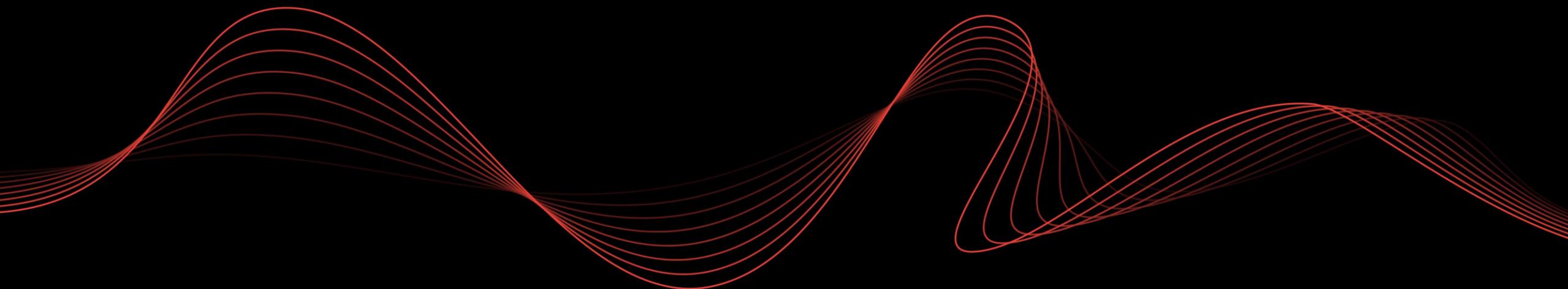




«Offensive OSINT»

Aleksandr Goncharov



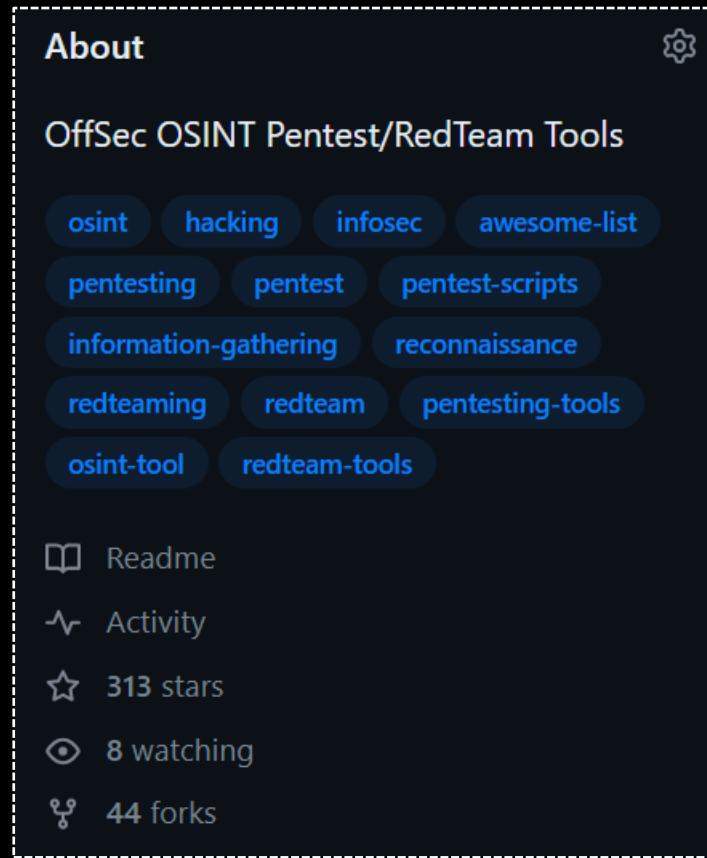
WHOAMI?

- 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

- Search Engines
- Emails collector
- References in the code
- SubDomain collector
- URL
- Dark Web
- Intelligence
- Network Info
- DnsHistory
- Certifications
- FTP servers
- Passive Infrastructure scanner
- Microsoft Exchange
- Telegram
- Google Dorks
- Nickname search
- Phone number
- Wifi
- Cloud



OSINT is dead?



Is OSINT actually Overrated?

161 views

← Thread Open app

 [Vic @ #AllThingsOpen](#)
@VicVijayakumar ...

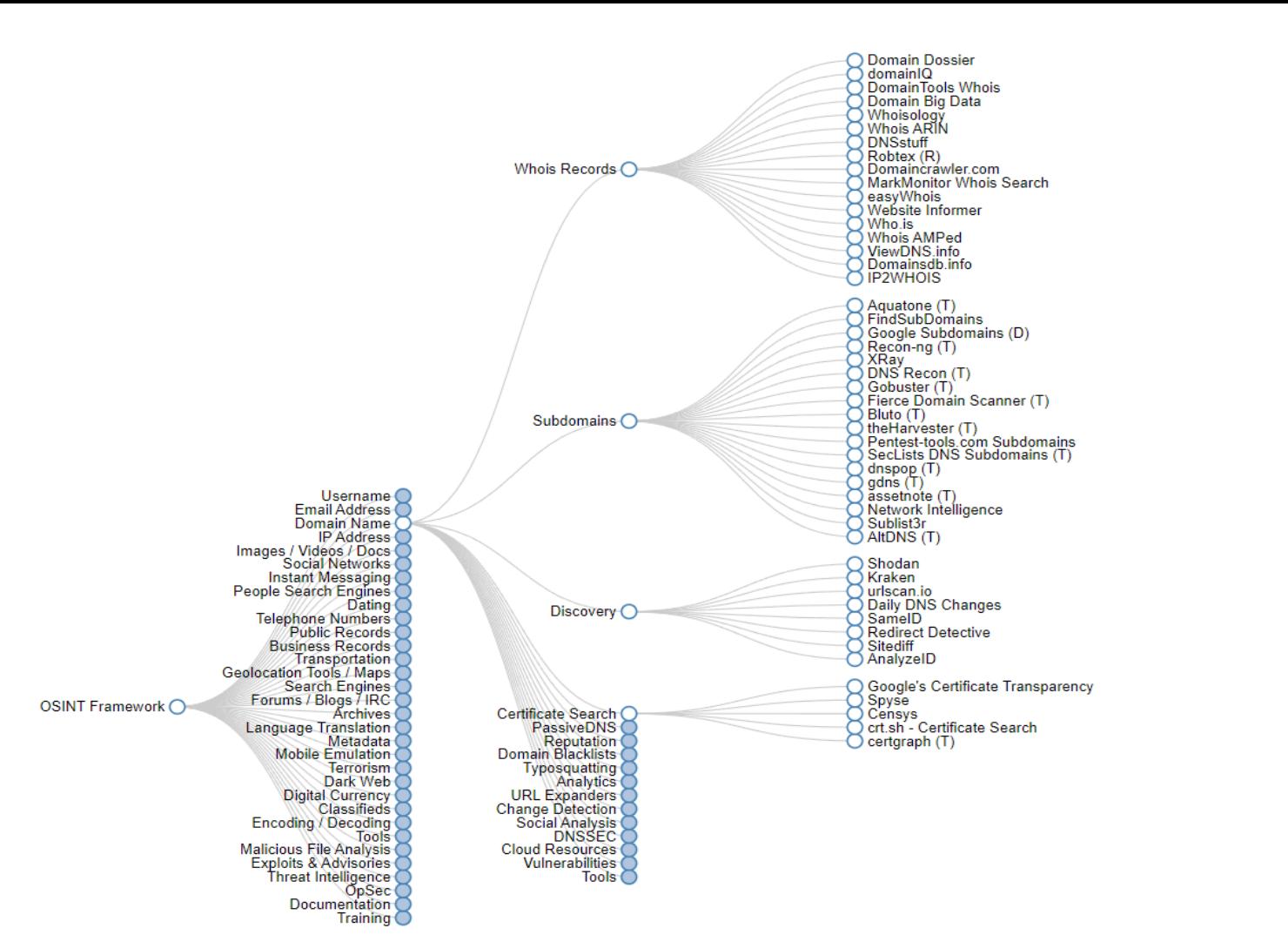
1995: OSINT is dead, learn ColdFusion
2002: OSINT is dead, learn ASP .net
2003: OSINT is dead, learn Django
2004: OSINT is dead, learn Ruby on Rails
2010: OSINT is dead, learn Flask
2011: OSINT is dead, learn AngularJS
2016: OSINT is dead, learn Next.js
2023: okay this is awkward

