

NO
FF
ONE
2022

 INNOSTAGE

Osinter's Notes

Goncharov Alexander

Engineer / Penetration Tester / Social Engineer

August, 2022



Whoami

Goncharov Alexander

- Engineer / Penetration Tester / Social Engineer
- Innostage
- PHDays speaker

Plan

- Who will benefit from this?
- Gathering information from the main site
- Leaks
- Metadata analysis
- Social media OSINT
- Passive Infrastructure Analysis
- Google Dorks
- Proof Of Concept

Who will benefit from this?

- Pentest
- RedTeam
- Social Engineer

Gathering information from the main site



- About company
- Contacts
- Career

✉ info@innostage-group.ru

info@offzone.moscow



Contacts

info@bi.zone

Gathering information from the main site – A real-life example



Result:

If you have any questions about participation, write and call!



Ziganshin Rinat

Rinat.Ziganshin@innostage-group.ru



Olga Yasoveeva

Olga.Yasoveeva@innostage-group.ru

Email: info@tel-int.ru

✉ info@innostage-group.ru

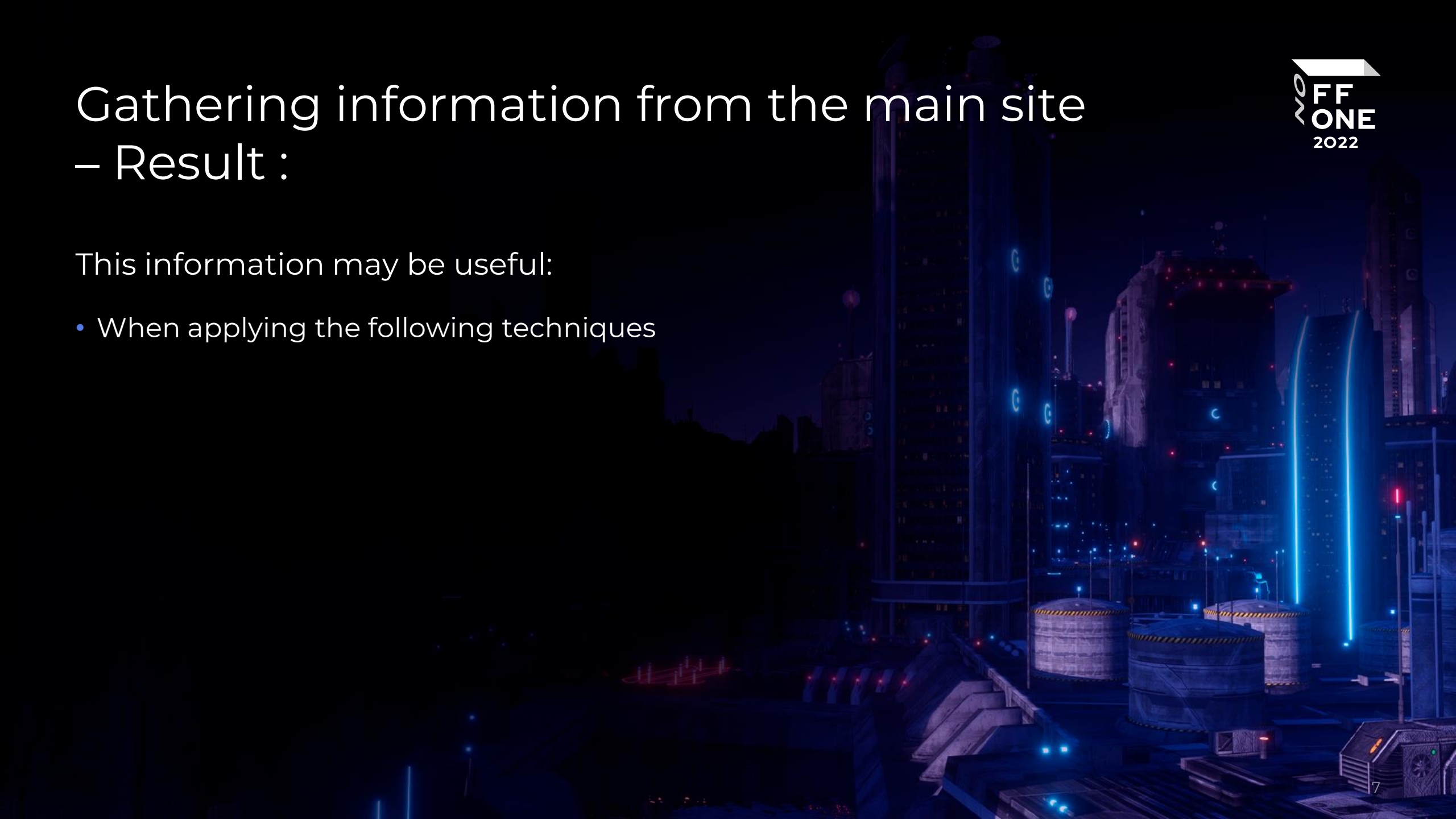
[@tel-int.ru](https://www.tel-int.ru)

