DNS4EU

DNS4GOV:
“EUROPEAN PDNS READINESS”

George Buhai | Government Liaison

Project number: 101095329 21-EU-DIG-EU-DNS
Project name: DNS4EU and European DNS Shield.
This project is co-funded by the European Union.

whalebone

Co-funded by
the European Union

DNS4EU

A project to strengthen Europe's digital security with independent DNS protection

Goal of European Commission

Strengthen the digital security and independence of the European Union — by providing EU citizens, institutions, and companies with a secure, privacy-compliant, and powerful recursive DNS.

Challenge

EU governmental institutions and citizens are not well protected, with slow reaction to threats. DNS-level protection was not located in the EU.

Solution

Create independent EU-based DNS protection with real-time reaction to threats — with easy distribution to citizens and institutions.

DNS4EU Consortium

Project Leader

Whalebone, s.r.o.

Consortium members

- CZ.NIC
- Czech Technical University Prague
- Time.lex
- deSEC
- HUN-REN
- ABI Lab Centro di Ricerca e Innovazione per la Banca
- Naukowa i Akademicka Sieć Komputerowa
- Directoratul Național de Securitate Cibernetică

Associated partners

- Ministry of Electronic Governance
- CESNET
- F-Secure
- Centro Nacional de Cibersegurança

DNS4EU Pillars

Project name: DNS4EU and European DNS Shield.
Project number: 101095329 21-EU-DIG-EU-DNS.
This project is co-funded by the European Union.

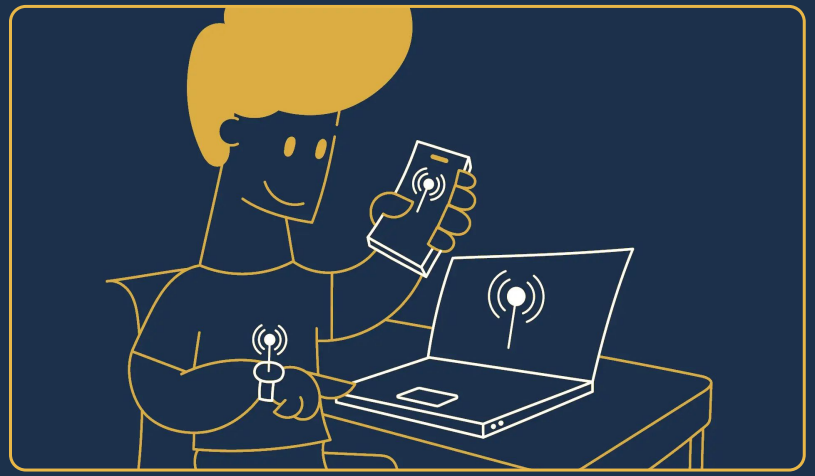
Governments and public institutions

Telco operators and ISPs

Threat Intelligence exchange

Public resolver for end-users

DNS ∩ Cybersecurity



~2B

connected devices

~448M unique users (+95% internet pen)
5.6% of world pop., 12% of WW devices

>90%

of attacks rely on DNS

DNS4GOV project

Co-funded by
the European Union

Main distribution channels

Already protecting millions of people in Europe (200+ connectivity providers)

DNS4EU

DNS4EU for Telcos & ISPs

- Main distribution channel
- Millions of users covered
- Offered as added-value service

DNS4EU for Public

- Pure resolution
- Protected resolution
- (Protected resolution with Adult filtering)
- (Protected resolution with Ad-filtering)

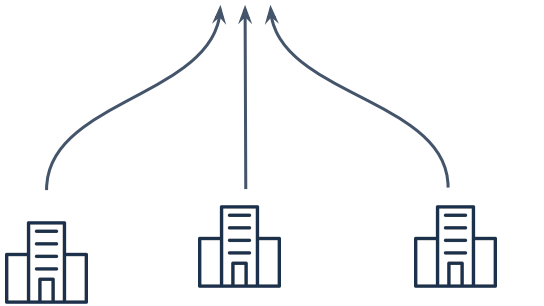
DNS4EU for Governments

- Main distribution channel
- Hierarchical structure with multi-tenancy
- (municipalities VS ministry)

DNS4EU for Governments

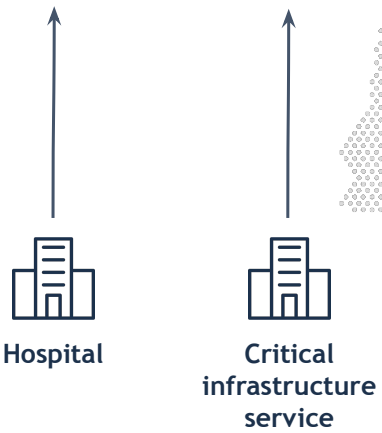
No deployment

National DNS resolver(s)