10:14 PM · Nov 1, 2022 · Twitter Web App

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

SecurityTrails

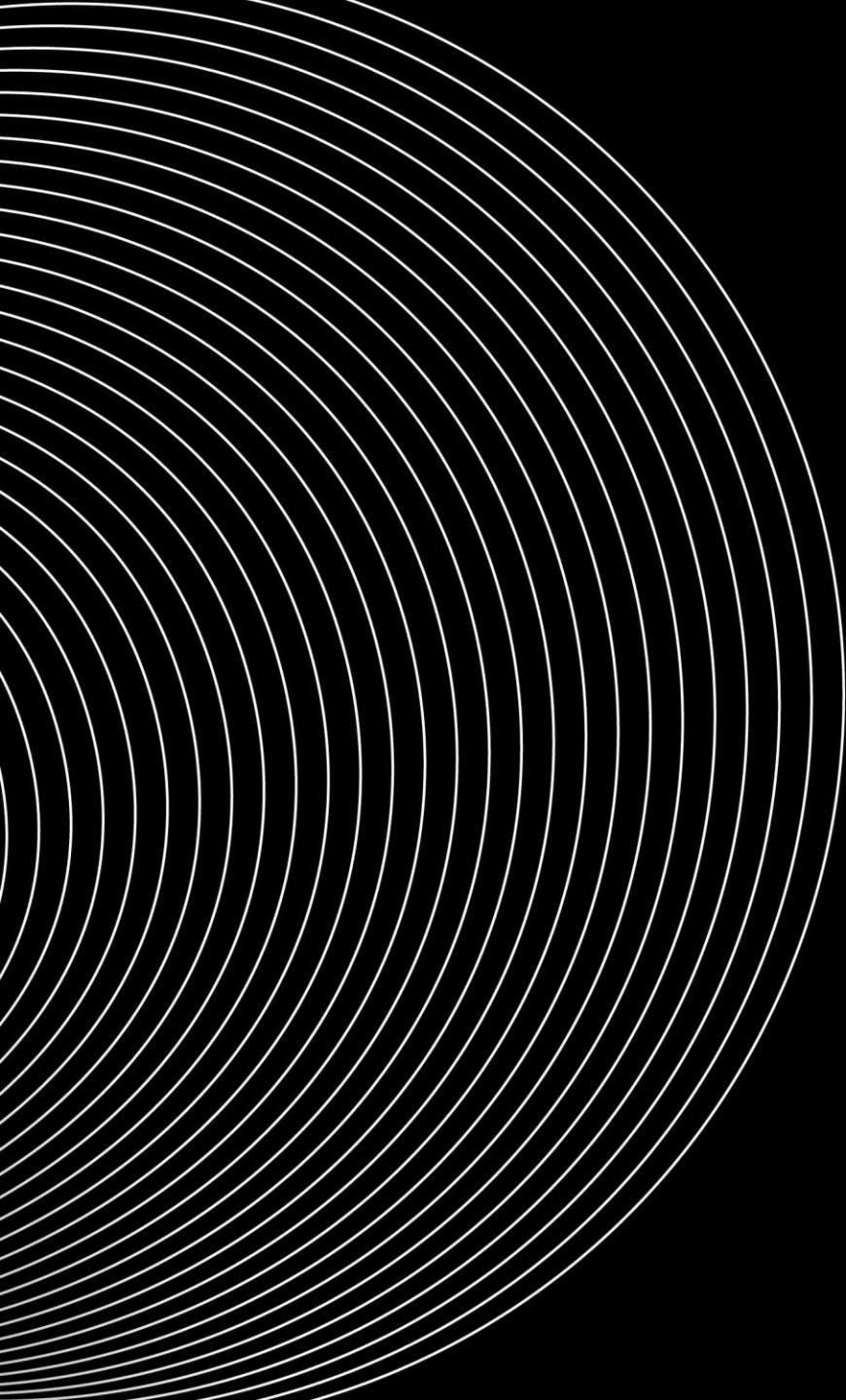
15 Top OSINT Tools

@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



S T Security 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

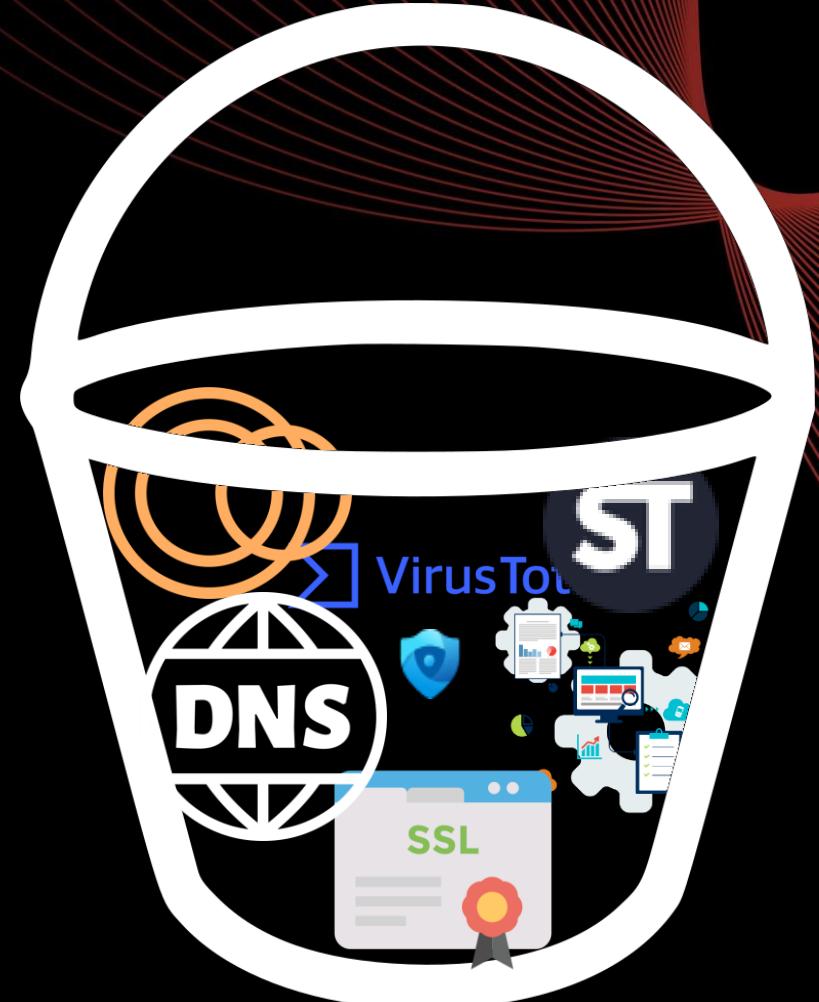
192.68.68.0/24
*.hackdomaim.com

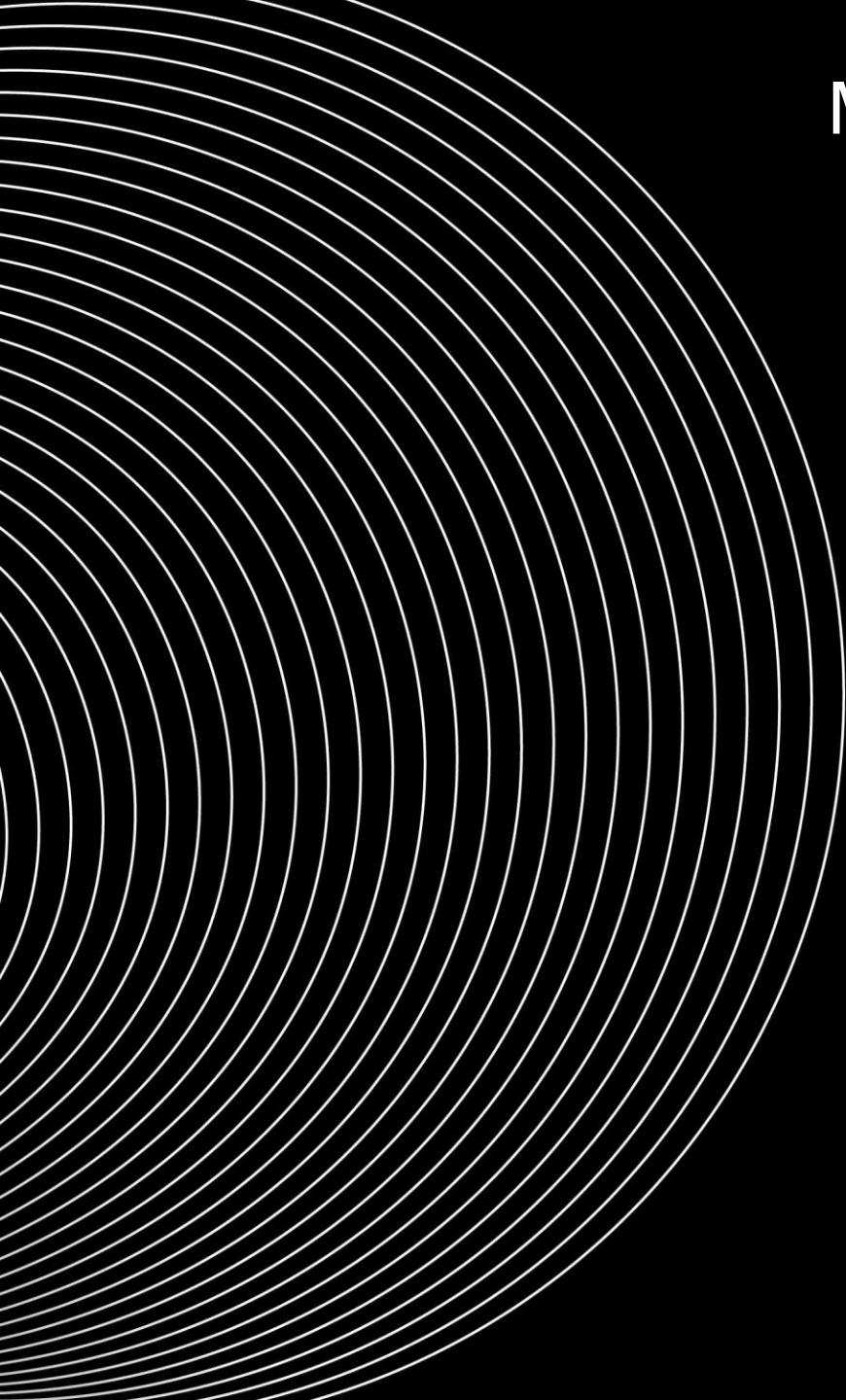
Just a name

Horns & Hooves

Where subdomains are born?

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



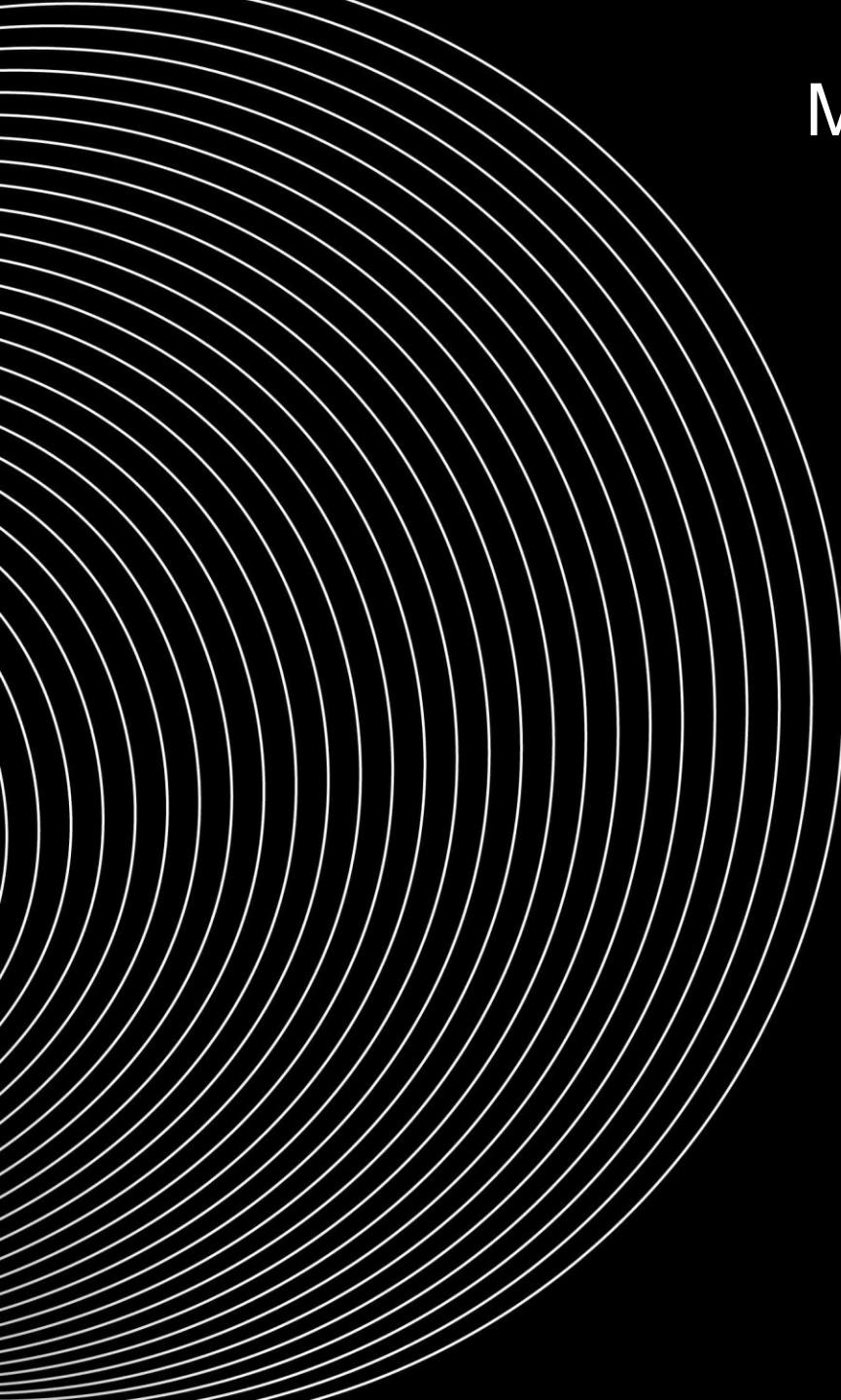


Most useful subdomain search tools

- 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
- goaldns
- gotator

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

```
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
```