Gathering information from the main site

– Result :

This information may be useful:

- When applying the following techniques



Leaks in 2022



Rostelecom

Yandex.Eda

Yandex.Eda.Couriers

2 Berega

Delivery Club

Umnij Dom

Yandex.Praktikum

Oriflame

Tele2

CDEK

Wildberries

Pikabu

Avito

Gemotest

CDEK v2.0

Russian Post

Kari

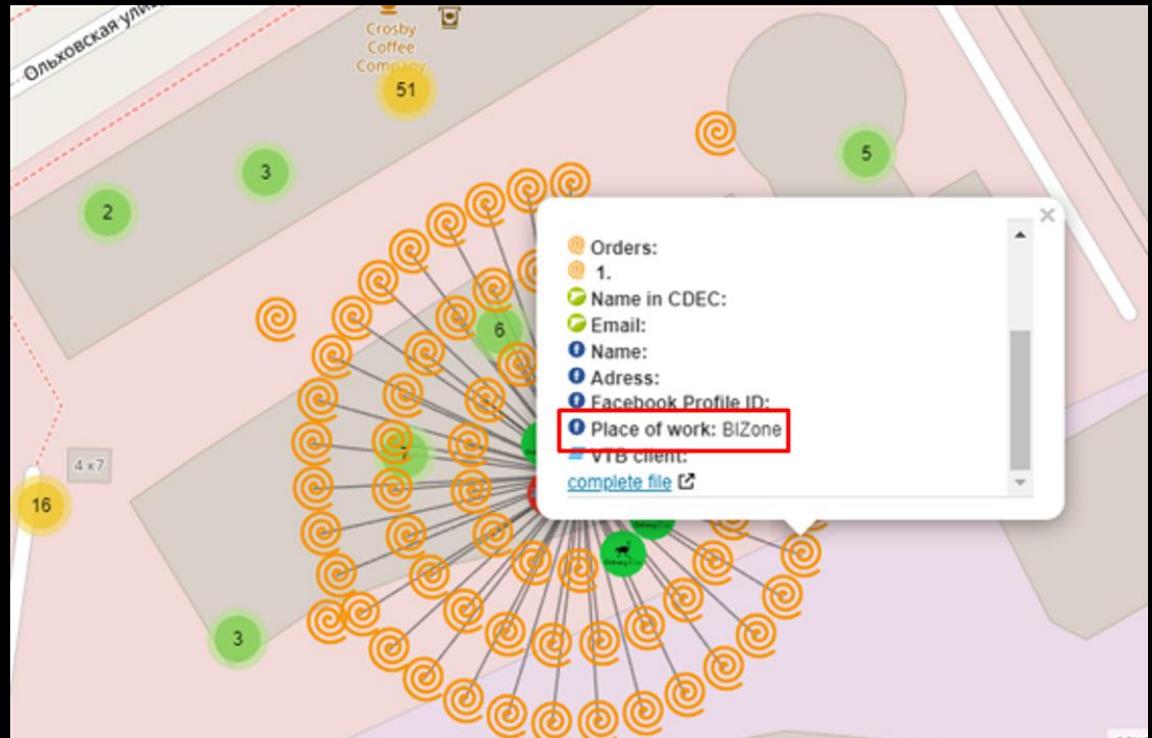
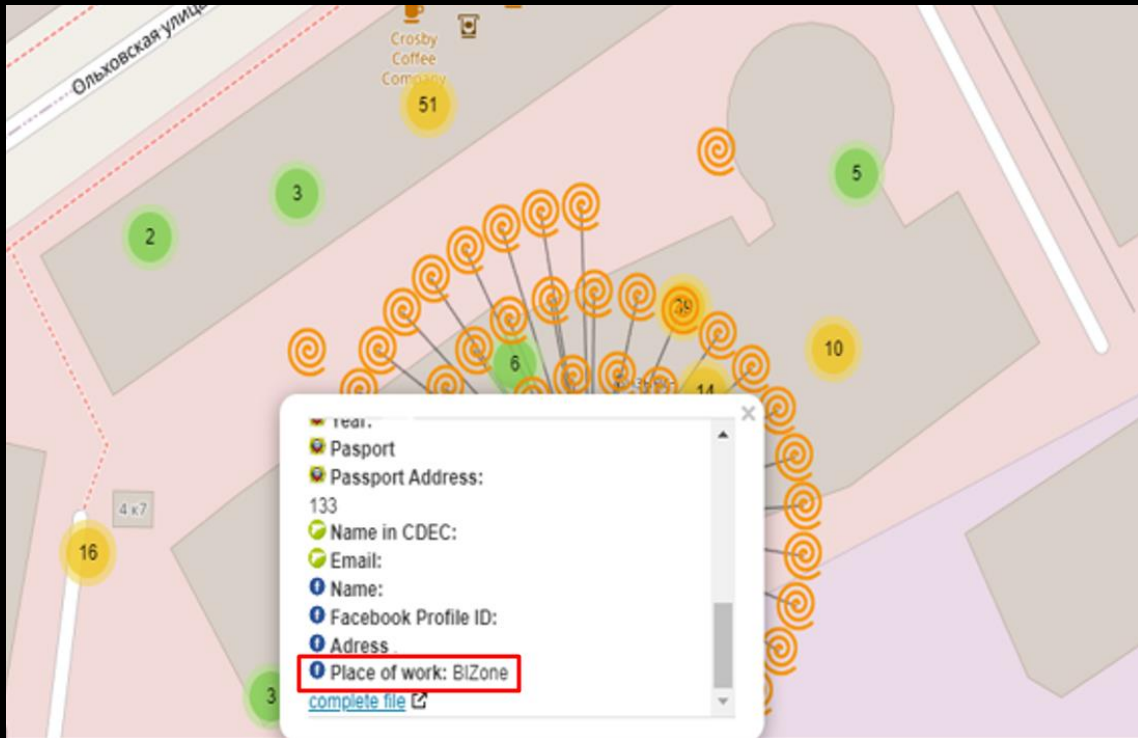


