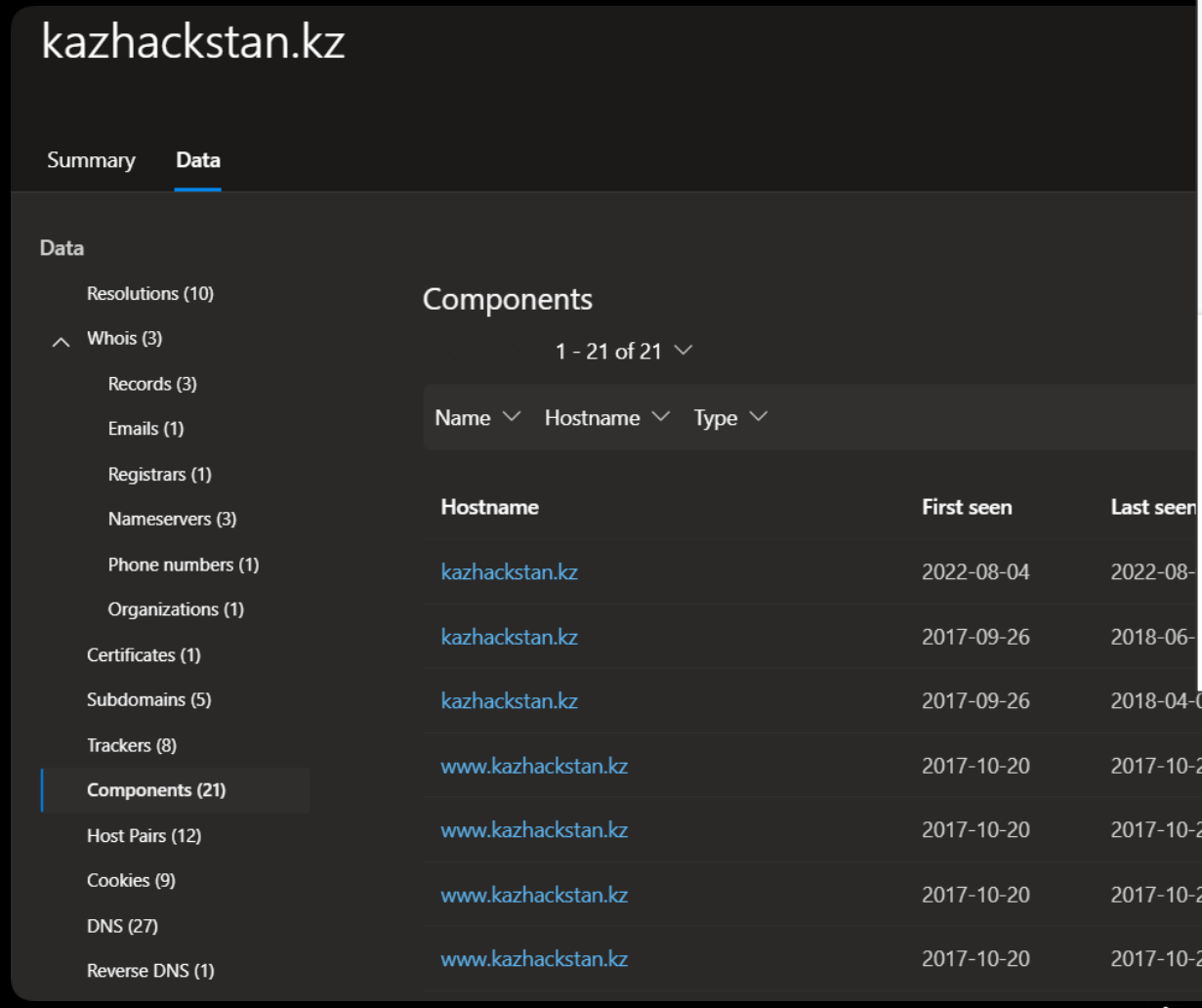
- Gau
- Xurlfind3r
- Unja
- Waymore
- Spiderfoot/theHarvester
- GooFuzz
- rextracter.streamlit.app/

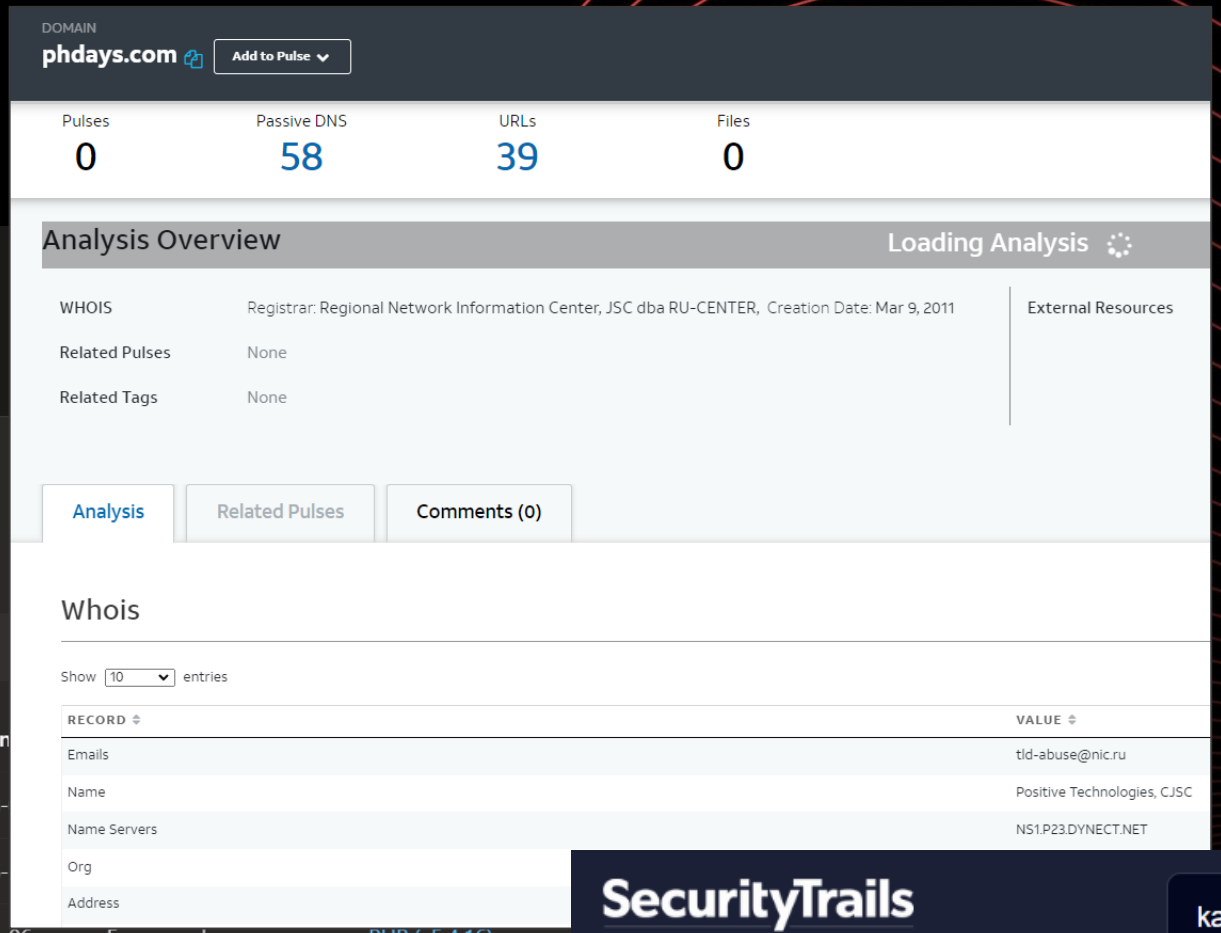
```
$ python3 waymore.py -i example.com -mode U


 _ _ _        _    _ ____
| | | |_____| | | /    \  ___    ____ _____
| | | (____ | | | | | |/ _ \ / ___) ___ |
| | | / ___ | |_| | | | |_| | |   | |_| |
 \___/\_____|\__  |_|_|_|\___/| |   | ____/
           (____/   by Xnl-h4ck3r  \_____)

Links found on archive.org: 1263388
Extra links found on commoncrawl.org: 366649
Extra links found on allienvault.com: 4980
Extra links found on urlscan.io: 219
Links found on *.exanple.com: 1635236
```