AI come's to help



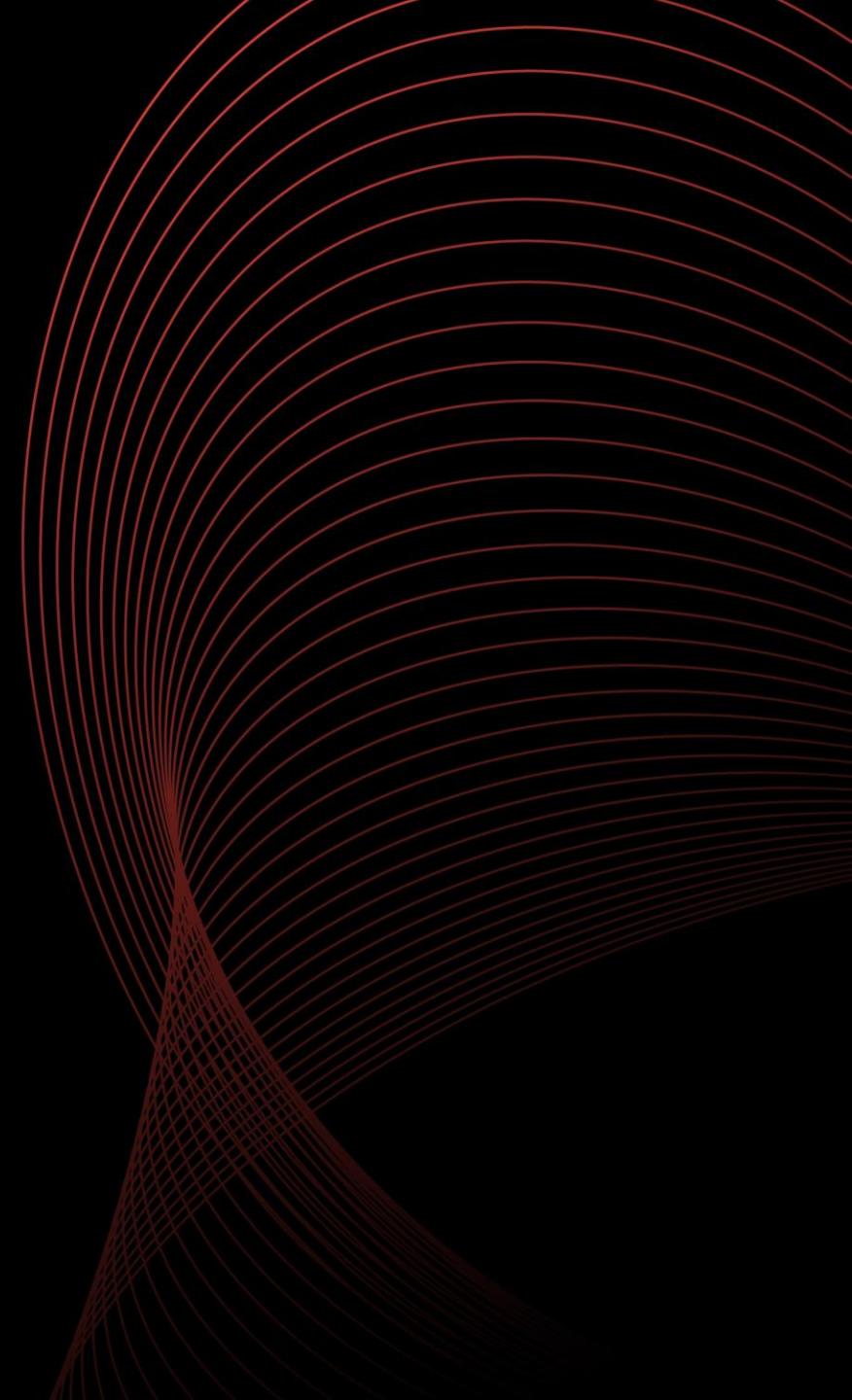
```
$ subgpt -i input.txt -o output.txt -c /path/to/cookies.json
```

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



SubGPT

KAZAKHSTAN  TURAN-2023



No IP/domain?



imgflip.com

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

The screenshot shows a network analysis interface for the IP address 195.210.47.144. The top bar displays the IP address with a Kazakhstan flag icon, its status as 'Unknown (Score : 0)', and metadata like 'First seen: 2009-11-10' and 'Last seen: 2023-09-04'. Below this, there are two tabs: 'Summary' and 'Data', with 'Data' being active. A sidebar on the left lists various data types with their counts: Resolutions (71), Whois (3), Records (3), Emails (2), Registrars (2), Nameservers (0), Phone numbers (2), Organizations (2), and Certificates (16). The main right panel is titled 'Resolutions' and shows a list of 1-25 of 71 entries, with 'Source' and 'Resolve' buttons. Two specific entries are highlighted: 'kazhackstan.kz' and 'kazhackstan.com'.

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



Hosts

cybersec.kz

Search

Results Try CensysGPT Beta

Host Filters

Labels:

2 remote-access

Autonomous System:

2 PSKZ-ALA
1 CLOUDFLARENET

Location:

2 Kazakhstan
1 United States

Service Filters

Service Names:

17 HTTP
2 SSH

Ports:

3 80
3 443
1 22
1 2052
1 2053

Hosts

Results: 3 Time: 0.20s

77.240.38.138

Linux PSKZ-ALA (48716) Almaty, Kazakhstan

remote-access

22/SSH

80/HTTP

443/HTTP

78.40.109.71

Ubuntu Linux 20.04 PSKZ-ALA (48716) Almaty, Kazakhstan

remote-access

80/HTTP

443/HTTP

51136/SSH

172.67.187.15

CLOUDFLARENET (13335) California, United States

80/HTTP

443/HTTP

2052/HTTP

2053/HT1

2083/HTTP

2086/HTTP

2087/HTTP

2095/HT1

8080/HTTP

8443/HTTP

8880/HTTP

◀ PREVIOUS NEXT ▶

DNSLdap webpack
Basic
Google Tag Manager

bi.zone

Results

Dashboard

Download Reports

Vulnerabilities

132 Discovered Assets

106 External Ports

dns

ns1.bi.zone

185.163.159.25 bi.zone

BiZone LLC

Russia, Moscow

Last seen: 2023-02-10 19:49:39

https php http

site:"bi.zone"