While writing this article,
I got tired of updating
the table

Leaks – Geolocation



Leaks – Geolocation – A real-life example



Leaks – Result

This information may be useful:

- In the internal/external pentest:
 - User/Mail verification
 - Bruteforce
 - Password Spray
 - During Active Directory pentest
- In phishing campaigns
- For the application of social engineering

Metadata

- Names of employees
- HostName
- Network share
- Software version
- Printer information



Metadata – Results

This information may be useful:

- In the internal/external pentest:
 - User / Mail verification
 - Bruteforce / Password Spray
 - During Active Directory pentest
- In phishing campaigns
- For the application of social engineering

Social media OSINT

- Search by place of work in VKontakte / Facebook / ok
- By geolocation in photos
- By hashtags
- Swapping geolocation
- Mentioning friends in photos on Instagram, VK
- The company's social media

Note:

To maximize the effectiveness of these methods, you need to know the format of the email

Social media OSINT – Search by place of work

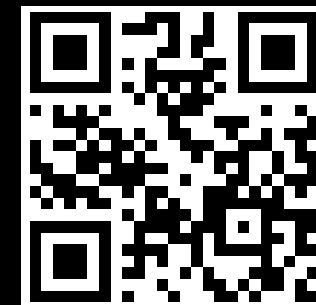
- VERY effective for compiling a list of users
- Easy to parsing

The screenshot displays a social media search interface. The main area shows a list of search results for users from Moscow, Russia, with 'BI.ZONE' highlighted in red in their work location. The search filters on the right include 'My friends', 'Friend requests', 'Find friends', 'Search parameters', 'Order' (By relevance), 'Region' (Select a country), 'School', 'College or university', 'Age' (From - To), 'Gender' (Female, Male, Any), 'Relationship' (Select a status), 'With photo' (checked), 'Online now', 'Personal views', 'Company' (Bi.Zone highlighted in red), 'Position', 'Military service', and 'Extra options'. An 'Invite friends' button is visible at the bottom right.