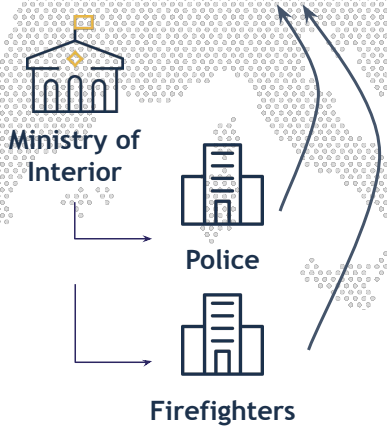
Standard deployment

On-Premise DNS resolver

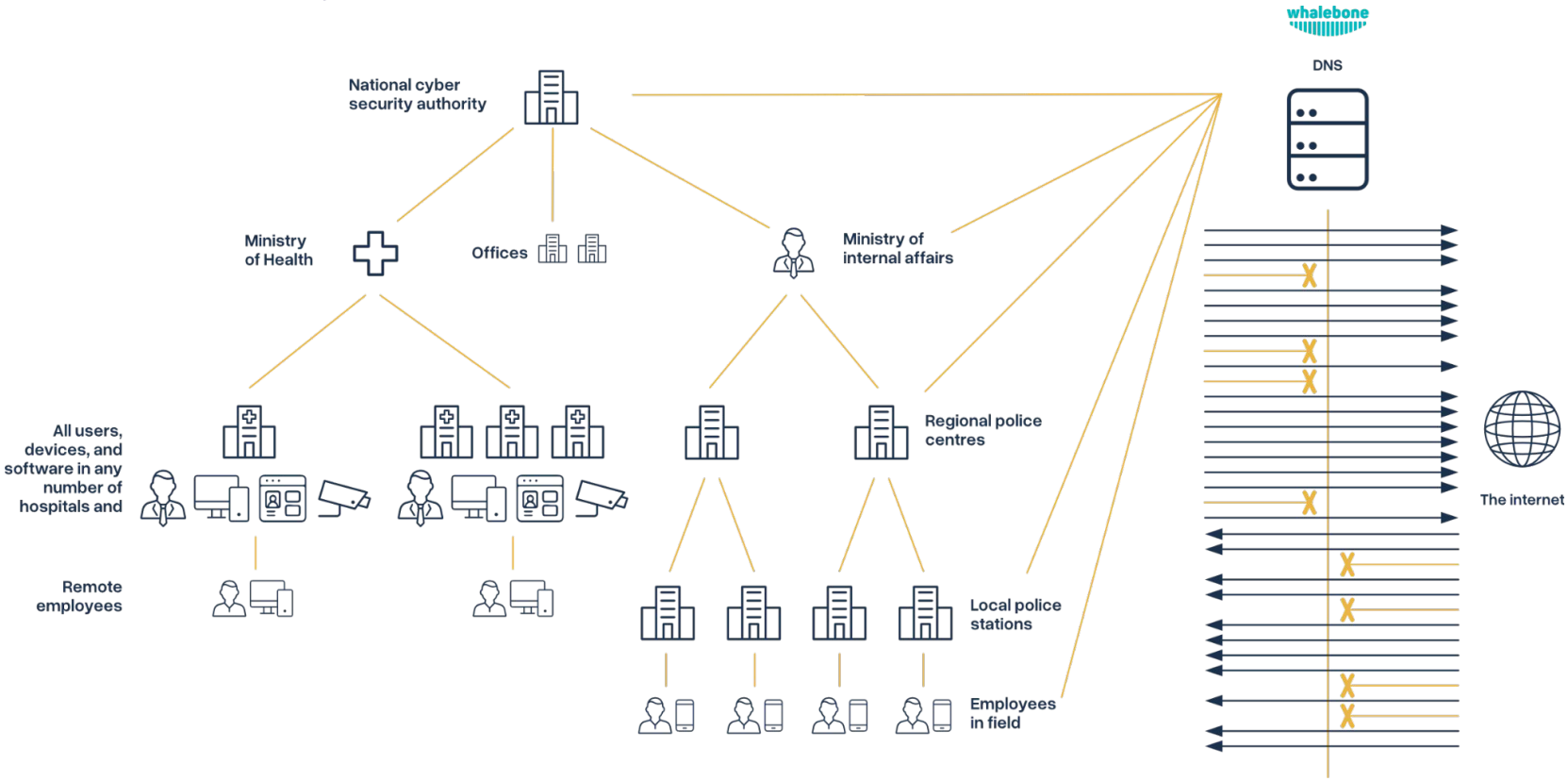


Multi-tenant deployment

On-Premise DNS resolver



Security Architecture



Basic Pillars

Input
Threat intelligence data

Output
Protection
of millions of users
and organisations

DNS4EU Success in Numbers

Solutions are readily available for DNS4EU, with DNS4GOV available for organizations outside the EU. Many new initiatives are already underway so far in 2025:

Onboarding and Collaborations

- +20 — NCSCs in later stages of onboarding cycle
- 18 — PoCs with European NCSCs
- First EU customer covering ~30,000 people in production (2024). First GOV deployment as of 2025. First Defense project in PoC (2025).

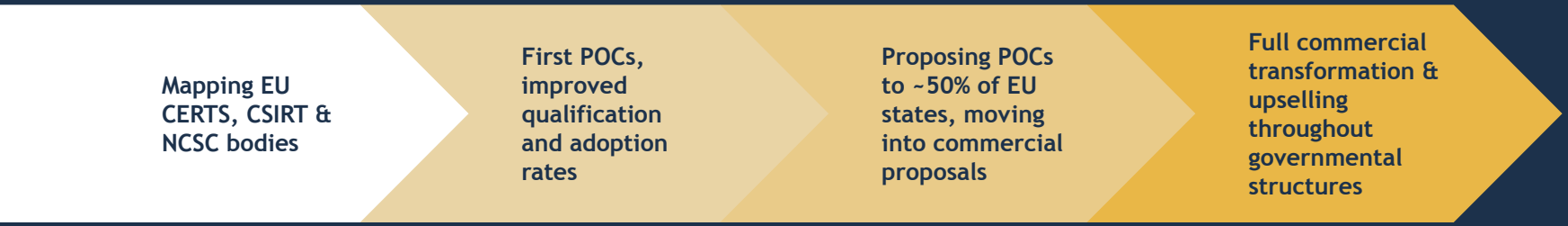
Threat Intelligence Sharing

- 14 (+3) — CERTs in Malware Information Sharing Platform (MISP) exchange Threat Intelligence
- +70 — Consortium contact with CERTs across Europe – for both public and private sectors

Engagement and Outreach

- +50 — Conferences
- +16 — Workshops & Webinars
- +800 — Participants Reached
- +500 — Stakeholder Community Members

Government Onboarding Lifecycle



- Communication campaigns
- Research extension on Gov structures throughout the EU
- Reaching out to operators and governments, establishing “champions”

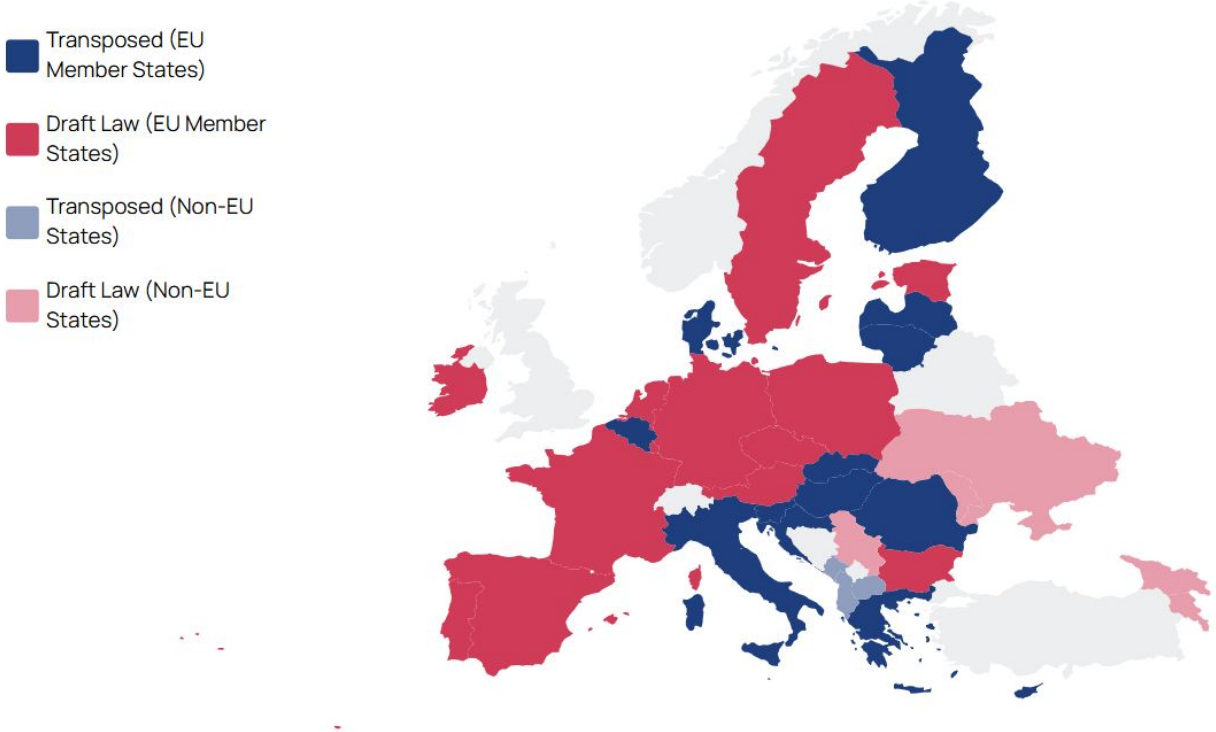
- Regional Threat Intelligence exchange setup
- Technology, Security and standards