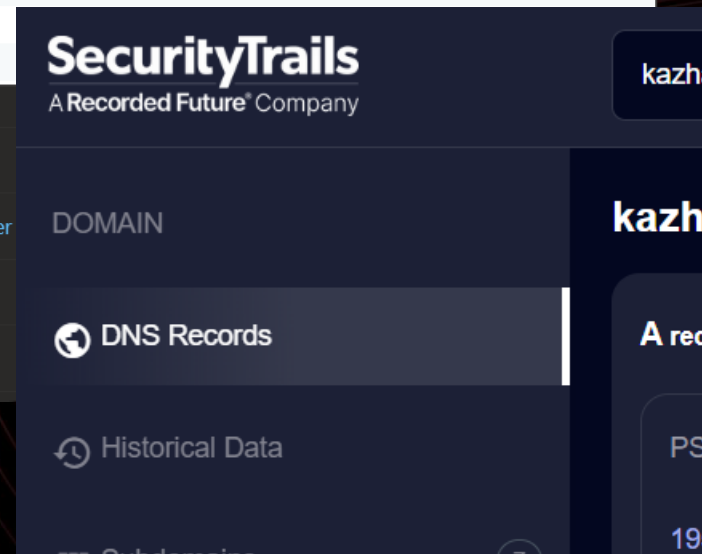
Intelligence systems

- Helpful in:
  - In a detailed analysis of the infrastructure;
  - Collecting subdomains;
  - Searching for Domain resolutions IP
  - Collecting trackers and components