Name	Location	Work Location	Action
Tatyana Deryusheva	Moscow, Russia	BI.ZONE	Add friend
Pavel Bannikov	Moscow, Russia	BI.ZONE	Add friend
SAVVA MOROZOV	Kaspersky		Add friend
Vasiliy Govich	Moscow, Russia	BI.ZONE Кибербезопасность Сбербанка	Add friend
Elizaveta Katyushina	Moscow, Russia	BI.ZONE	Add friend
Vladislav Merkulov	Moscow, Russia	BI.ZONE	Add friend
Roman Andreev	Moscow, Russia		Add friend
Nadezhda Martyshko	Taganrog, Russia	BI.ZONE	Add friend
Artur Stepanov	Moscow, Russia	BI.ZONE	Add friend

Social media OSINT – By geolocation in photos

- Useful for social engineering
- May be effective for compiling a list of users



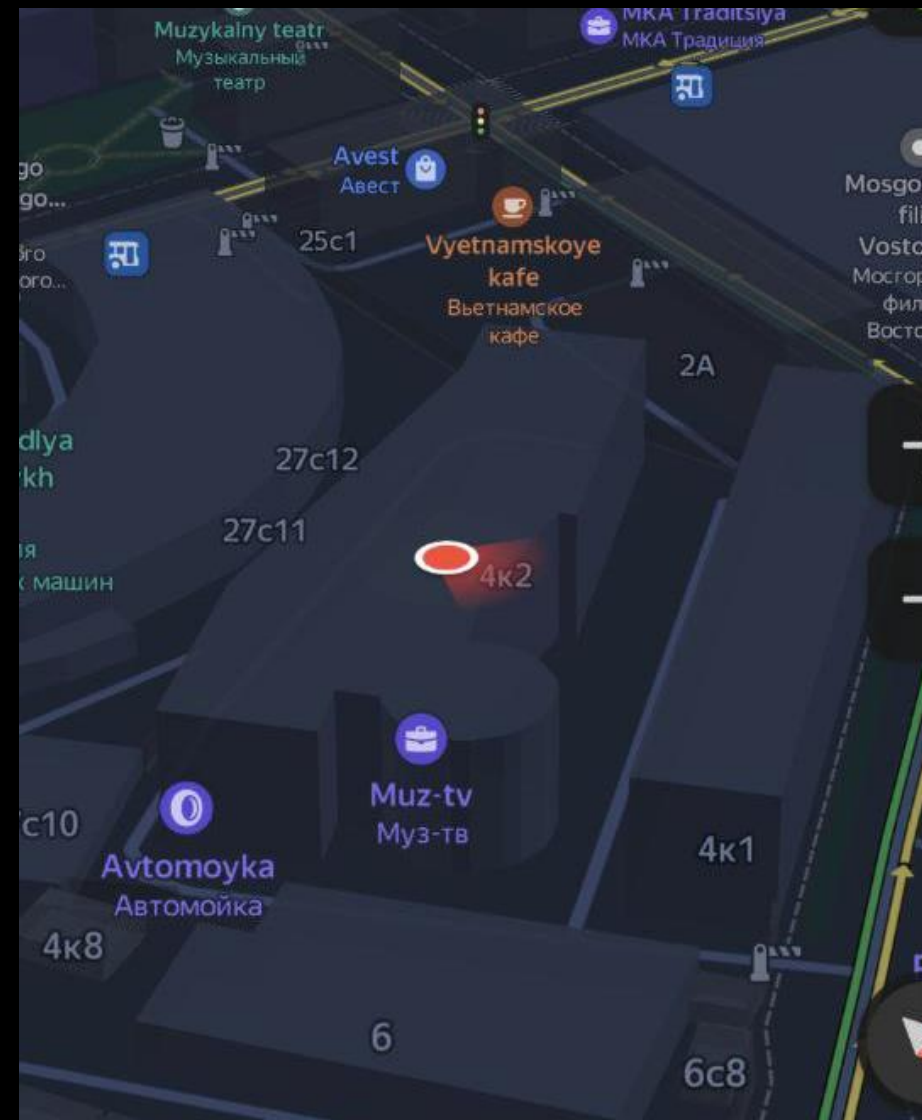
✉ info@innostage-group.ru

📍 Kazan, Podluzhnaya str. 60,

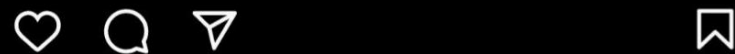
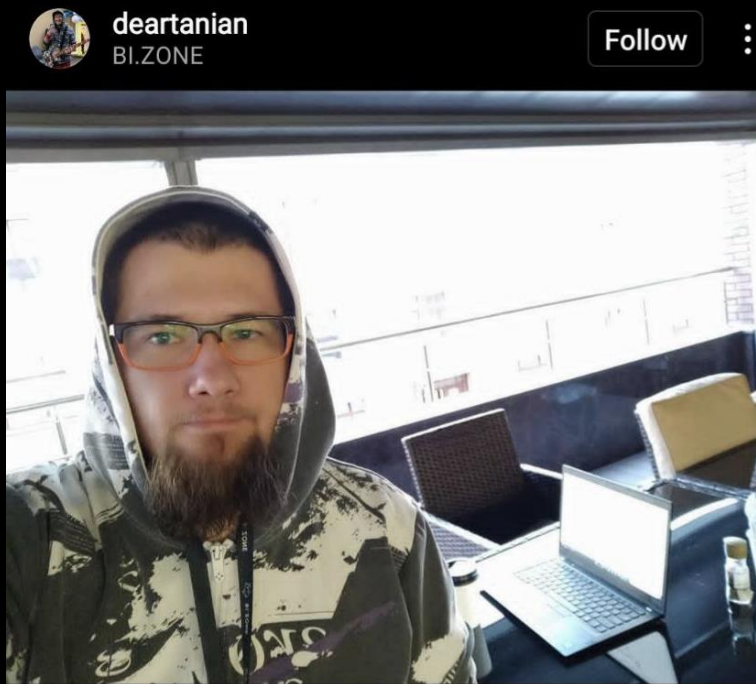


Social media OSINT – Swapping geolocation

- Detects People Nearby
- Useful for social engineering
- Works in Telegram and VK



Social media OSINT – By hashtags / Mentioning friends



63 likes
deartanian Good morning, йопта!

#morning #work #job #bizone #mood #beard #live #smile