- Discoverability
- Attracting end-users
- Scaling the deployments as needed

- Sustainability and continuous service improvement

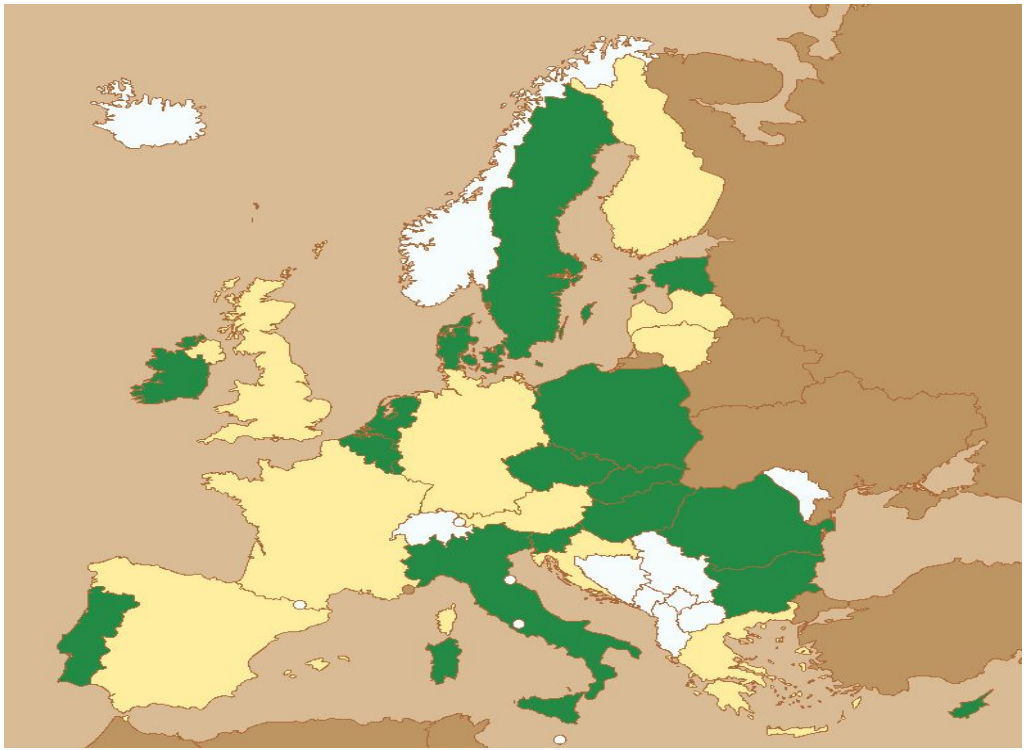
ECSO - transposition tracker NIS2

As of 09.2025



DNS4GOV acquisition readiness

MISP and / or POC successfully kicked off



DNS4EU project - Get it now!

Co-funded by
the European Union

Questions? Thank you.

George Buhai

george.buhai@whalebone.io

+40.746.122.823 / +47.413.555.66

www.linkedin.com/in/georgebwhalebone/

DNS4EU

European PDNS readiness: Leveraging CERT Insights for Advanced Threat Intelligence

Viliam Péli | Threat Intelligence Lead

Project number: 101095329 21-EU-DIG-EU-DNS
Project name: DNS4EU and European DNS Shield.
This project is co-funded by the European Union.

whalebone

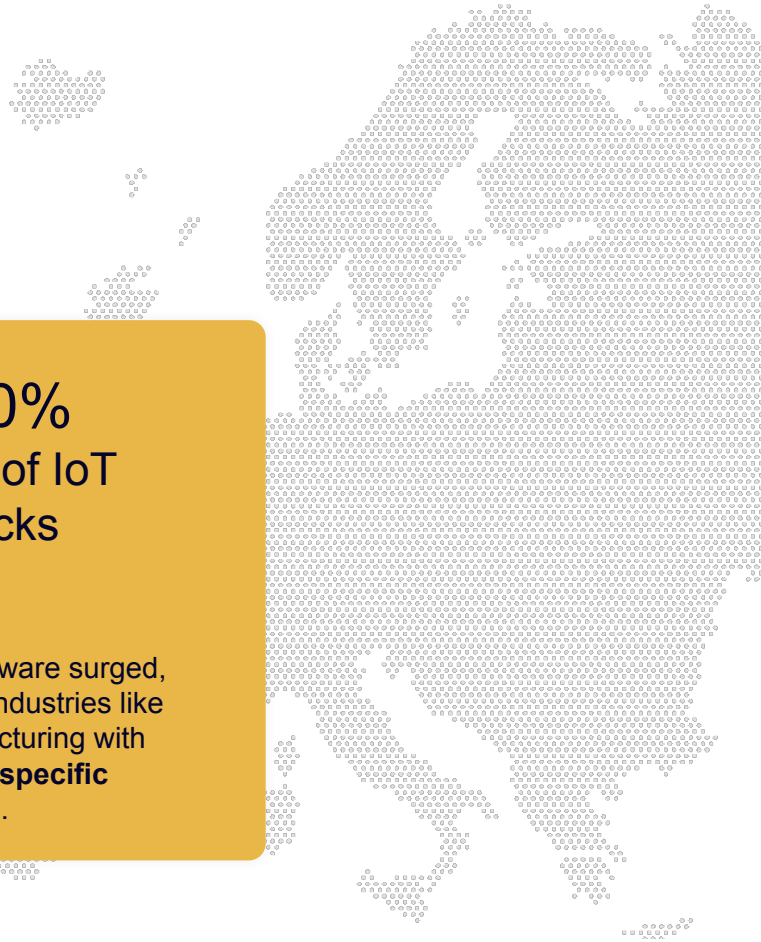
Co-funded by the European Union

"In today's threat landscape, speed is everything. It’s not just about identifying threats but stopping them before they cause damage, and regional intelligence gives us that edge."