Intelligence systems







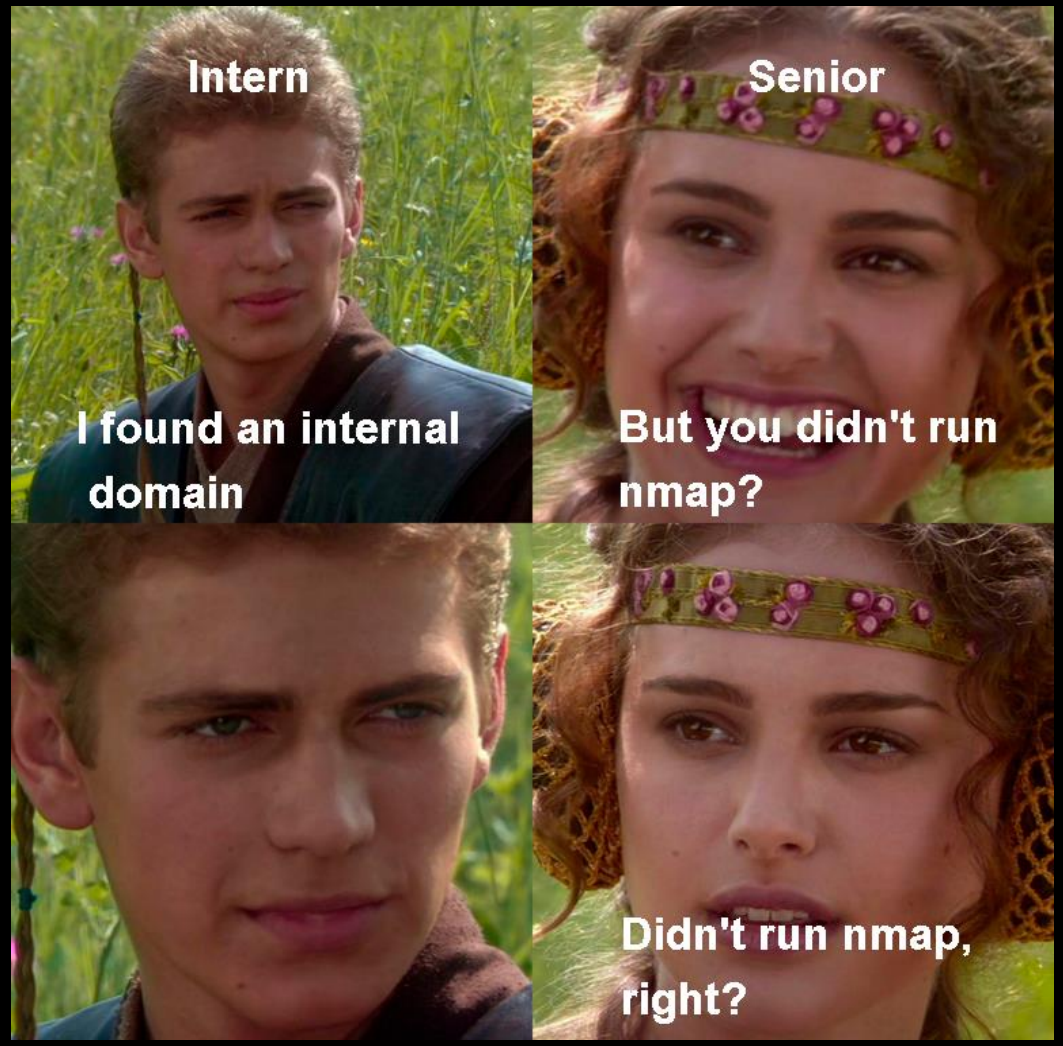
KAZHACKSTAN TURAN — 2023

Hacktricks

```
└─# curl -I -k -X POST -H 'Authorization: NTLM TlRMTVNTUAABAAAAB4IIogAAAAAAAAAAAAAAAAAAAAAKANc6AAAADw==' -H 'Content-L
HTTP/1.1 401 Unauthorized
Server: Microsoft-IIS/10.0
request-id: 0287a547-54f3-46ed-bd7e-68862174516d
WWW-Authenticate: NTLM TlRMTVNTUAACAAAADgAOADgAAAAFgomiZzeoaM1ekfIAAAAAAAAAAPwA/ABGAAAACgBjRQAAAA9SAEEATQBCAEwARQBSAAI
GkAYQAuAGMAbwBtAAMATgBzAHIAdgAtAG0AYQBpAGwAMQAwAC0AbwBzAHQALgByAGEAbQBiAGwAZQByAC4AcgBhAG0AYgBsAGUAcgBtAGUAZABpAGEALgB
X-OWA-Version: 15.2.1118.20
WWW-Authenticate: Negotiate
X-Powered-By: ASP.NET
X-FEServer: SRV-MAIL10-OST
WWW-Authenticate: Basic realm="mail.rambler-co.ru"
Date: Mon, 06 Mar 2023 14:13:34 GMT
Content-Length: 0


┌──(root㉿kali)-[/home/kali]
└─# echo 'TlRMTVNTUAACAAAADgAOADgAAAAFgomiZzeoaM1ekfIAAAAAAAAAAPwA/ABGAAAACgBjRQAAAA9SAEEATQBCAEwARQBSAAIADgBSAEEATQBC
BtAAMATgBzAHIAdgAtAG0AYQBpAGwAMQAwAC0AbwBzAHQALgByAGEAbQBiAGwAZQByAC4AcgBhAG0AYgBsAGUAcgBtAGUAZABpAGEALgBjAG8AbQAFADAA
Found NTLMSSP header
Msg Type: 2 (Challenge)
Target Name: u'RAMBLER' [520041004d0042004c0045005200] (14b @56)
Challenge: 0xf2915ecd68a83767
Context: '' [] (0b @0)
Target: [block] (252b @70)
    AD domain name (2): RAMBLER
    Server name (1): SRV-MAIL10-OST
    DNS domain name (4): rambler.ramblermedia.com
    FQDN (3): srv-mail10-ost.rambler.ramblermedia.com
    Parent DNS domain (5): rambler.ramblermedia.com
    Server Timestamp (7): ♦ў♦5P♦
OS Ver: '??cE????'
Flags: 0x-5d767dfb ["Negotiate Unicode", "Request Target", "Negotiate NTLM", "Negotiate Always Sign", "Target Type Dom
```

```
passport.use(new LdapStrategy({
  server: {
    url: 'ldap://ldcro.rambler.ramblermedia.com:389',
    bindDn: "ldap.library",
    bindCredentials: "PZKFsS45M3ctYKb",
    searchBase: "ou=company,dc=rambler,dc=ramblermedia,dc=com",
    searchFilter: "(&(objectcategory=person)(objectclass=user)(|(samaccountname={{username}})(mail={{username}})))",
    searchAttributes: ["cn", "uid", "id", "ruid", "displayName", "mail", "givenname", "enabled", "role", "projects"]
  }
}));
```

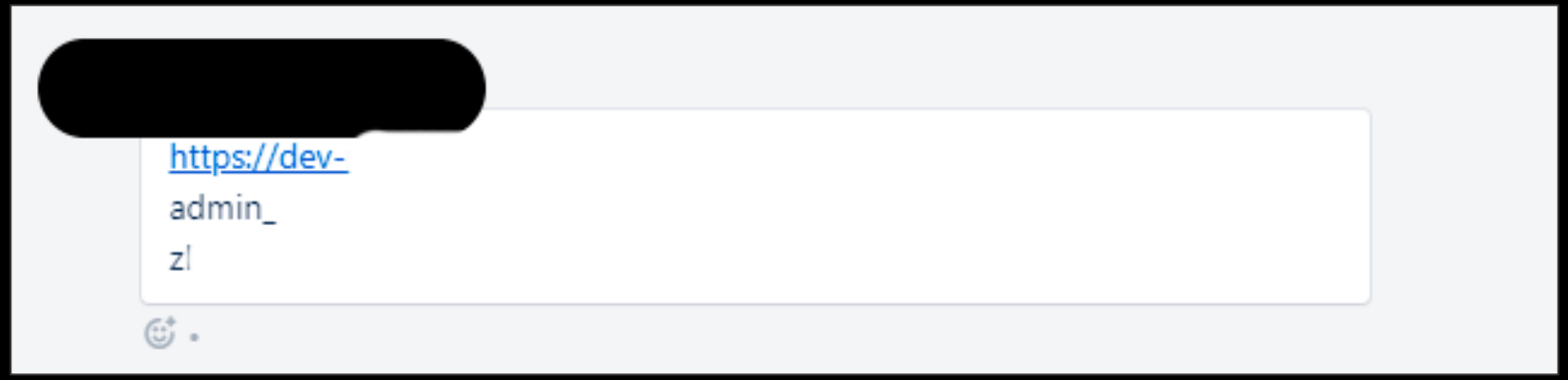
NO NMAP!


Intern
I found an internal domain
Senior
But you didn't run nmap?
Didn't run nmap, right?

HackTricks or Luck?

One of the largest stock exchanges in the world:

- 3 internal domains/subdomains,
- internal information
- 4 external subdomains of development department
- Account for logging in to the administrative panel of the site development



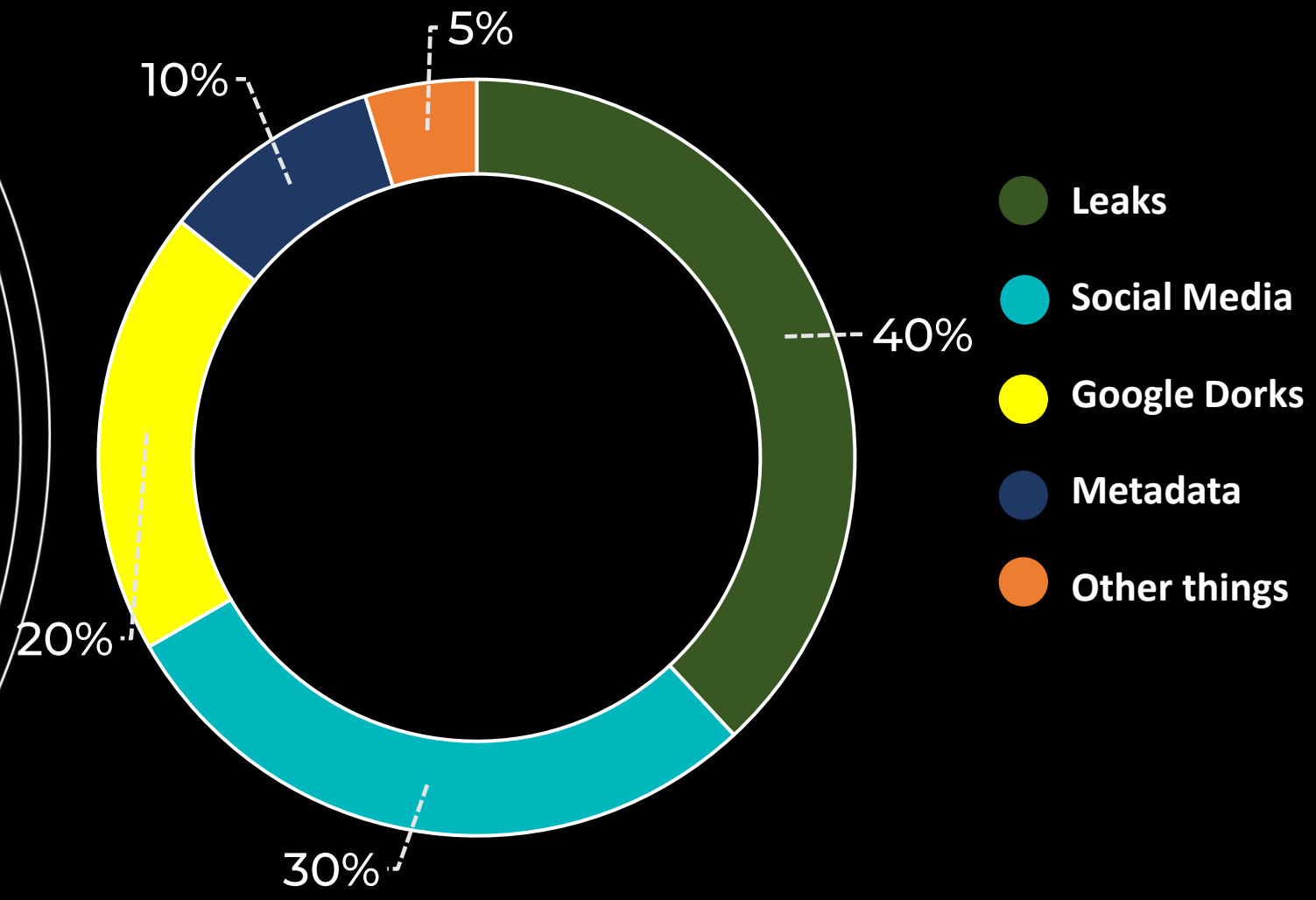
Сотрудник: Выкладывает любую информацию о себе в социальные сети