#notebook #coffee #инстаграмопозер



28 likes
a.trofimov1991 #бегущиесердца #бизон #bizone
May 28 · See translation

← Posts

innostage_group
Innopolis

1/10

gb_zaf

kovrevskii alinasukorkina viktoriya_isl ina_sb

In this photo

- alinasukorkina Алина Follow
- kovrevskii Артём Ковревский Follow
- bogdana_sb Богдана Табакова Follow
- viktoriya_isl Vika Follow
- gb_zaf Гульнара Zafirovna Follow

Social media OSINT – The company's social media

- Useful for social engineering
- May be effective for compiling a list of users



96 likes

innostage_group Разработки Innostage на Startup Village 2021 презентуют руководитель проектов Леонид Филиппов и бизнес-аналитик Фарида Галимзянова. На третьем фото в карусели – наш брендированный плакат в стилистике события.

Social media OSINT – Results

This information may be useful:

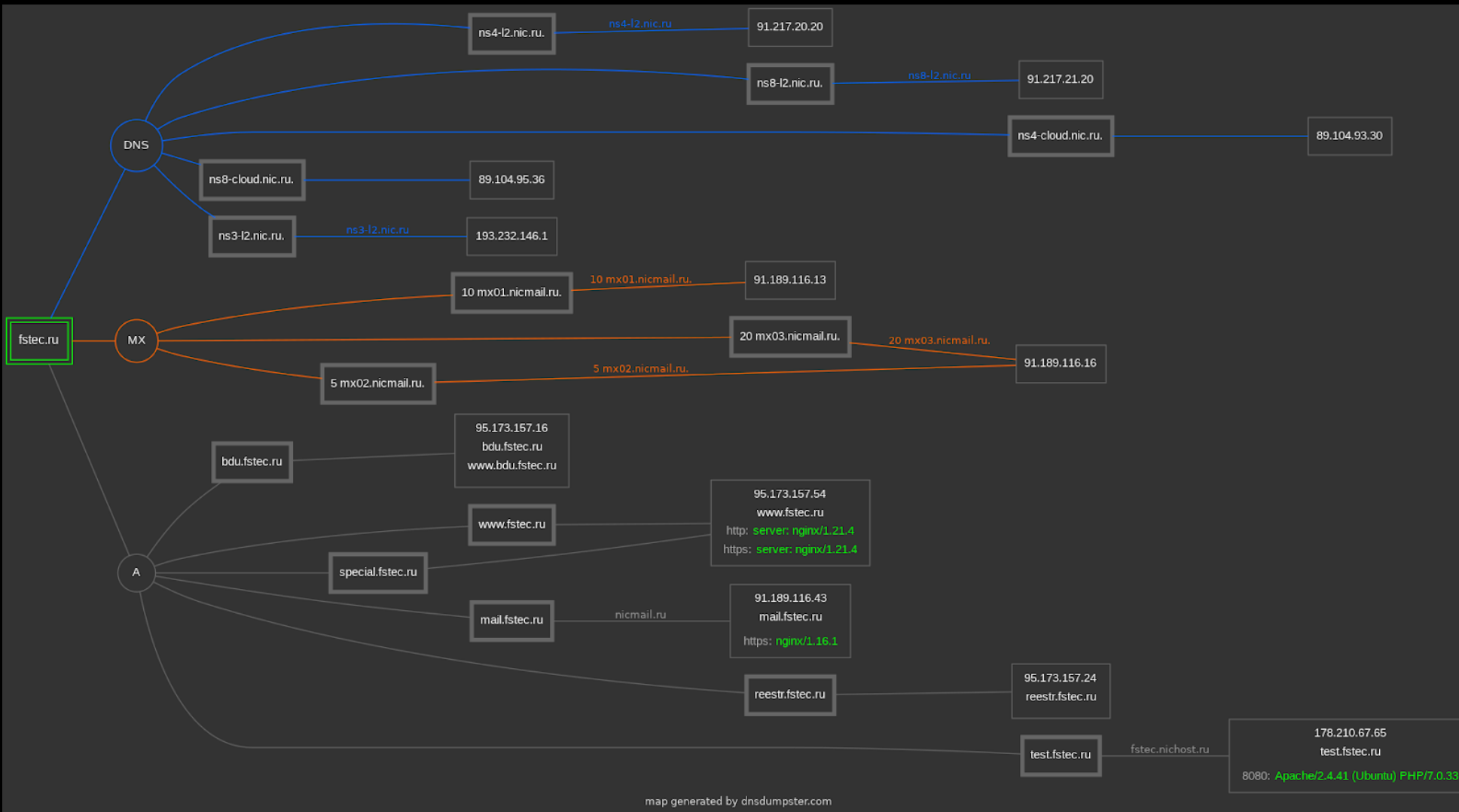
- In the internal/external pentest:
 - User / Mail verification
 - Bruteforce / Password Spray
 - During Active Directory pentest
- In phishing campaigns
- For the application of social engineering