Result

Report

Maps

Vulnerability

Subscribe Collected

About 45 results (Nearly year: 27 results) 1.782 seconds

Value ranking

site:"bi.zone" X

185.163.158.25

mxsas.bi.zone

80/http/TCP

Russian Federation, Moscow

2023-07-01 07:15

Banner

HTTP/1.1 403 Forbidden

Content-Type: text/html

Content-Length: 548

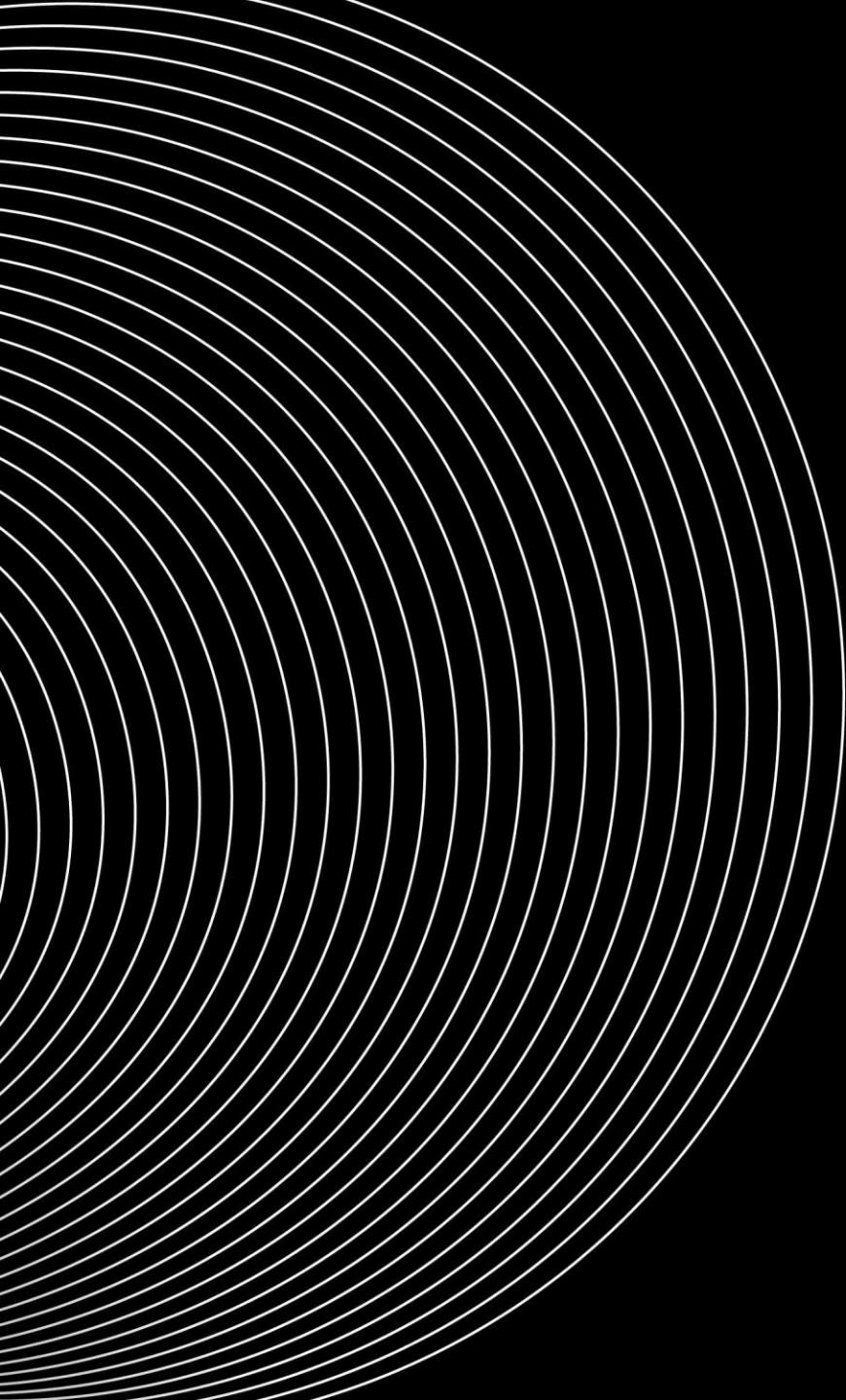
Connection: keep-alive

Server: nginx

Date: Fri, 30 Jun 2023 23:15:25 GMT

<html><head><title>403 Forbidden</title></head><body>

Data update



Search engines

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

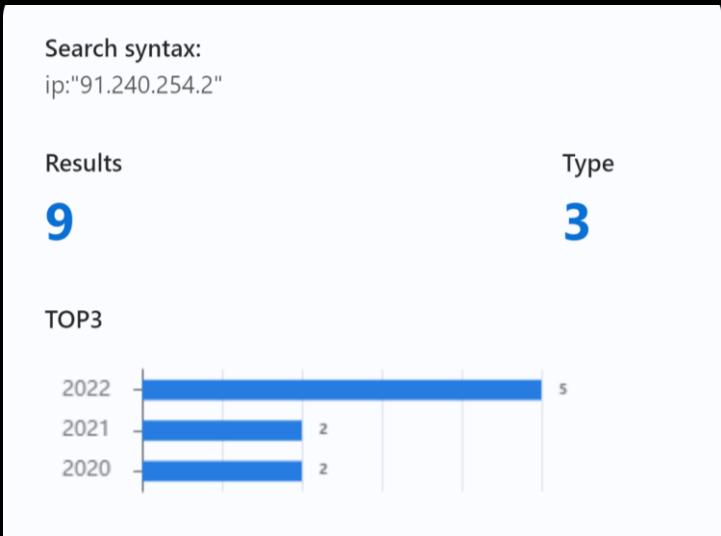
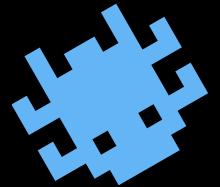
Search engines – Scanned ports

- 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



91.240.254.2

mkt01-mdf01-mos.delta.gmbh

1723/pptp/TCP MikroTik

Poland, Wroclaw

2022-09-15 13:53

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

Postfix smtpd

Version

smtp

Service

TCP

ProtType

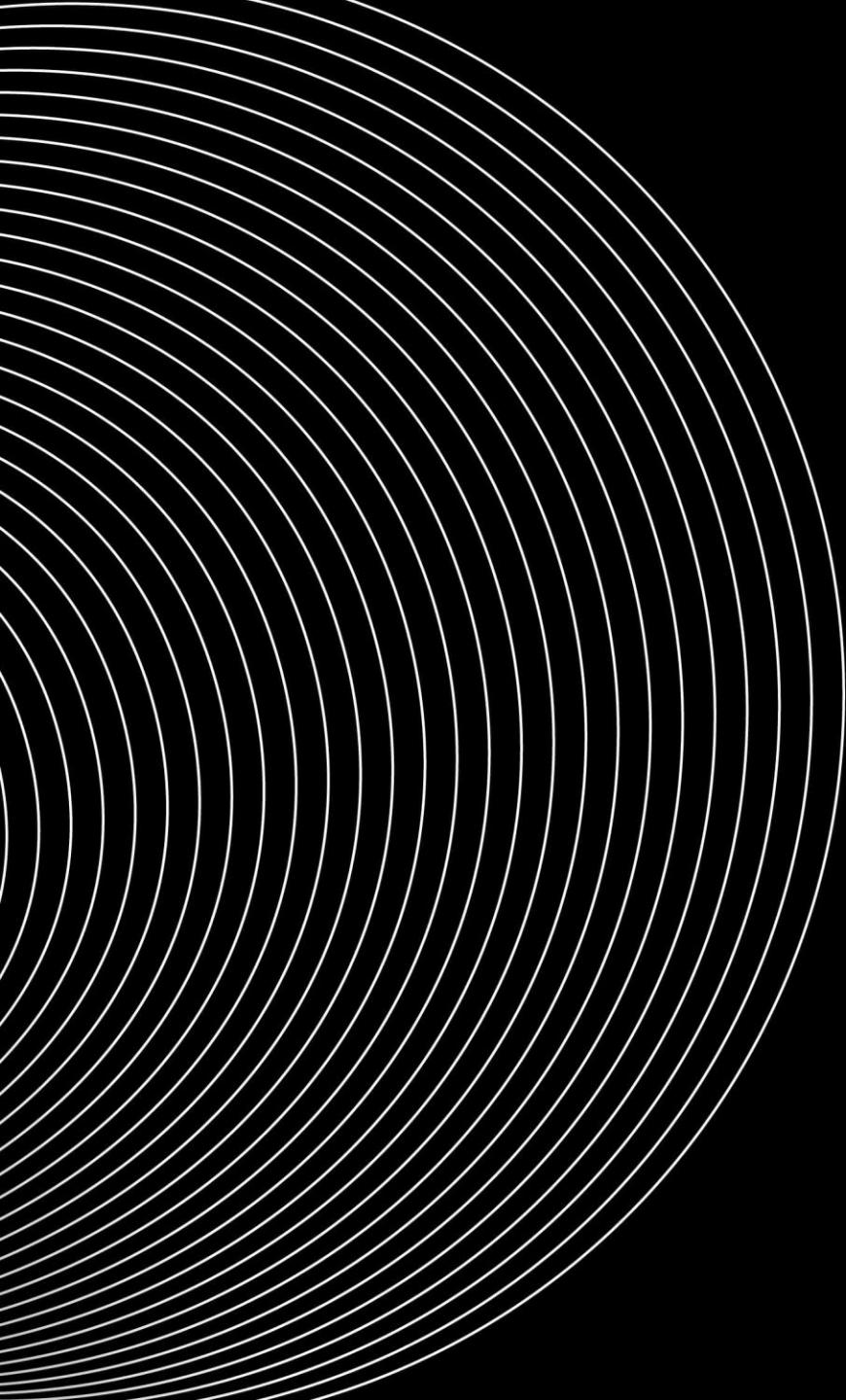
OS

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
 - **reextracter.streamlit.app/**

1

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

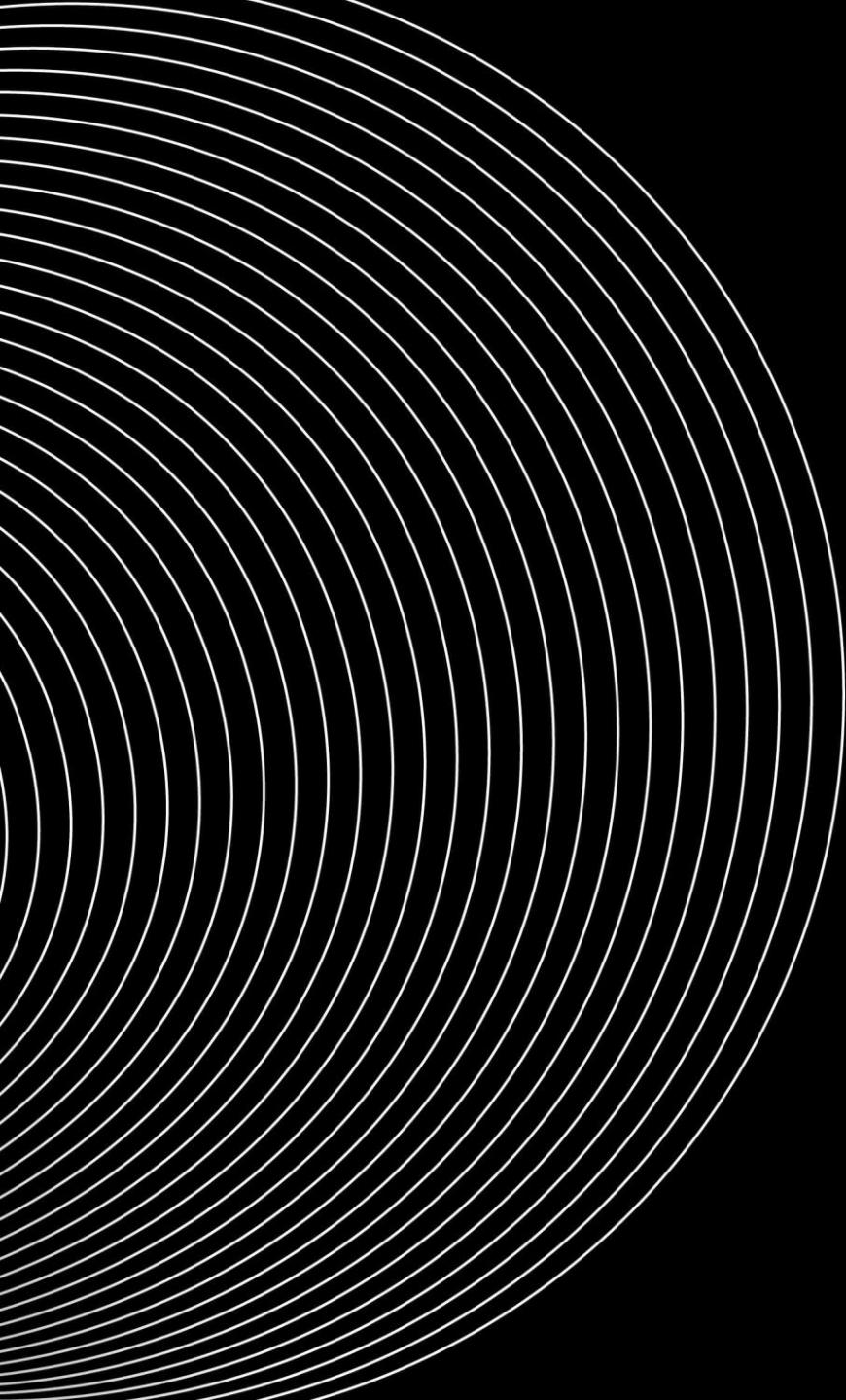
Links found on archive.org: 1263388

Extra links found on commoncrawl.org: 366649

Extra links found on allienvault.com: 4980

Extra links found on urlscan.io: 219

Links found on *.example.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.kz

Summary Data

Data

Resolutions (10)

Whois (3)

Records (3)

Emails (1)

Registrars (1)

Nameservers (3)

Phone numbers (1)

Organizations (1)

Certificates (1)