Осинтер:

Looking for

- Full name
- Emails / Logins
- Passwords
- Phone number
- Personal data (everything else)

Main sources of info

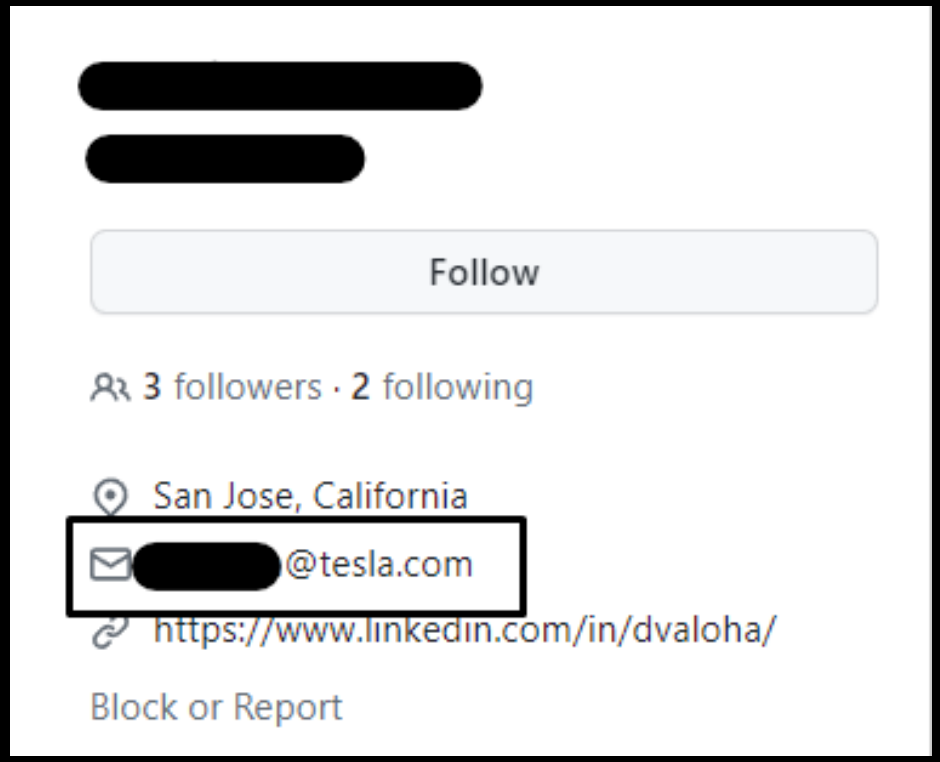


KAZHACKSTAN TURAN - 2023

Leaks

- Rostelecom
- Яндекс Еда
- 2 Berega
- Delivery Club
- Умный дом
- Яндекс Практикум
- Oriflame
- Туту.ру
- Tele2
- Twitter
- Facebook
- Онлайн Трейд
- CDEK
- Wildberries
- Pikabu
- Avito
- Гемотест
- CDEK v2.0
- Почта России
- Kari
- DNS
- ВкусВилл