VILIAM PÉLI

Threat Intelligence Lead
Whalebone

The rise of regionally focused cyber threats



5,600+ ransomware attacks

A significant number of **ransomware** attacks were **regionally targeted**, disrupting critical sectors.

60% zero-day attacks

Most zero-day exploits targeted network edge vulnerabilities in specific **regional infrastructures**.

400% rise of IoT attacks

IoT malware surged, hitting industries like manufacturing with **region-specific attacks**.

DNS4EU project

Co-funded by
the European Union

DNS4EU Threat Intelligence

INTRODUCTION: Threat intelligence exchange is one of the key pillars of the DNS4EU project.

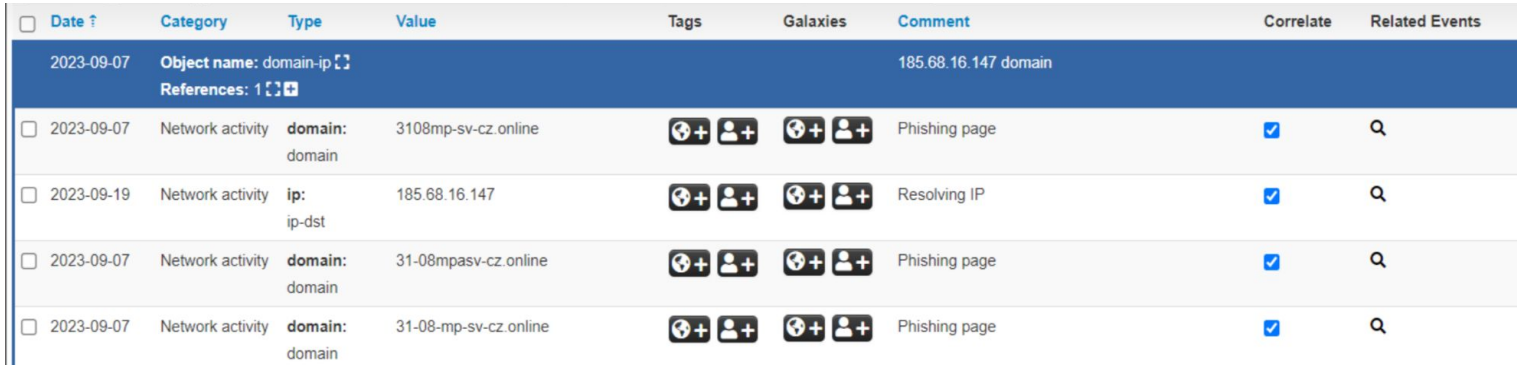
GOAL: Protect Europe from regional and global threats

CHALLENGE: Quickly propagate CERT's knowledge of threats to real people

SOLUTION: Newly identified threat can propagate to DNS4EU resolver in real time. CERTs and CSIRTs are highly endorsed to join the project in order to effectively cover the global and local threats.

Regional Threat Intelligence (MISP)

- Open-source Threat Intelligence and sharing platform
- Distributed servers which can create, consume or forward TI data about malicious domains, IPs and more
  - Any CERT, CSIRT or commercial subject can run their own instance
- Allow to enter many types of threats with context, tags, commentary and more



Date	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events
2023-09-07	**Object name:** domain-ip **References:** 1					185.68.16.147 domain		
2023-09-07	Network activity	**domain:** domain	3108mp-sv-cz.online			Phishing page	☑	
2023-09-19	Network activity	**ip:** ip-dst	185.68.16.147			Resolving IP	☑	
2023-09-07	Network activity	**domain:** domain	31-08mpasv-cz.online			Phishing page	☑	
2023-09-07	Network activity	**domain:** domain	31-08-mp-sv-cz.online			Phishing page	☑	

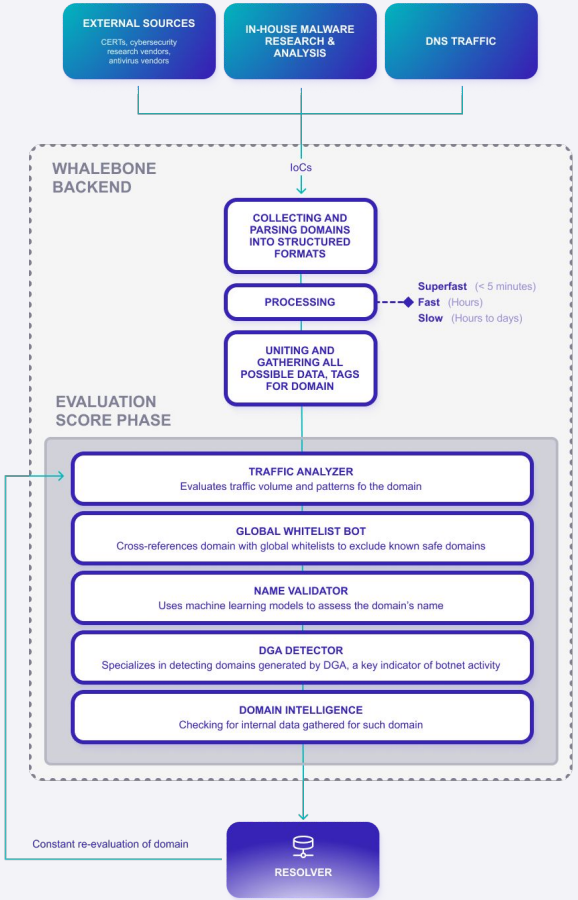
From DNS4EU to Whalebone DNS4GOV: The Journey Continues