Subdomains (5)

Trackers (8)

Components (21)

Host Pairs (12)

Cookies (9)

DNS (27)

Reverse DNS (1)

Components

1 - 21 of 21 ▾

Name ▾ Hostname ▾ Type ▾

	Hostname	First seen	Last seen	Framework	PHP (v5.4.16)
	kazhackstan.kz	2022-08-04	2022-08-04	Server	Apache
	kazhackstan.kz	2017-09-26	2018-06-12	Analytics Service	Google Tag Manager
	www.kazhackstan.kz	2017-10-20	2017-10-20	Tracking Pixel	Google Analytics
	www.kazhackstan.kz	2017-10-20	2017-10-20	Javascript Library	jQuery

DOMAIN
phdays.com Add to Pulse

Pulses 0 Passive DNS 58 URLs 39 Files 0

Analysis Overview Loading Analysis

WHOIS Registrar: Regional Network Information Center, JSC dba RU-CENTER, Creation Date: Mar 9, 2011 External Resources

Related Pulses None

Related Tags None

Analysis

Related Pulses

Comments (0)

Whois

Show 10 entries

RECORD	VALUE
Emails	tld-abuse@nic.ru
Name	Positive Technologies, CJSC
Name Servers	NS1.P23.DYNECT.NET
Org	
Address	

SecurityTrails
A Recorded Future® Company

DOMAIN

DNS Records

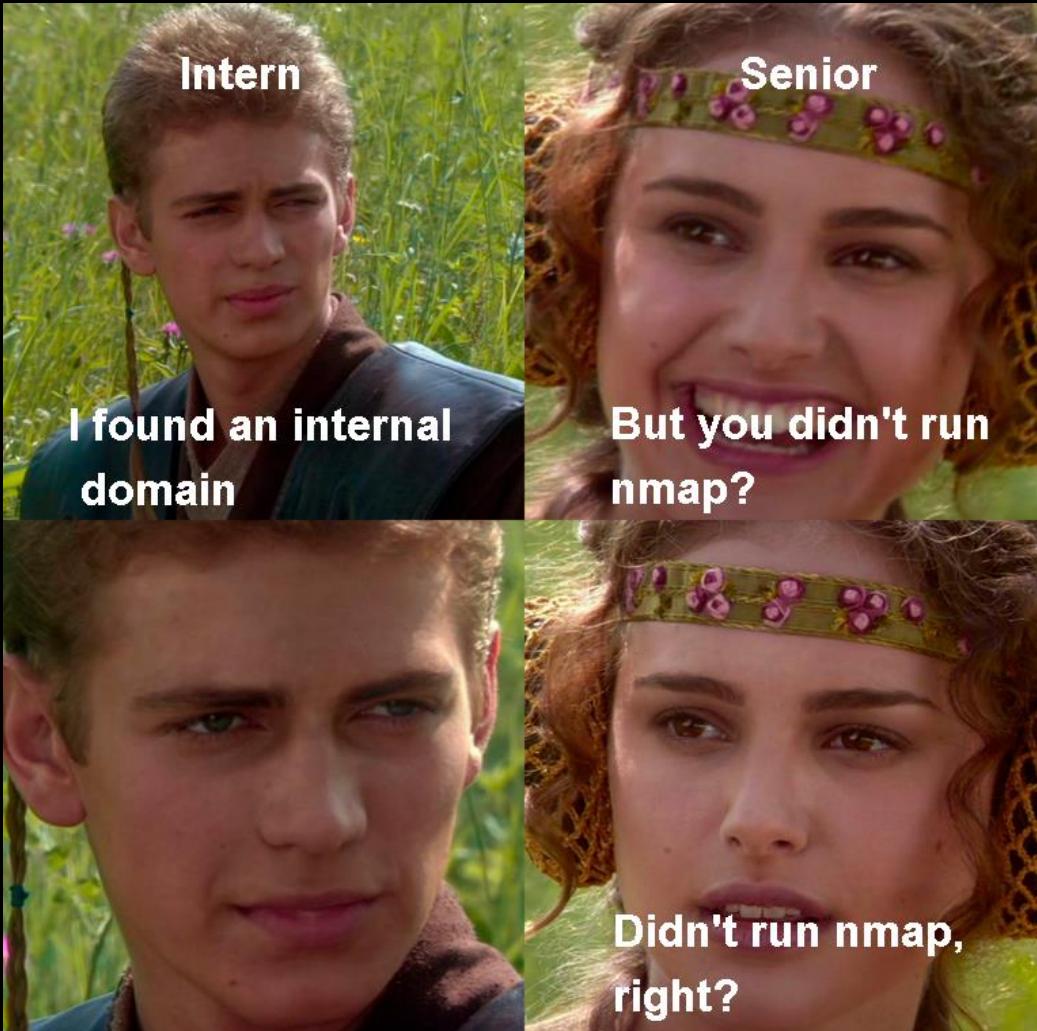
Historical Data

Hacktricks

```
# curl -I -k -X POST -H 'Authorization: NTLM TlRMTVNTUAABAAAAB4IlogAAAAAAAAAAAAAKANC6AAAADw==' -H 'Content-L  
HTTP/1.1 401 Unauthorized  
Server: Microsoft-IIS/10.0  
request-id: 0287a547-54f3-46ed-bd7e-68862174516d  
WWW-Authenticate: NTLM TlRMTVNTUAACAAAADgAOADgAAAAFgomizzeoaM1ekfIAAAAAAAAAAPwA/ABGAAAACgBjRQAAA9SAEEATQBCAEwARQBSAAI  
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 ~]# ./changeIndex.py  
[root@kali ~]# curl -I -k -X POST -H 'Authorization: NTLM TlRMTVNTUAACAAAADgAOADgAAAAFgomizzeoaM1ekfIAAAAAAAAAAPwA/ABGAAAACgBjRQAAA9SAEEATQBCAEwARQBSAAI  
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): +ÿ+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"]  
  }  
}));
```

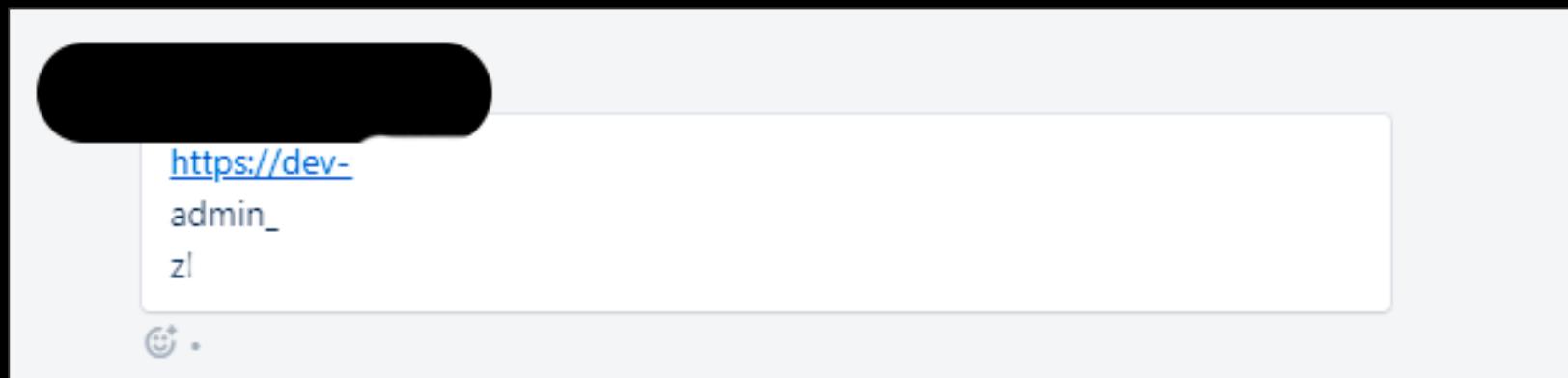
NO NMAP!



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:

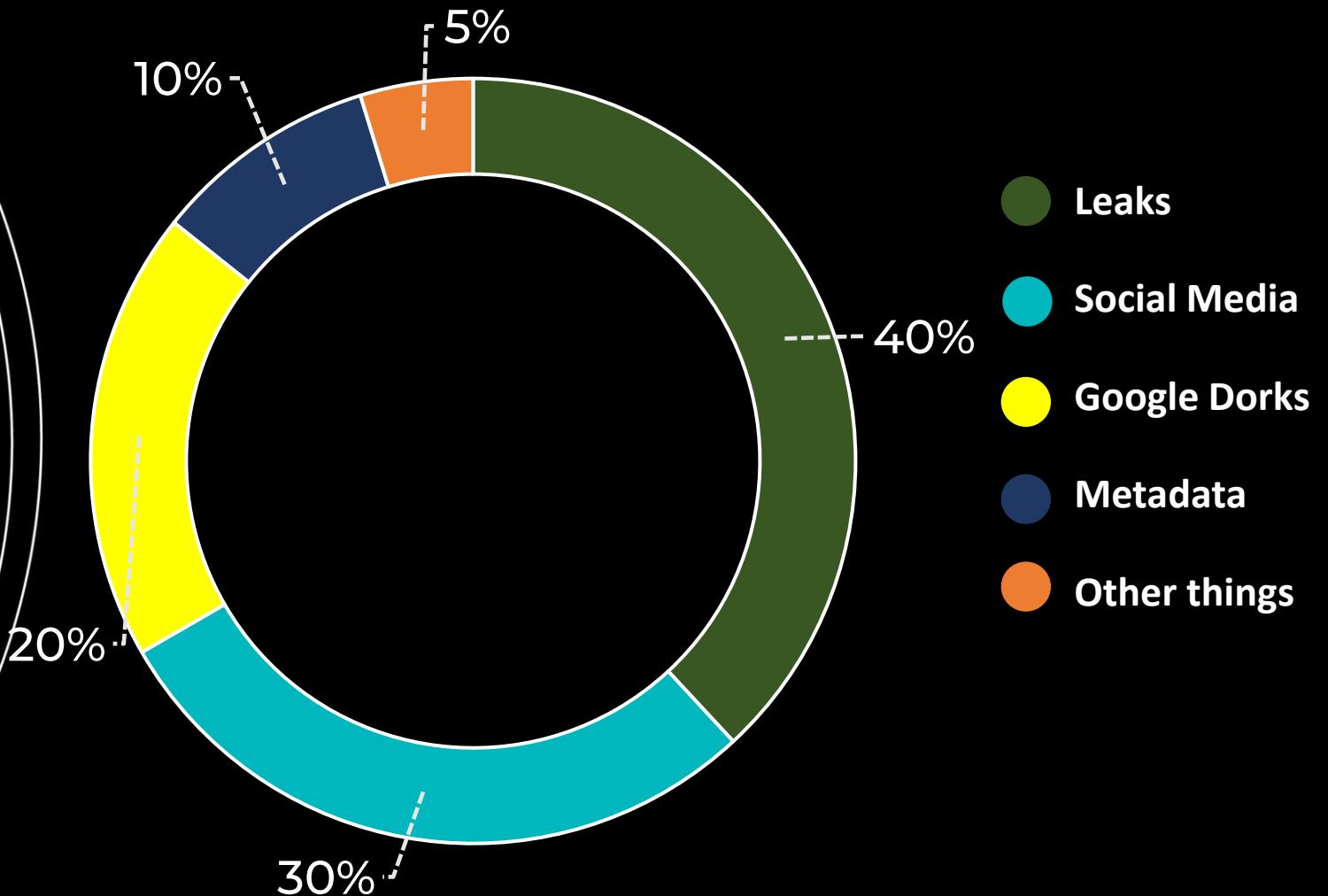


Looking for

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



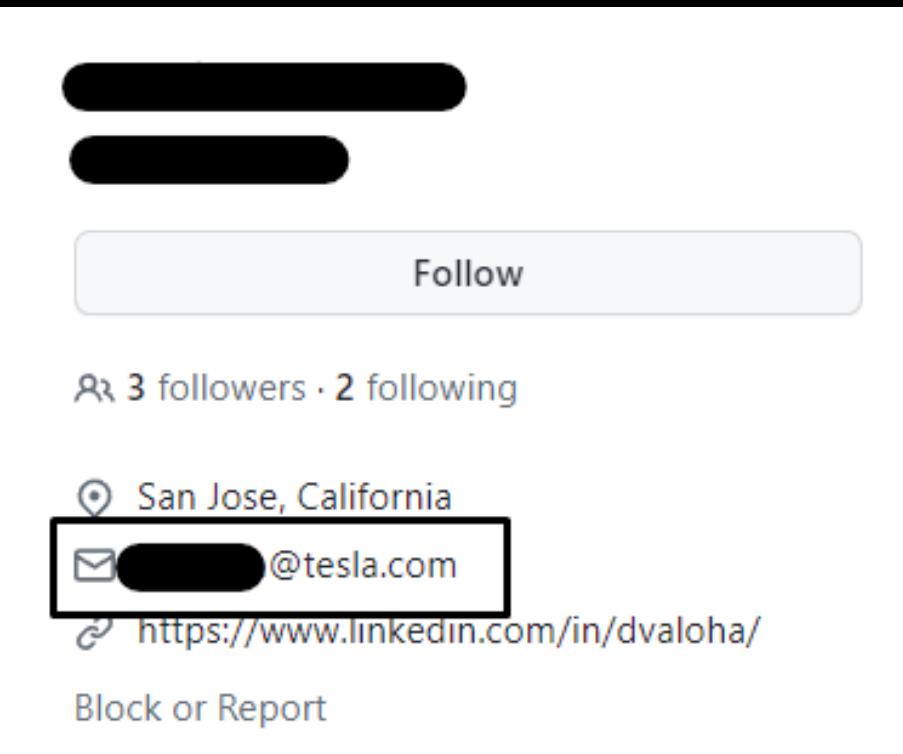
Main sources of info



Leaks

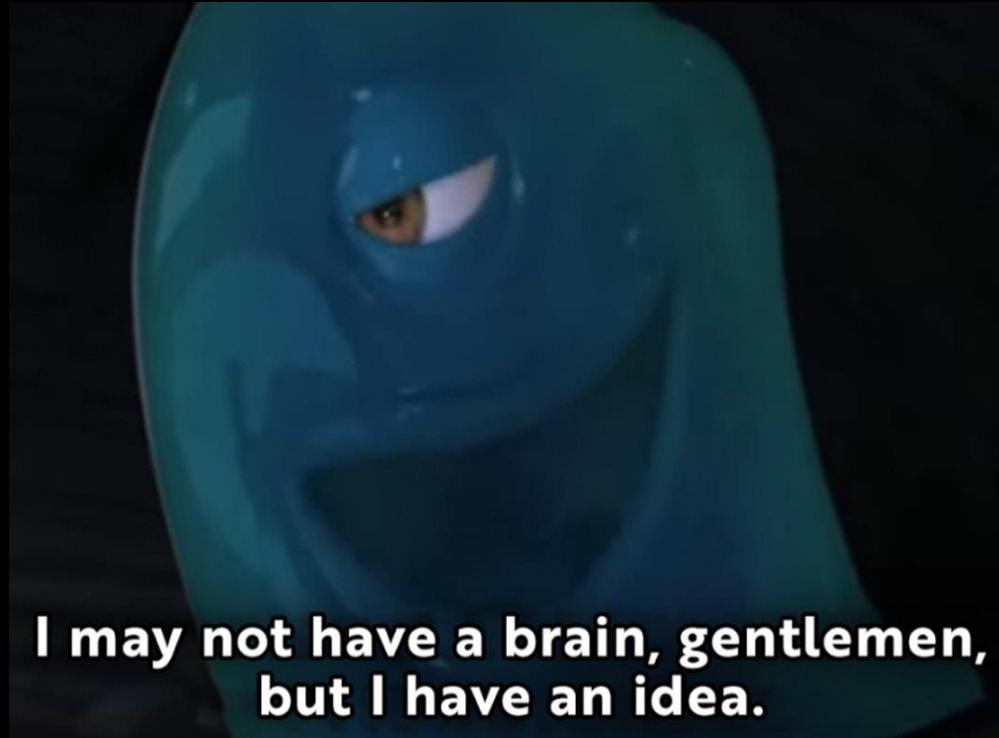
- Rostelecom
- Яндекс Еда
- 2 Berega
- Delivery Club
- Умный дом
- Яндекс Практикум
- Oriflame
- Туту.ру
- Tele2
- Twitter
- Facebook
- Онлайн Трейд
- CDEK
- Wildberries
- Pikabu
- Avito
- Гемотест
- CDEK v2.0
- Почта России
- Kari
- DNS
- ВкусВилл