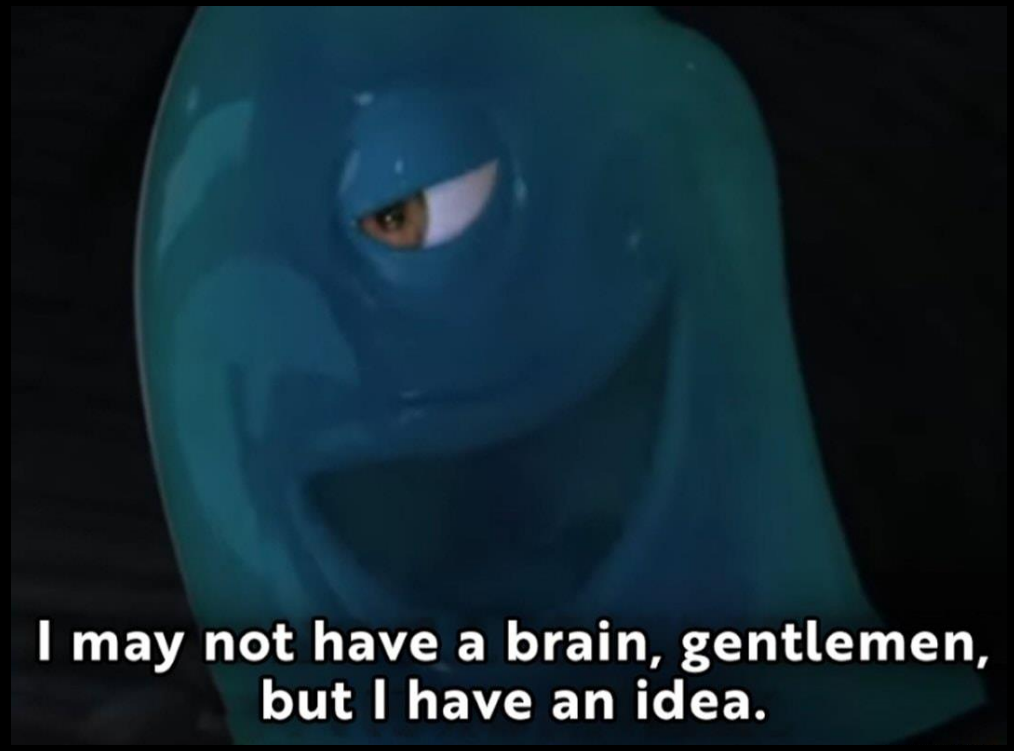
Public(?) Leaks



KAZHACKSTAN TURAN - 2023

Public(?) Leaks

- 2+2 = + 5 000 000 GitHub users emails
- Company emails, names

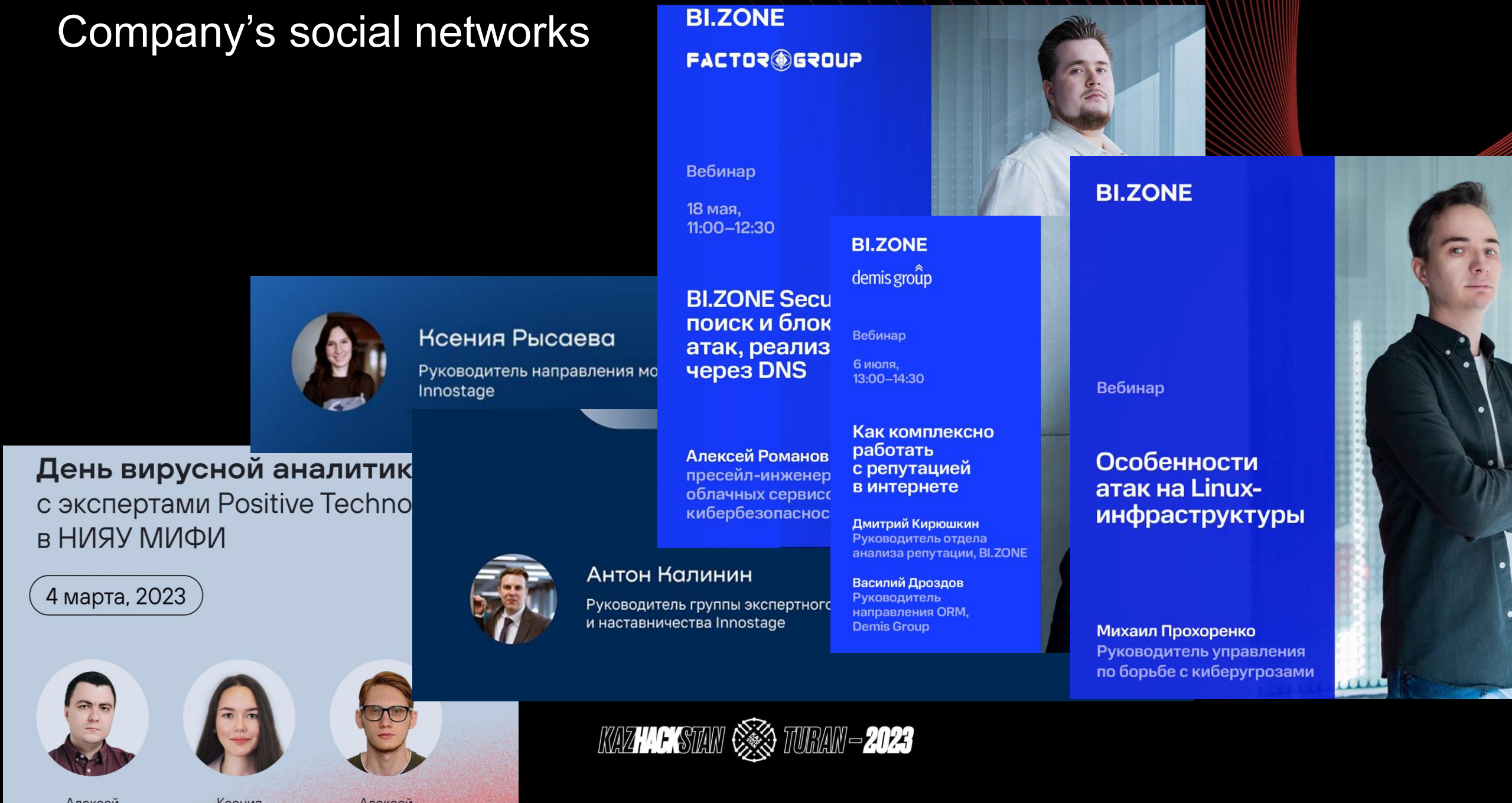


Company’s social networks

- Posts mentioning employees/positions/events
- Analyzing the drafting of messages
- Collection of employee social media accounts
- Partner analysis