whalebone

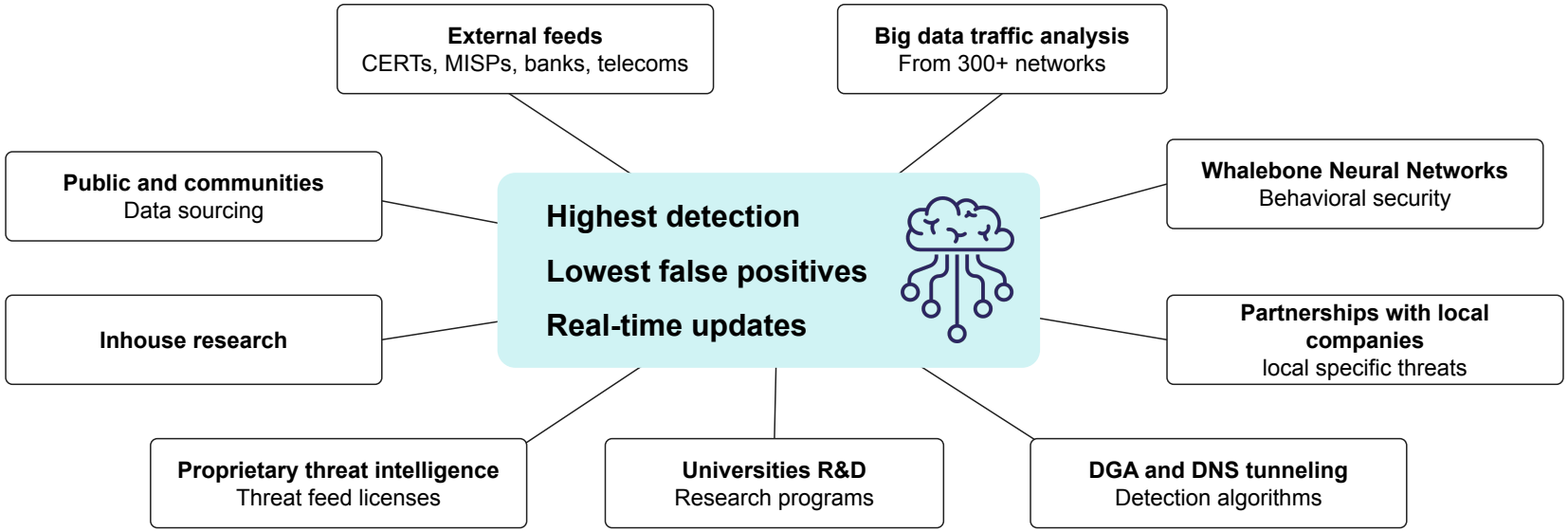
Whalebone Global Threat Intelligence

DNS Threat Intelligence

- We combine inhouse research with data from external partnerships.
- Every second we are detecting millions of possible online threats in the network and automatically evaluate and pass them to resolvers.
- We use machine learning techniques, AI, and statistics to achieve the best ratio of false and true positives.



Whalebone Threat Intelligence sources



Result? High-quality protection with Low false positive rates.

Whalebone Global Threat Intelligence Overview

Unparalleled Threat Detection and Prevention

3.8+ billion malicious domain accesses blocked in the past month

26.5+ million unique malicious domains in our database

350,000 new domains added **daily** for up-to-date protection

Comprehensive Threat Coverage

56% Malware

18.28% Command & Control (C&C)

12.2% Phishing

8.5% Blacklists

4.65% Coinminers

Industry-leading performance

Independent benchmarking shows that we consistently outperform competitors, delivering significantly higher blocking rates.

Low false positives ensure security and user trust.

whalebone

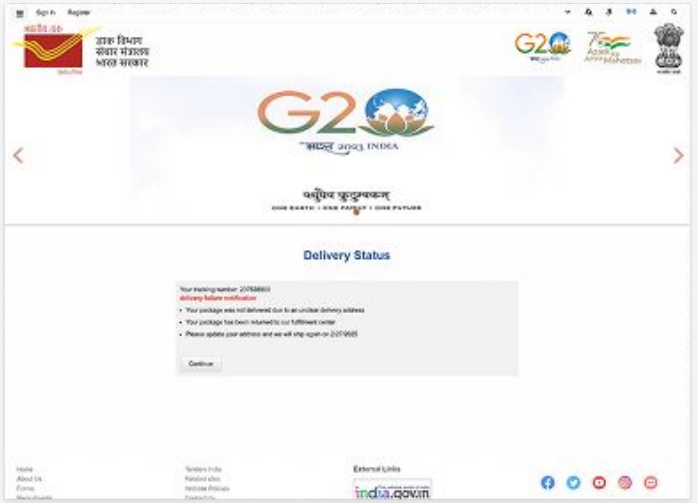
Local & Regional Threat Intelligence

Global and Regional threat detection

Global phishing campaign

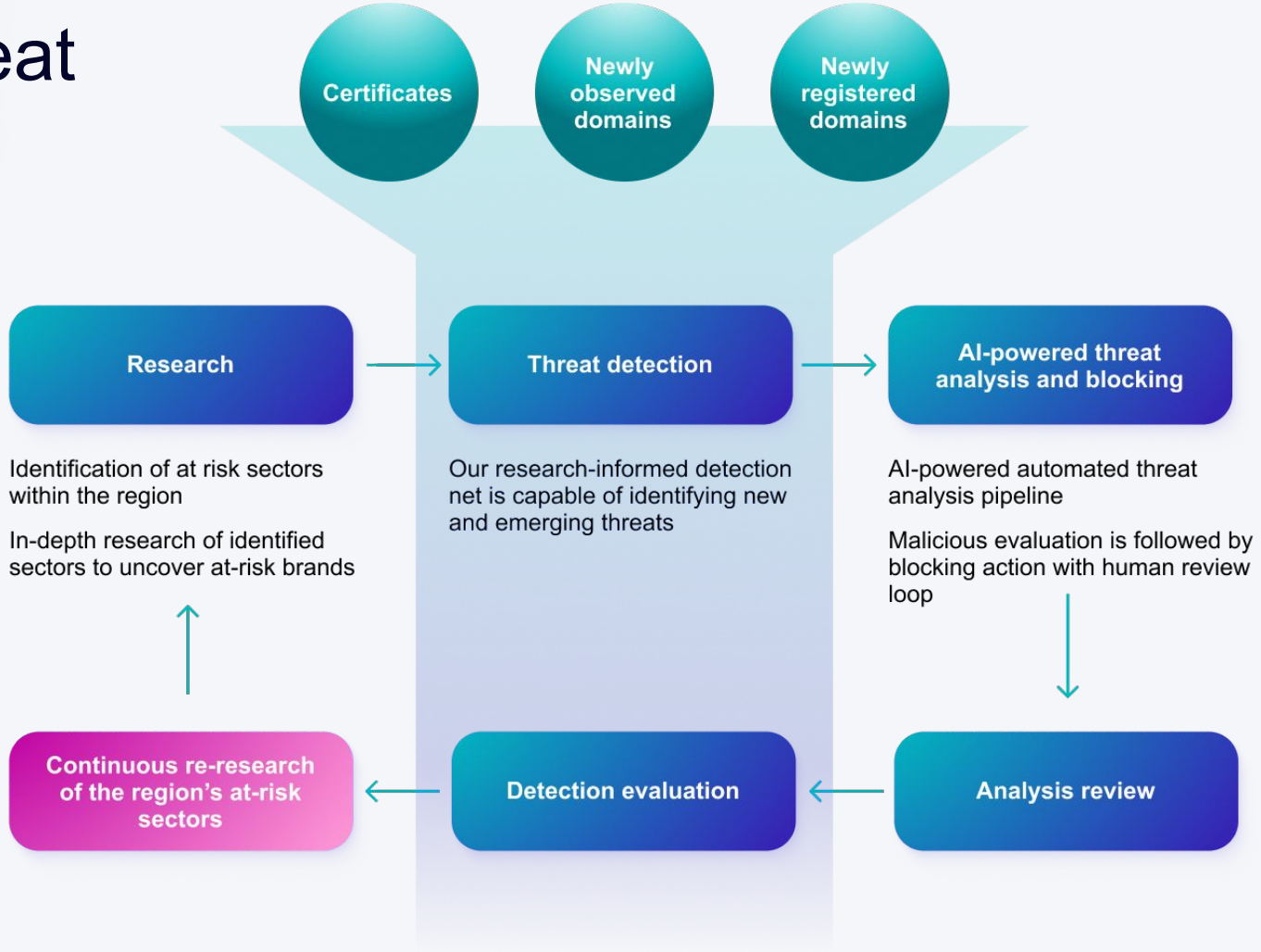
Phishing attacks using global brands as an attack vector can be detected by global solutions, as their MO does not differ across regions