Passive Infrastructure Analysis

- Searching for subdomains
- Automating work with Shodan
- Automating info collection



Passive Infrastructure Analysis – Subdomains



Passive Infrastructure – Smap

Features

- Scans 200 hosts per second
- Makes no contact to the targets
- Doesn't require any account/api key
- Vulnerability detection
- Supports all nmap's output formats
- Service and version fingerprinting



Passive Infrastructure – Smap – Example



```
smap -sV 178.237.██████
```

```
Starting Nmap 9.99 ( https://nmap.org ) at 2022-03-19 15:50 IST  
Nmap scan report for ns233.████████████████████.com (178.237.██████)  
Host is up.
```

PORT	STATE	SERVICE	VERSION
80/tcp	open	http	Apache httpd
25/tcp	open	smtp	Sendmail 8.14.4/8.13.8
22/tcp	open	ssh?	
53/tcp	open	domain?	
443/tcp	open	https?	
995/tcp	open	pop3s?	

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

Passive Infrastructure – Shodanalyzer



Features

- Open ports
- Makes no contact to the targets
- Required account/api key
- Vulnerability detection
- Service and version fingerprinting
- Technologies
- Honeyscore



Passive Infrastructure – Shodanalyzer – Example

```
[*] Starting scan for ip address [REDACTED]...  
  
[*] General Information  
Cloud Provider: Azure  
Cloud Region: southcentralus  
Cloud Service: AzureCloud  
Country: United States  
City: San Antonio  
Organization: Microsoft Corporation  
ISP: Microsoft Corporation  
ASN: AS8075  
  
[*] Open Ports for 13.84.220.249  
80 tcp  
  
[*] Uncommon open ports  
[-] No uncommon opened ports found  
  
[*] Web Technologies  
Bootstrap  
jQuery  
Microsoft ASP.NET  
Modernizr  
  
[*] Services  
80 tcp  
Microsoft IIS httpd8.5  
  
[*] Vulnerabilities  
CVE-2014-4078  
  
The IP Security feature in Microsoft Internet Information Services (IIS) 8.0 and 8.5 does not properly process wildcard allow and deny rules for domains within the "IP Address and Domain Restrictions" list, which makes it easier for remote attackers to bypass an intended rule set via an HTTP request, aka "IIS Security Feature Bypass Vulnerability."  
  
[*] Honeypot  
[+] 13.84.220.249 is not a honeypot. It has a 0.0/1 honeyscore
```

- Passive Infrastructure Analysis - Automating info collection

- Harvester
- SpiderFoot
- etc...