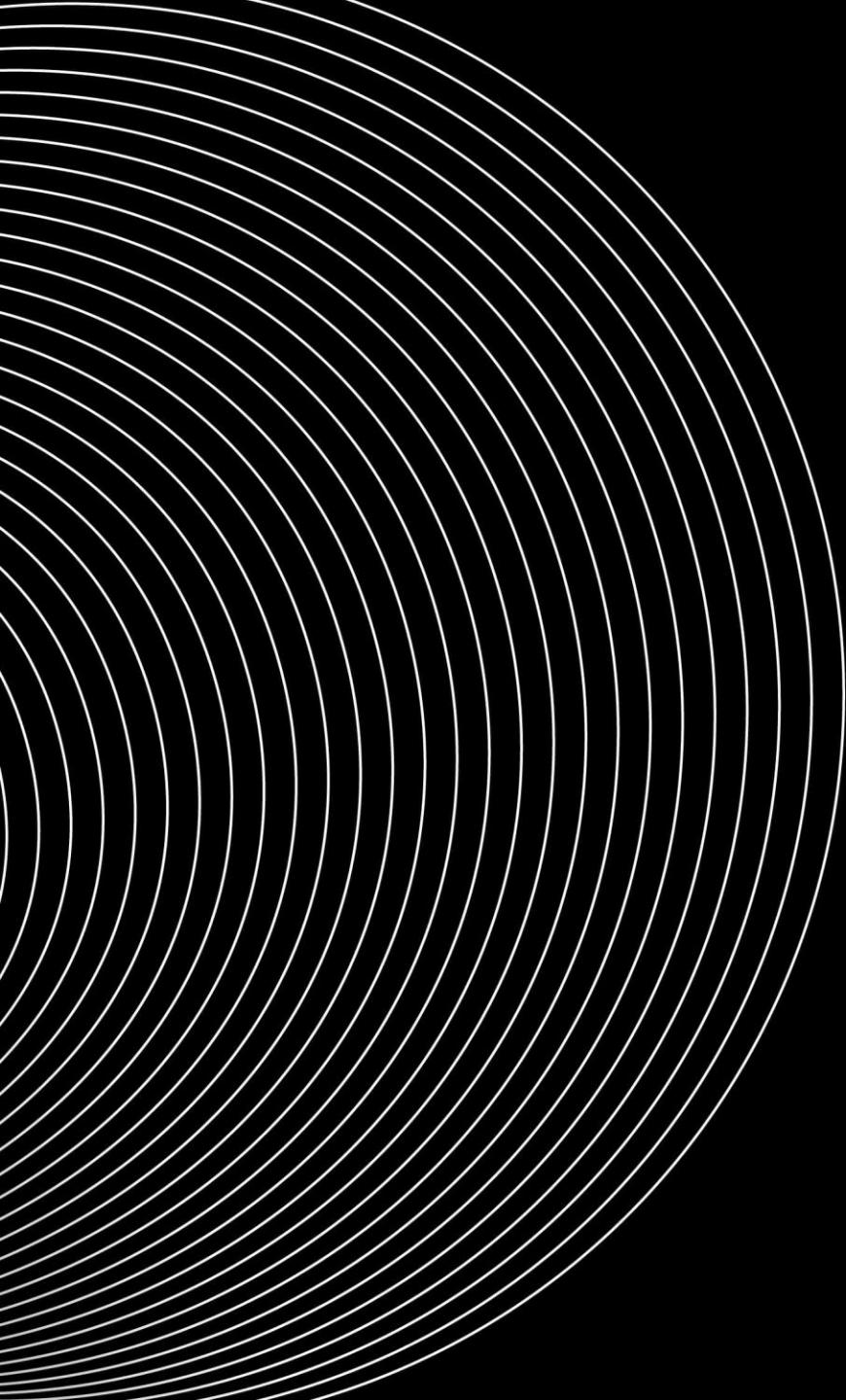
Public(?) Leaks



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

Company's social networks

День вирусной аналитик с экспертами Positive Techno в НИЯУ МИФИ

4 марта, 2023



Ксения Рысаева
Руководитель направления мониторинга
Innostage



Антон Калинин
Руководитель группы экспертизного и наставничества Innostage



Алексей Романов
пресейл-инженер облачных сервисов
кибербезопасности
Innostage



Ксения



Алексей



Вебинар

18 мая,
11:00–12:30

BI.ZONE Secu
 поиск и блок
 атак, реализ
 через DNS

Алексей Романов
пресейл-инженер
облачных сервисов
кибербезопаснос

Антон Калинин

Руководитель группы экспертизного
и наставничества Innostage

BI.ZONE

demis group

Вебинар

6 июля,
13:00–14:30

Как комплексно
работать
с репутацией
в интернете

Дмитрий Кирюшкин
Руководитель отдела
анализа репутации, BI.ZONE

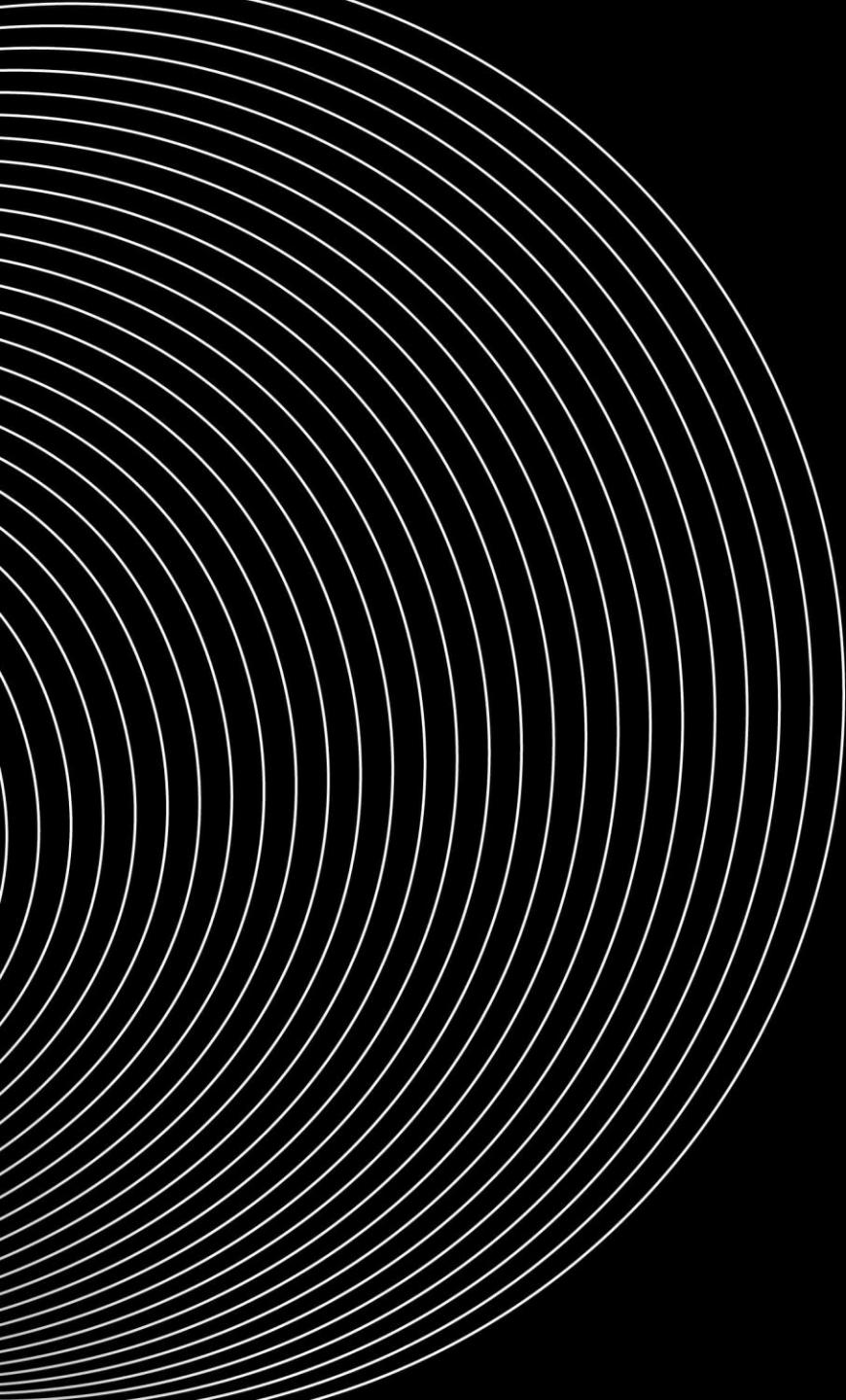
Василий Дроздов
Руководитель
направления ORM,
Demis Group

Вебинар

Особенности
атак на Linux-
инфраструктуры

Михаил Прохоренко
Руководитель управления
по борьбе с киберугрозами

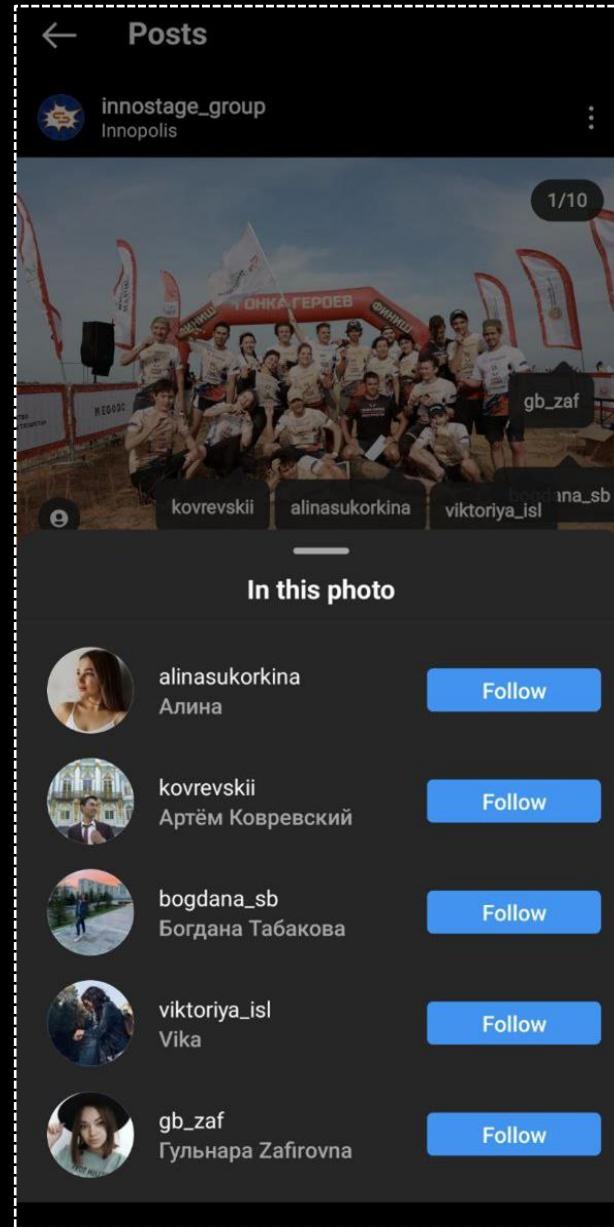
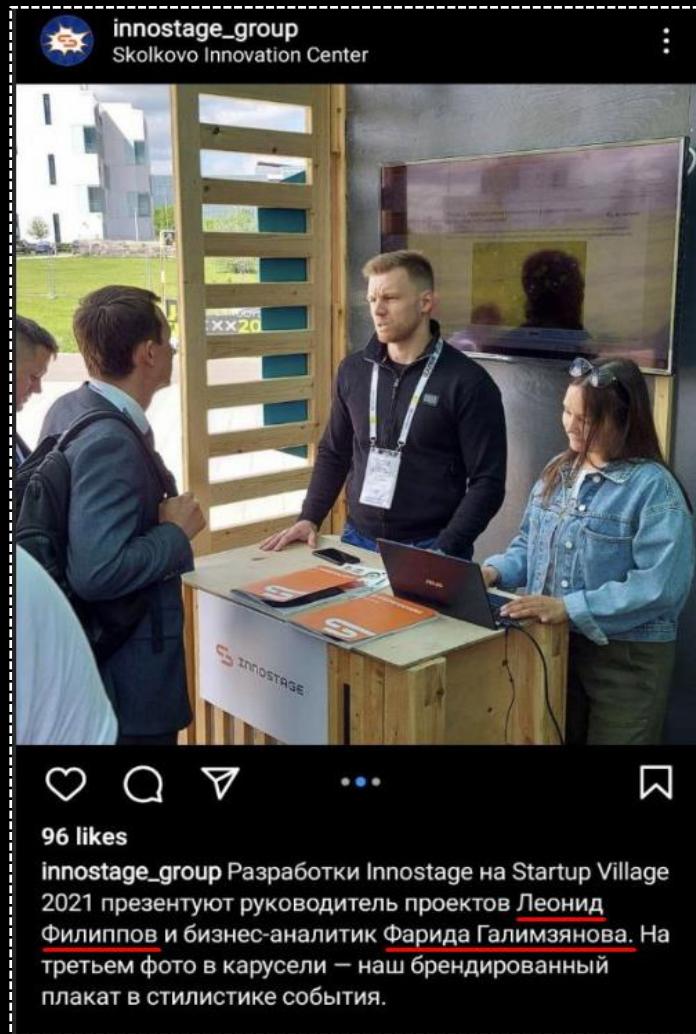
KAZHAKSTAN TURAN-2023



Employee's social networks

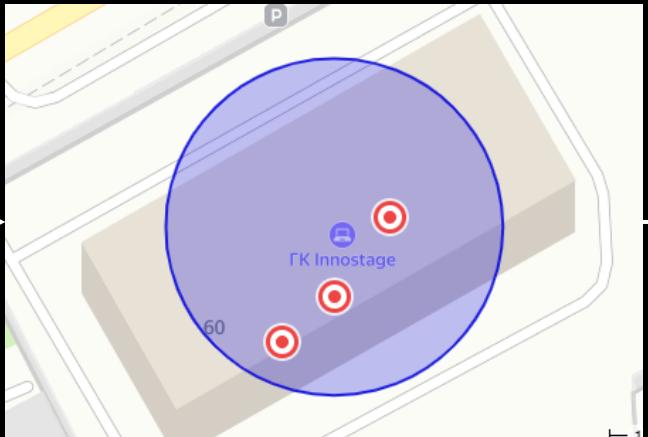
- Workplace
- #Hashtags / Photo Mentions
- Geolocation on photo
- Geolocation spoofing