Phishing campaign targeting India



Phishing attacks using local brands and other local points of interest as attack vectors can evade well-primed global solutions due to local differences

Regional Threat Intelligence Life-Cycle



Regional Threat Intelligence process: Research and Detection

Research process within the region of interest

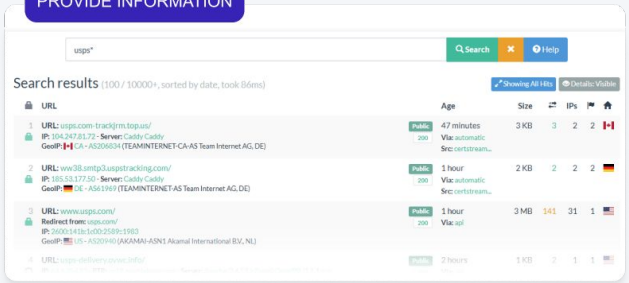
(USA example)

PROVIDE INFORMATION

USPS.COM

The **United States Postal Service** (USPS), also known as the **Post Office**, **U.S. Mail**, or simply the **Postal Service**, is an independent agency of the executive branch of the United States federal government responsible for providing postal service in the United States, its insular areas and associated states. It is one of a few government agencies explicitly authorized by the Constitution of the United States. As of 2023, the USPS has 525,469 career employees and

PROVIDE INFORMATION



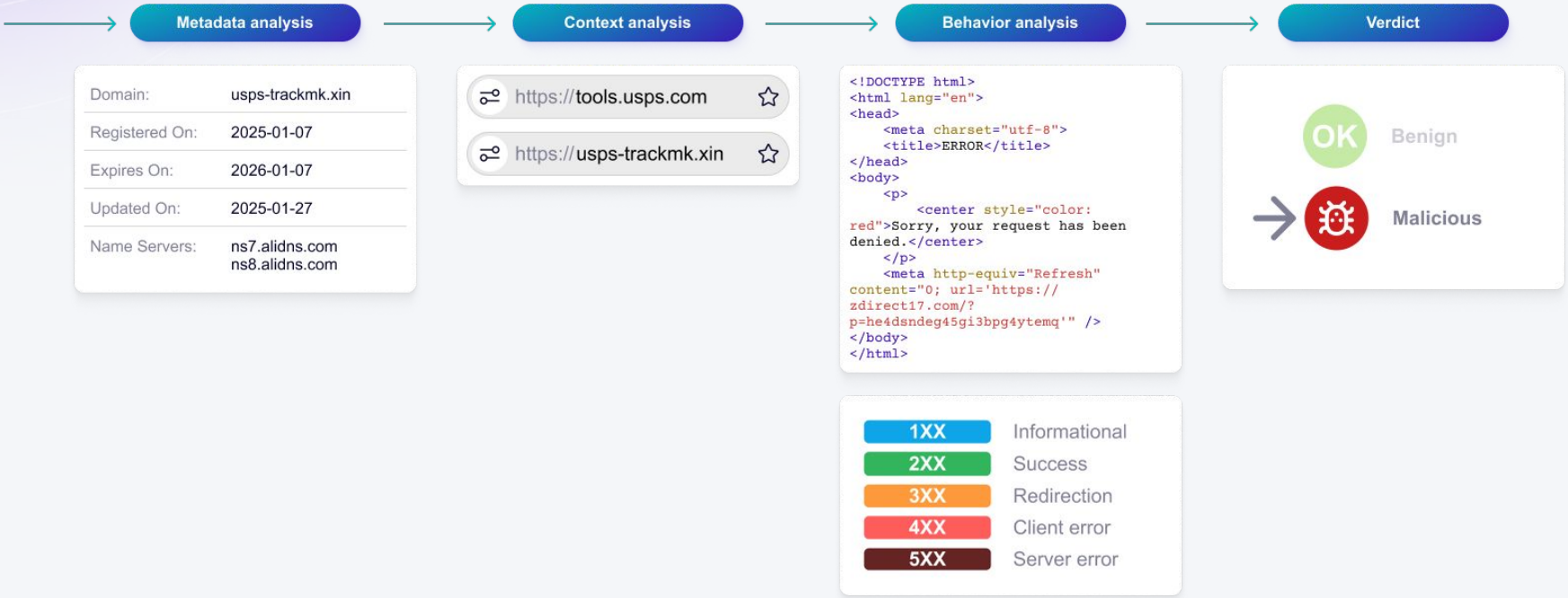
Refinement of detection by historical analysis of existing threats from open sources (shown on URLscan) and from our existing data

DETECTED

https://usps-trackmk.xin

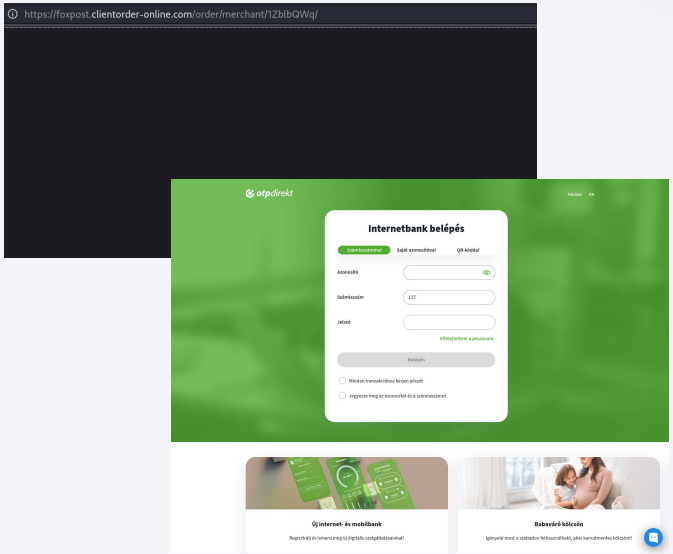
Domain:	usps-trackmk.xin
Registered On:	2025-01-07
Expires On:	2026-01-07
Updated On:	2025-01-27
Name Servers:	ns7.alidns.com ns8.alidns.com