KAZAKHSTAN TURAN – 2023

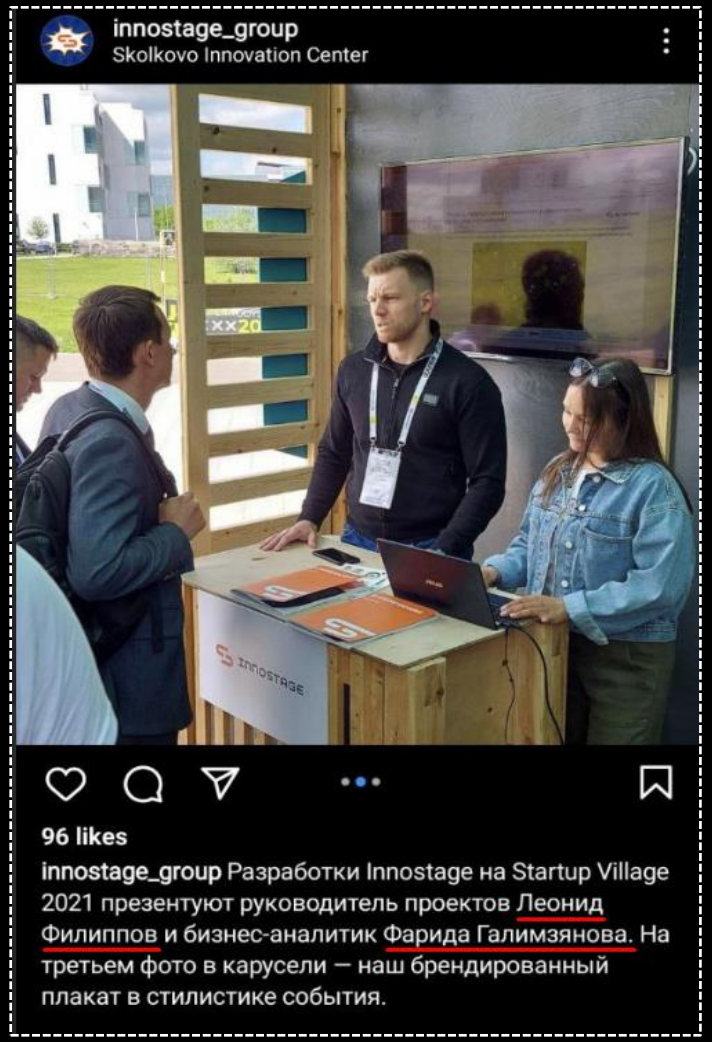
Company’s social networks

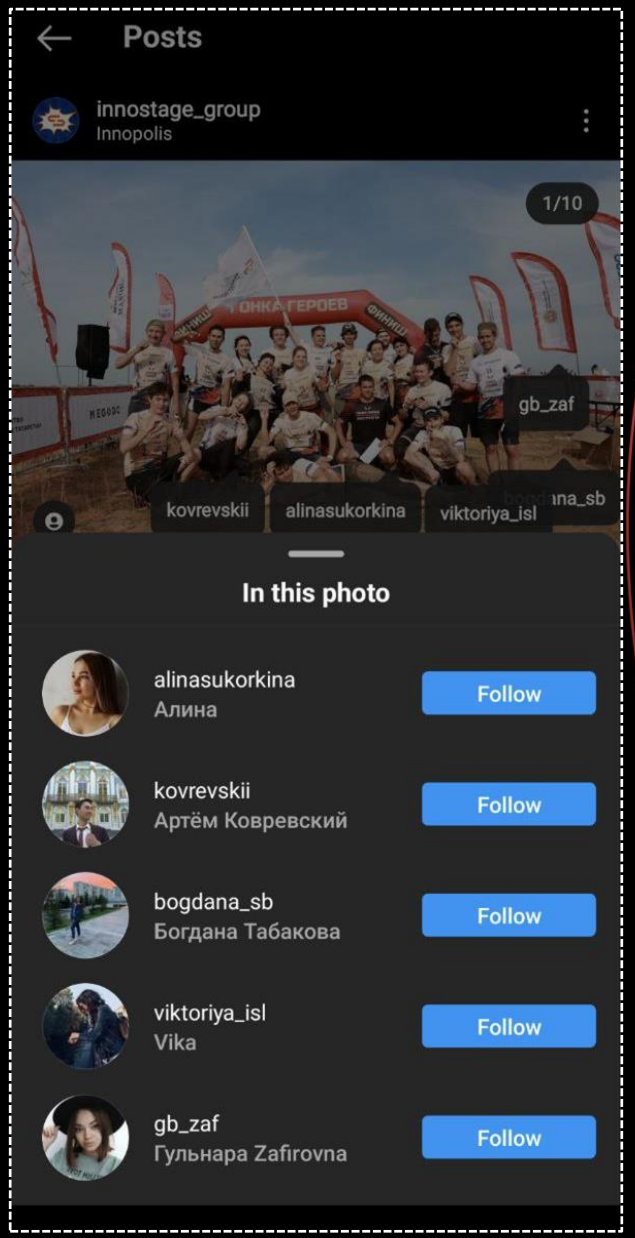


Employee’s social networks

- Workplace
- #Hashtags / Photo Mentions
- Geolocation on photo
- Geolocation spoofing