#Hashtags / Photo Mentions



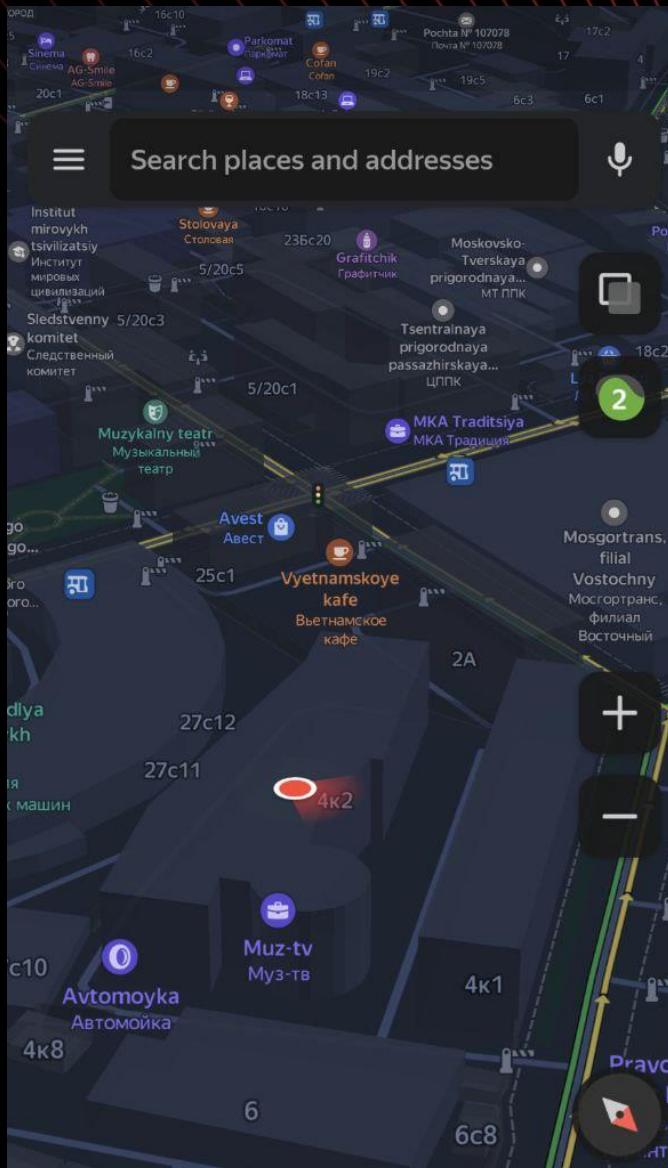
Employee's social networks

✉ 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



Job aggregators

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

Positive Technologies
Company

Add to list

City: Moscow Industry: Computer & Network Security
Website: www.ptsecurity.com Size: 501-1000
Social: in

Less

Prospects 243 All Domain Emails 455 Generic Contacts 11 Technologies 29

Filter by position
e.g. Sales specialist Search Refresh

PROSPECTS	EMAILS	POSITION	LISTS
<input type="checkbox"/> Paula Dunne CONTOS DUNNE COMMUNICATIONS	Click Add to list to initiate email search	Agency of Record	+ Add to list
<input type="checkbox"/> Pavel Novoseltsev	Click Add to list to initiate email search	Lead Web Developer	+ Add to list
<input type="checkbox"/> Andrew B.	Click Add to list to initiate email search	Chief Technology Officer	+ Add to list
<input type="checkbox"/> Maxim Pustovoy	Click Add to list to initiate email search	Executive Director, Deputy CEO, Chief Operating Officer COO	+ Add to list
<input type="checkbox"/> Alexandra Murzina	Click Add to list to initiate email search	Machine learning engineer	+ Add to list
<input type="checkbox"/> Tatyana Rodionova	Click Add to list to initiate email search	Director of Products Services	+ Add to list

Контактные лица

 Polina Voloshina IT рекрутер
 Анна Кудрявцева Менеджер по внутренним ком...
 Полина Перова Researcher
 София Бернацкая Sourcer
 Ирина Завьялова
 Наталья Косых
 Мария Вальд IT Recruiter
 Анастасия Грунева IT HR
 German Kholmov
 Александра Кузьминова менеджер по подбору персонала
 Дарья Лисица

Positions in company

Реестр деклараций

ИИН юридического лица (индивидуального предпринимателя), подавшего декларацию

9701036178

Регион

ГИТ в г. Москве

Поиск

Профессия, должность, специальность работника (работников), занятых на данном (данных) рабочем месте (рабочих местах)

8,459,460 Директор по противодействию мошенничеству; номер рабочего места 1, Директор; номер рабочего места 2, Исполнительный директор; номер рабочего места 3, Финансовый директор; номер рабочего места 4, Аудитор; номер рабочего места 5, Аудитор



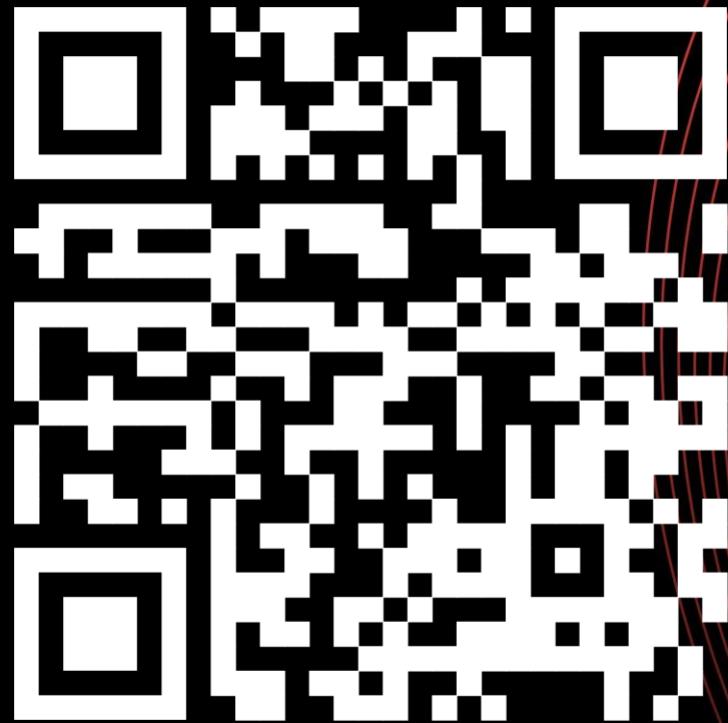
GitHub Dorks

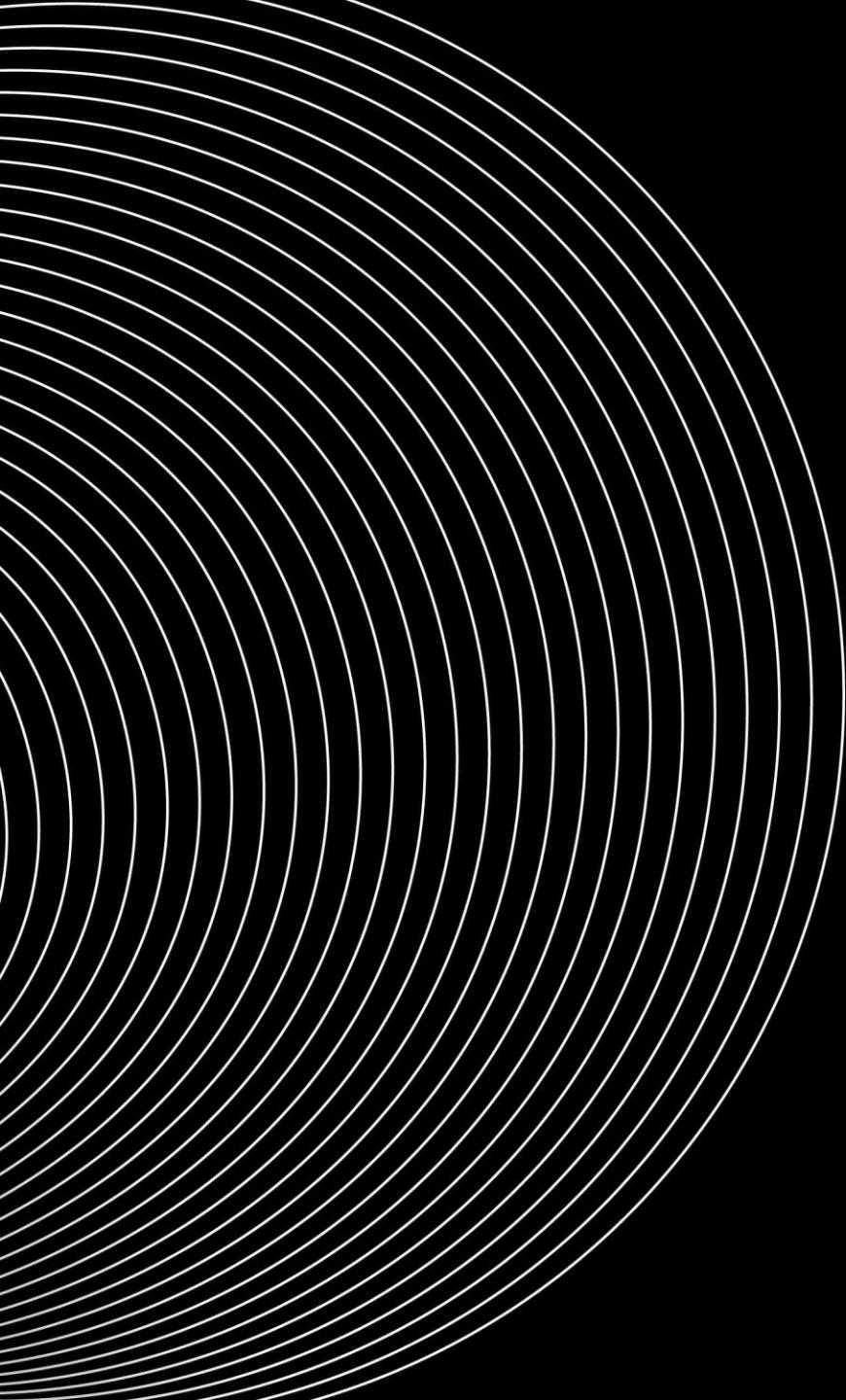
- Looking for additional emails
- <company> login/user/pass/password
- <company> ldap
- <company> wiki
- <company> connectionstrings



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.

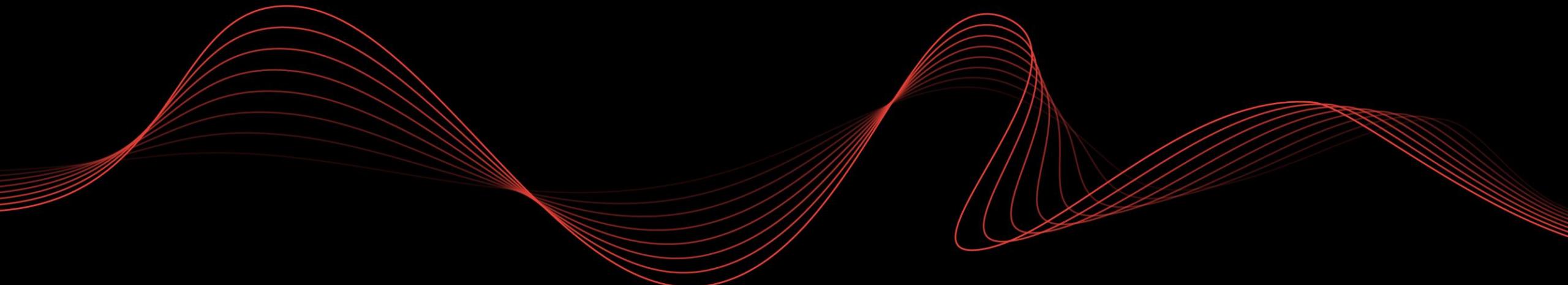


Комитет по
информационной
безопасности
МЦРИАП РК



Служба
государственной
охраны

MHS
thank you for your attention



Questions?