• Passive Infrastructure Analysis - Automating info collection

- Email
- Sub-domain
- Ip
- Url
- Phone number
- Username
- Network subnet (CIDR)
- Hostname
- ASN
- etc...

Passive Infrastructure Analysis – Results

This information may be useful:

- During the active stage of penetration testing
- For understanding external infrastructure



Google Dorks

Features

- Files Containing Usernames
- Sensitive Directories
- Web Server Detection
- Vulnerable Servers
- Error Messages
- Files Containing Juicy Info
- Files Containing Passwords
- Network or Vulnerability Data
- Pages Containing Login Portals
- Various Online Devices
- Vulnerabilities

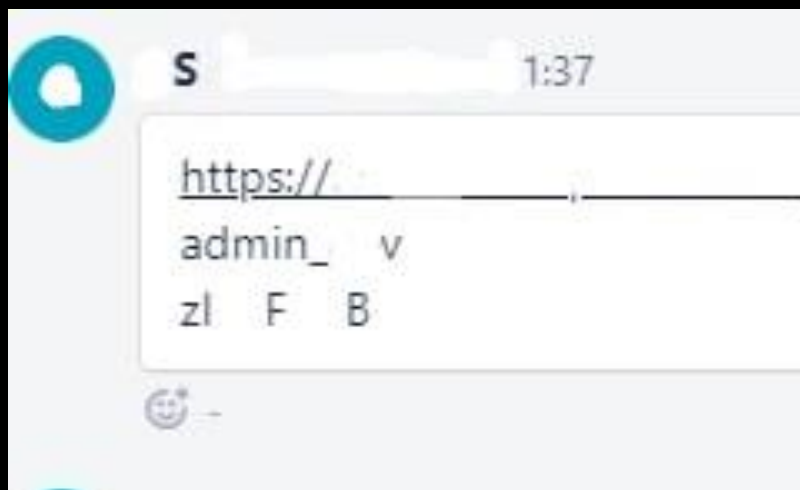



Google Dorks – Result

This information may be useful:

- To search for sensitive information
- To search projects on github / stackoverflow / pastebin / trello
- To search for internal/interesting files

Proof of Concept



// 10000 / TCP 

MiniServ 1.890

```
HTTP/1.0 200 Document follows
Date: Sun, 7 Aug 2022 13:06:55 GMT
Server: MiniServ/1.890
```

[https://github.com > foxsin34](https://github.com/foxsin34) ▾ [Перевести эту страницу](#)

[foxsin34/WebMin-1.890-Exploit-unauthorized-RCE - GitHub](#)

WebMin-1.890-Exploit-unauthorized-RCE. Script to get rce on Webmin version 1.890. Read this article to get more information ...

[https://www.webmin.com > ex...](https://www.webmin.com/ex...) ▾ [Перевести эту страницу](#)

[Webmin 1.890 Exploit - What Happened?](#)

Webmin version **1.890** was released with a backdoor that could allow anyone with knowledge of it to execute commands as root. Versions 1.900 to 1.920 also ...

[https://www.infosecmatter.com > ...](https://www.infosecmatter.com/...) ▾ [Перевести эту страницу](#)

[Webmin 1.890 - 1.920 Remote Command ... - InfosecMatter](#)

Public **Exploits** — The **Webmin** install hosted on the remote host is affected by a remote command execution **vulnerability**. A remote, unauthenticated attacker ...

[Plugin Overview](#) · [Vulnerability Information](#) · [Public Exploits](#) · [Risk Information](#)

[https://medium.com > webmin...](https://medium.com/webmin...) ▾ [Перевести эту страницу](#)

[WebMin 1.890 Exploit unauthorized RCE\(CVE-2019-15107\)](#)

I was able to get rce on **Webmin** version **1.890**, then i made a simple python3 script to launch attack automatically, i will post it on my github which you can ...

Proof of Concept



Simple user verification

Citrix Gateway

Войдите в систему

Имя польз.

Пароль

✘ Неправильный пароль.

Войти

Запрос пароля

Выслать контрольную строку

Логин

E-mail или

Авторизоваться

Ошибка восстановления пароля!
Профиль пользователя не найден.

Если вы забыли пароль, введите ваш логин или E-Mail, указанный при регистрации. Контрольная строка для смены пароля будет выслана вам по электронной почте.