#Hashtags / Photo Mentions

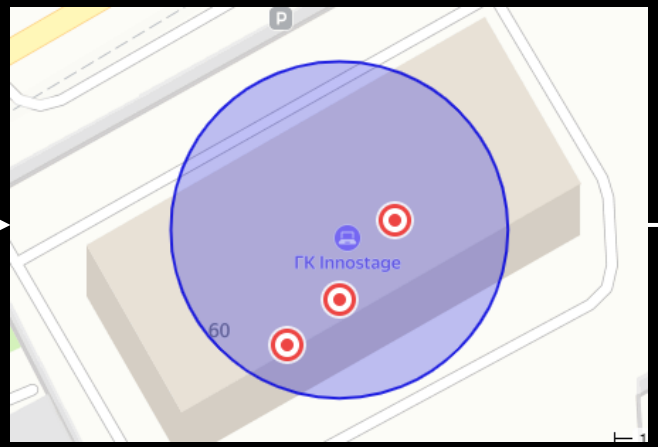


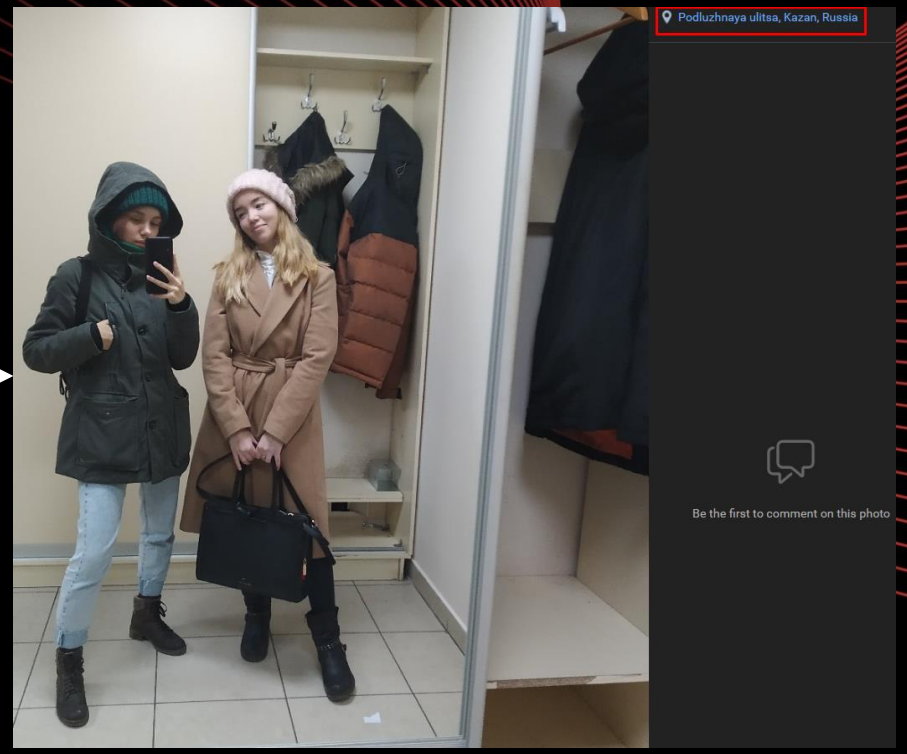


Employee's social networks

info@innostage-group.ru

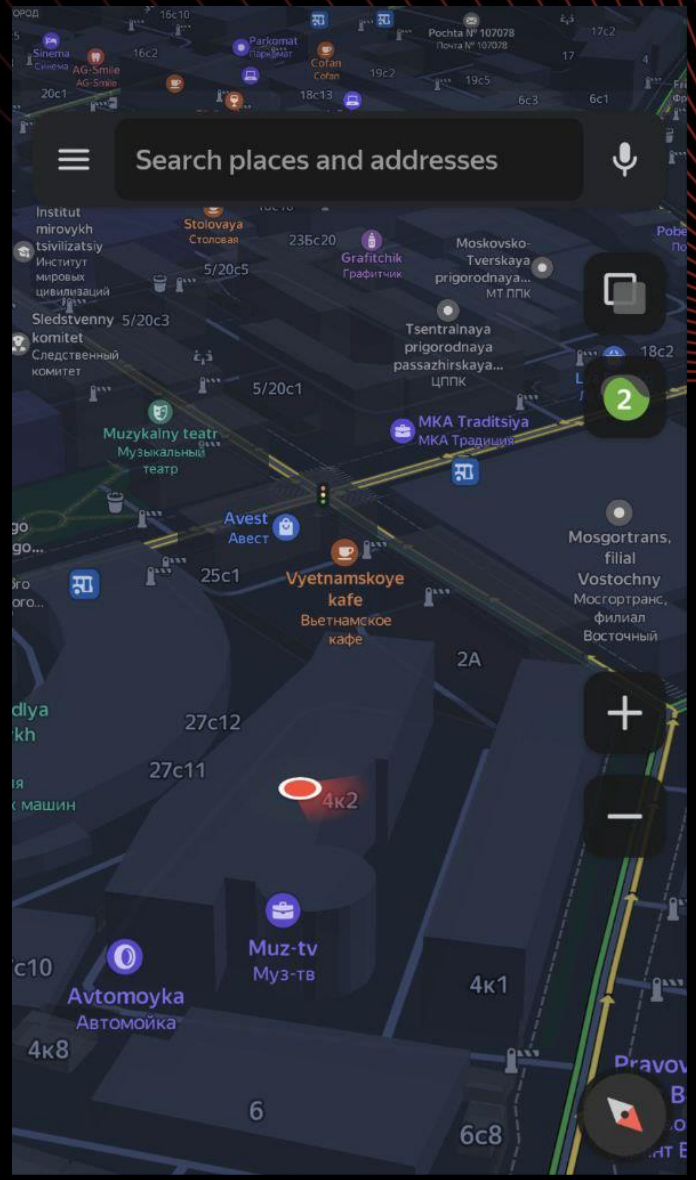
Kazan, Podluzhnaya str. 60,





Geolocation spoofing

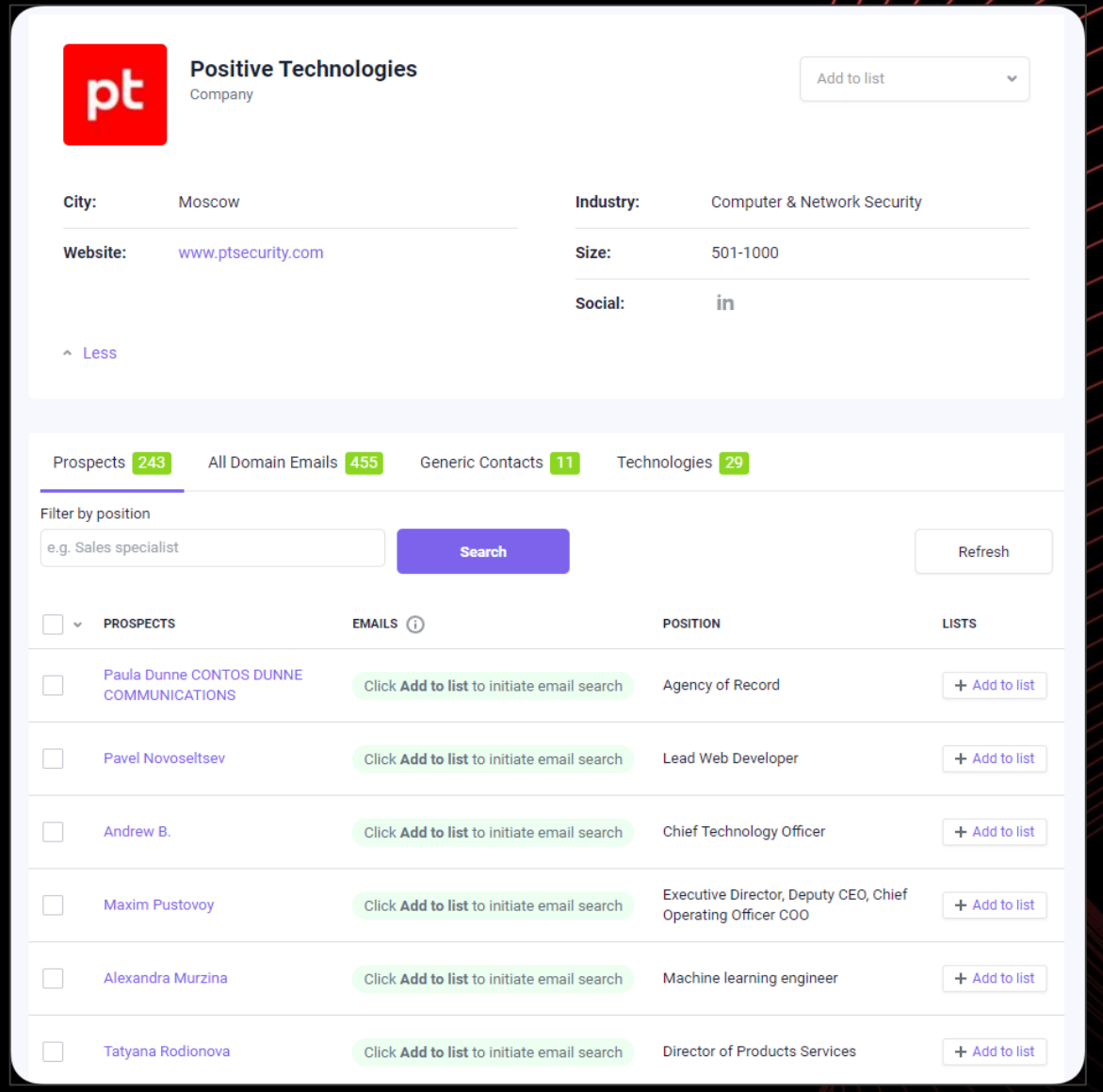
- **Geolocation spoofing**
- **Detects People Nearby**
- **Works in Telegram and VK**
- **Verification can be done by common groups**