Regional Threat Intelligence process: Automated Analysis Pipeline examples



One example out of many:

foxpost[.]clientorder-online[.]com



Case study: Attack by APT29 group targeting political parties in Germany

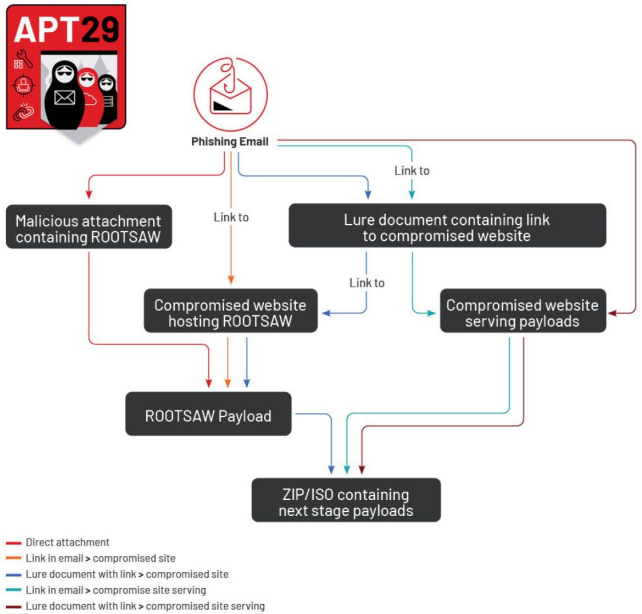
- Attack by APT29 - Cozy Bear
- A known threat group linked to Russia's Foreign Intelligence Service, which has been active since at least 2008.
- In 2023 They targeted German embassy in ICEBEAT Campaign.

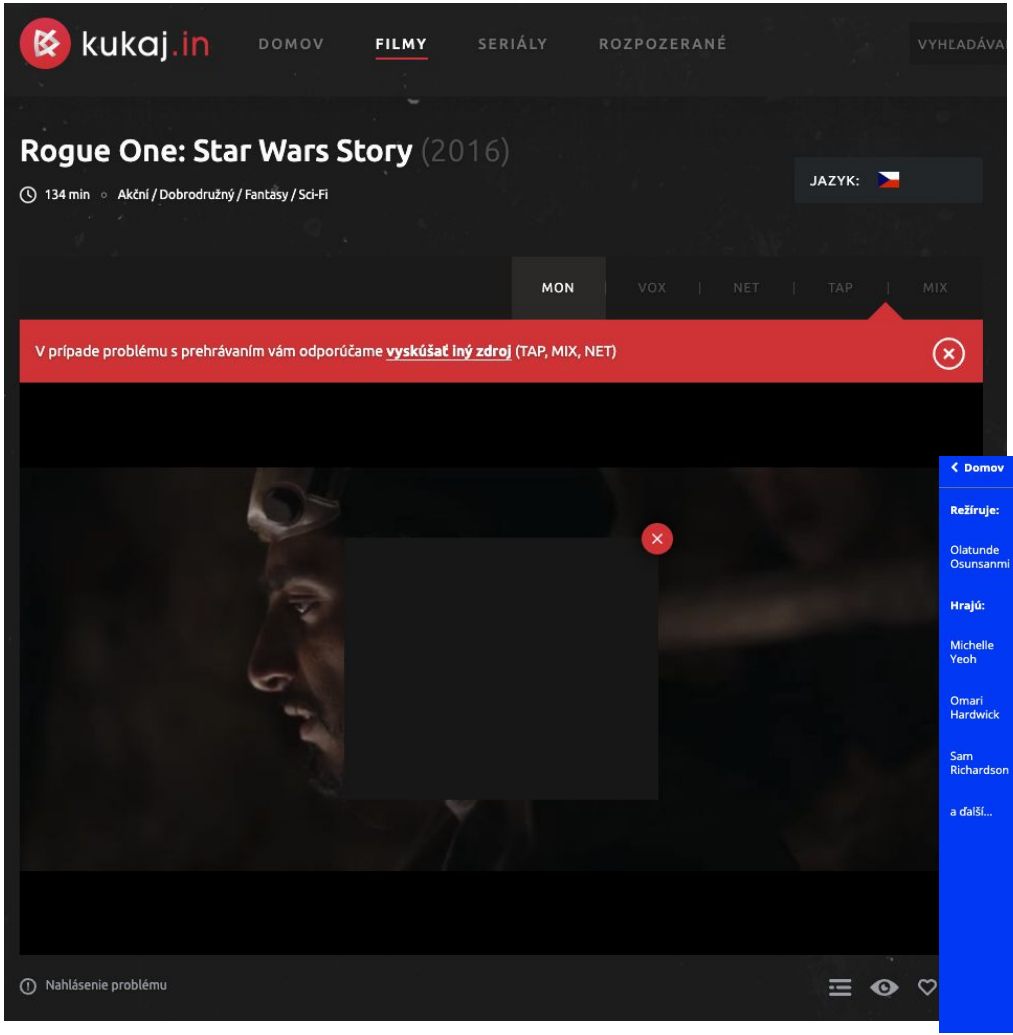
- They compromised WordPress sites to redirect unsuspecting victims to a malware installer called ROOTSAW.
- These sites were cleverly disguised as invitations to a fake event hosted by the **CDU (Christian Democratic Union).**