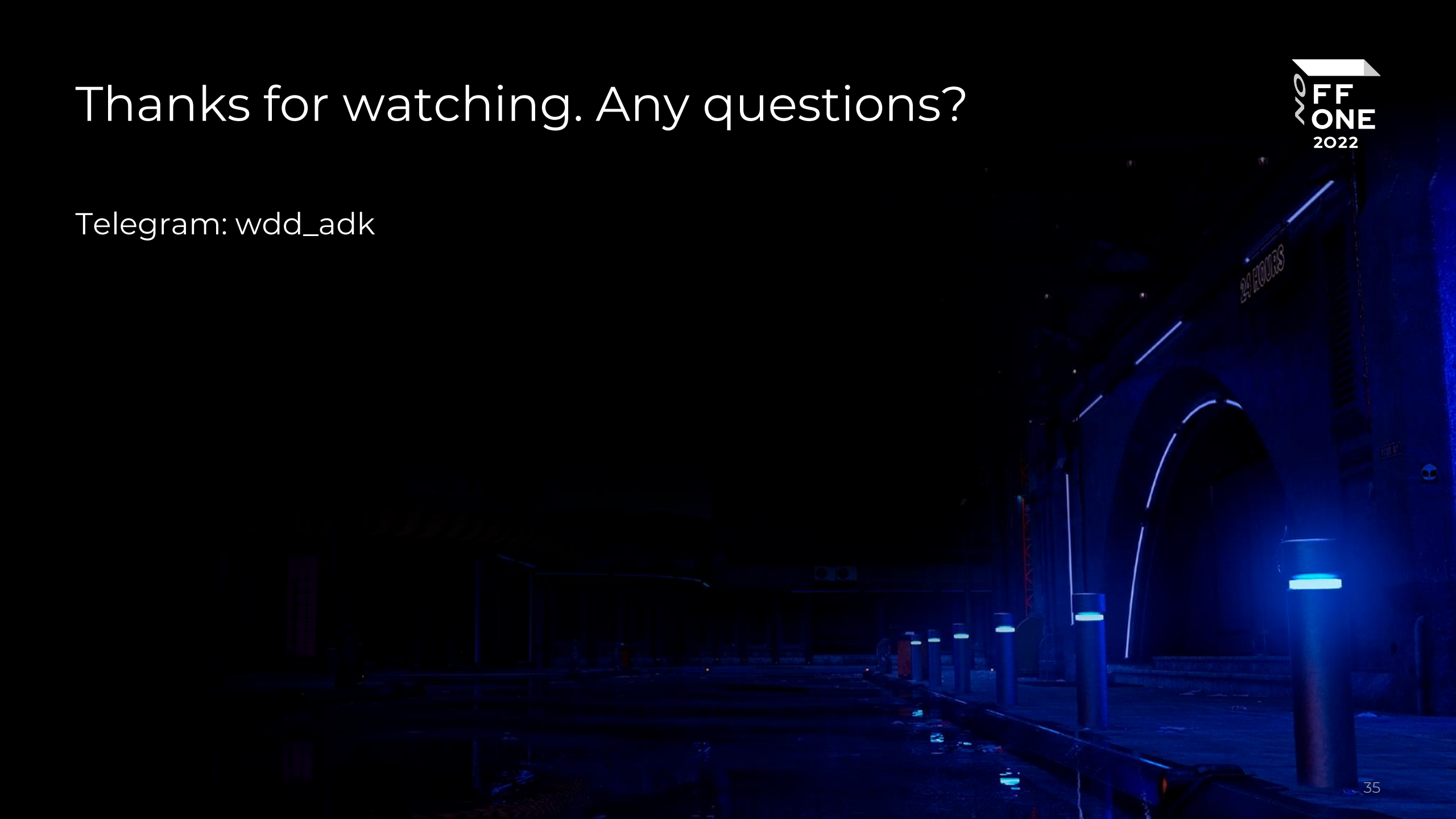
Proof of Concept

OWA timing attack

```
(kali@kali)-[redacted]
└─$ sudo proxychains -q python3 req.py -f user.txt
Username: [redacted] Time 0.6745681762695312
Username: [redacted] 1.6661546230316162
Username: [redacted] Time 0.6792502403259277
Username: [redacted] 1.7752964496612549
Username: [redacted] 1.7363462448120117
Username: [redacted] Time 0.5963304042816162
Username: [redacted] 1.6828045845031738
Username: [redacted] Time 0.5772366523742676
Username: [redacted] 1.7034144401550293
Username: [redacted] Time 0.6259281635284424
Username: [redacted] Time 0.607682466506958
Username: [redacted] 1.7082912921905518
```

Thanks for watching. Any questions?

Telegram: wdd_adk





**NO
OFF
ONE
2022**