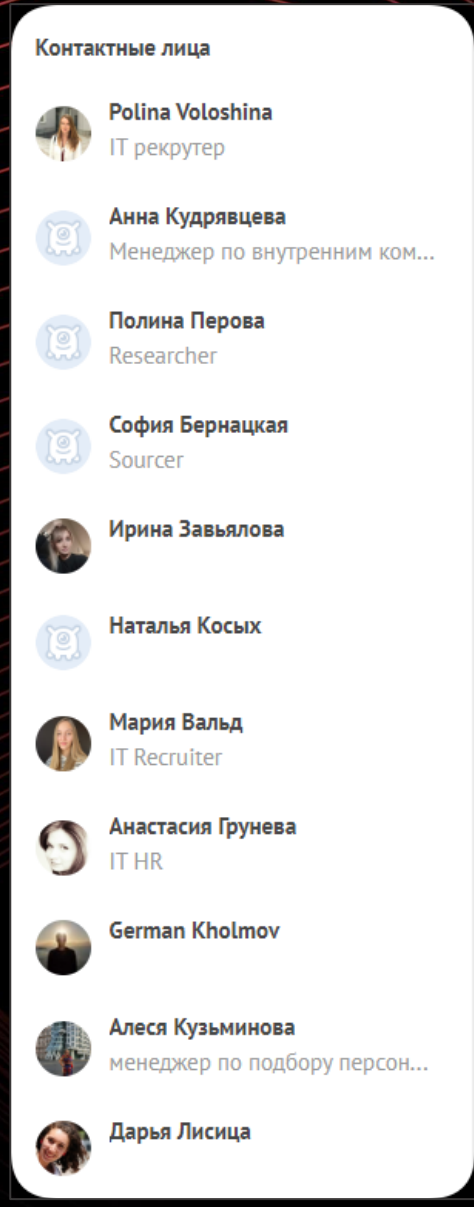


KAZHACKSTAN TURAN – 2023

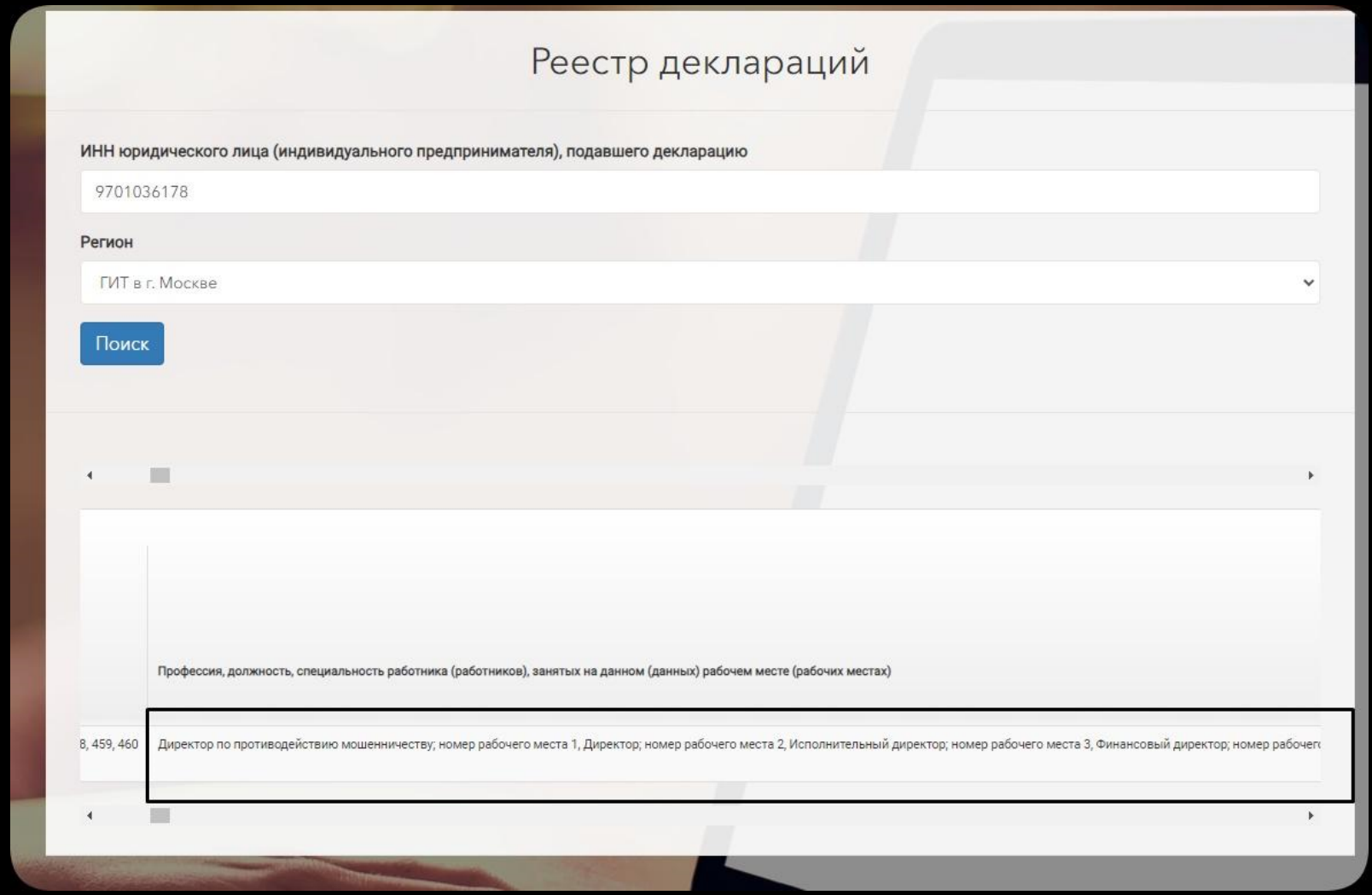
Job aggregators

- VK, FB, etc...
- hh.ru, Habr page
- LinkedIn page (hunter.io, snov.io)





Positions in company

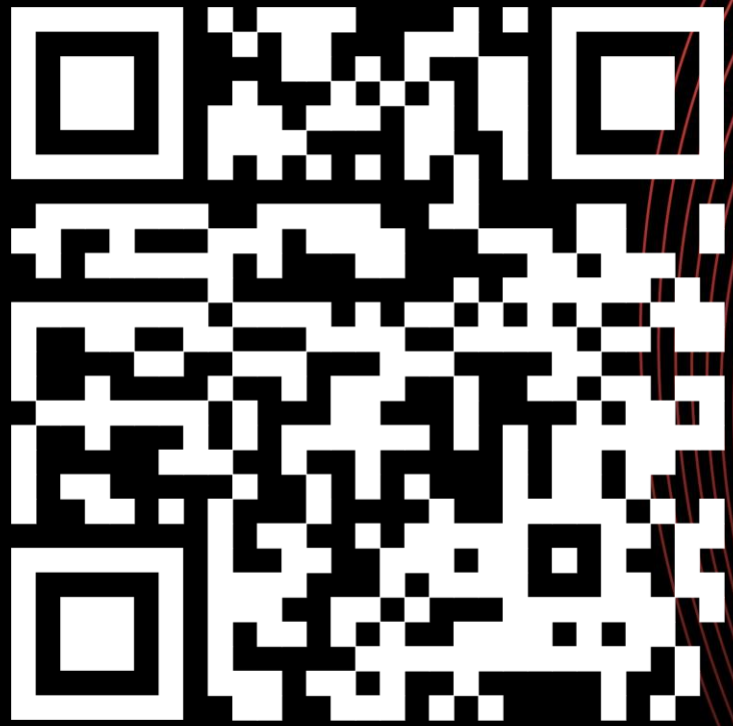


GitHub Dorks

- Looking for additional emails
- <company> login/user/pass/password
- <company> ldap
- <company> wiki
- <company> connectionstrings

Google Dork

- Subdomains
- Emails
- Juicy files/hosts
- GitHub/GitLab/Pastebin /etc mentions



Practice time

- TryHackMe
  - seargoogledorking
  - chlightosint
  - shodan
  - geolocatingimages
  - somesint
  - Sakura
  - Redteamrecon
- CTF
- Just pick a company and start Recon

FREEDOM HOLDING CORP.

Комитет по информационной безопасности МЦРИАП РК

Служба государственной охраны

KHS

thank you for your attention

Questions?