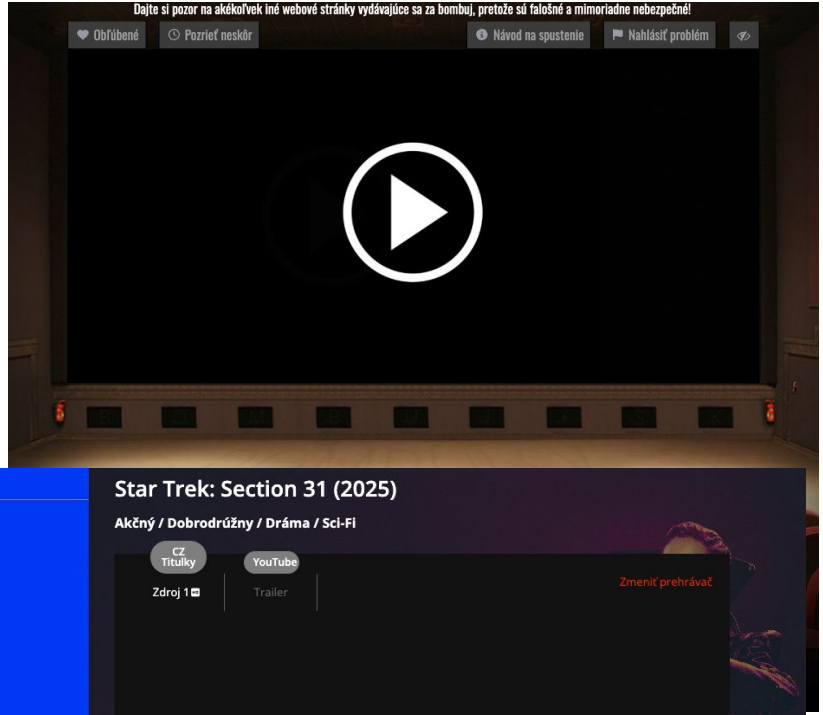
CDU

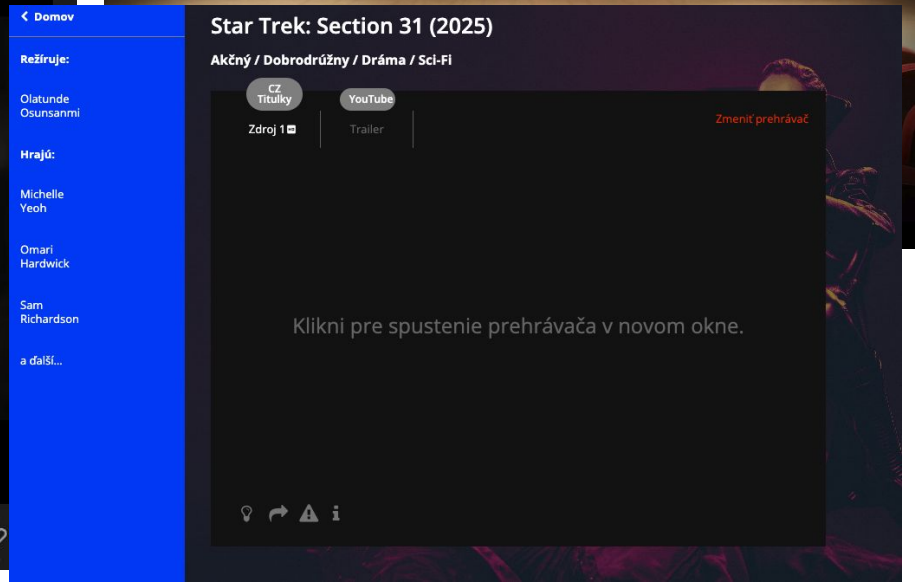
Wir freuen uns, Sie zu einem Abendessen des regionalen repräsentativen Amtes der Partei einzuladen, das am 1. März um 19 Uhr helfen wird

Um an der Veranstaltung teilzunehmen, füllen Sie bitte einen Fragebogen aus und senden Sie ihn in den nächsten Tagen per E -Mail. Einladungen werden in die ordnungsgemäße Zeit gesendet.




kukaj.in
DOMOV
FILMY
SERIÁLY
ROZPOZERANÉ
VYHĽADÁVA
Rogue One: Star Wars Story (2016)
134 min ○ Akční / Dobrodružný / Fantasy / Sci-Fi
JAZYK:
MON
VOX | NET | TAP | MIX
V prípade problému s prehrávaním vám odporúčame vyskúšať iný zdroj (TAP, MIX, NET)
Nahlásenie problému

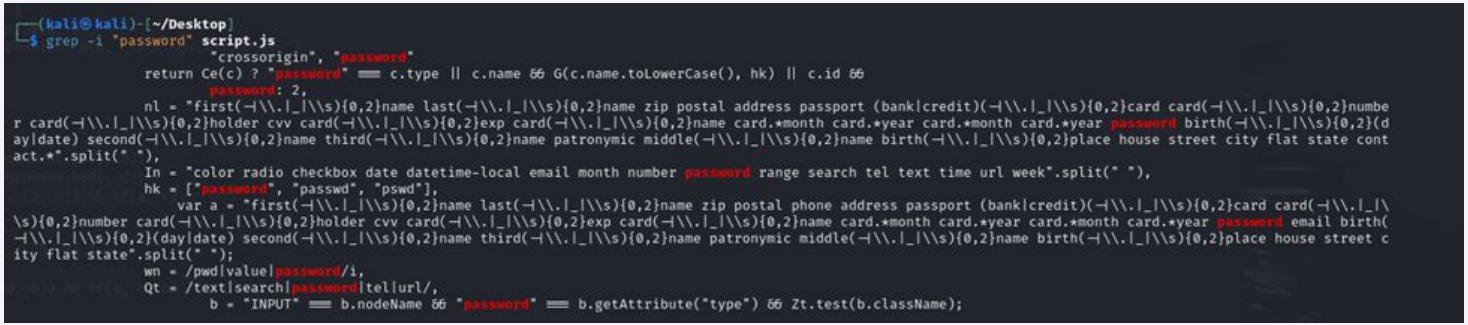

Dajte si pozor na akékoľvek iné webové stránky vydávajúce sa za bombuj, pretože sú falošné a mimoriadne nebezpečné!
Obľúbené
Pozrieť neskôr
Návod na spustenie
Nahlásiť problém


Domov
Režíruje:
Olatunde Osunsanmi
Hrajú:
Michelle Yeoh
Omari Hardwick
Sam Richardson
a ďalší...
Star Trek: Section 31 (2025)
Akčný / Dobrodružný / Dráma / Sci-Fi
CZ Titulky
YouTube
Zdroj 1
Trailer
Zmeniť prehrávač
Klikni pre spustenie prehrávača v novom okne.

Free movie traps

Exploiting video streaming sites with fake downloads

- Malicious advertisements saturating video streaming websites
- After clicking on the advertisement, it will start a 13000 line javascript from a Russian domain
- Script begins to monitor HTML forms and **identifying password, personal and financial data**
    - Script is also able to work with various languages and alphabets



Interested
in more details?

joindns4.eu

linkedin.com/showcase/dns4eu/

twitter.com/dns4eu

facebook.com/dns4eu

Let's discuss safer Europe together.

Thank you.

Viliam Péli

whalebone.io

viliam.peli@whalebone.io