



From DNS4EU to Global Telecom Security: Leveraging Threat Intelligence For Resilient Networks

Viliam Péli | Threat Intelligence Specialist

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



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 Specialist
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

= safe, stable and private
internet for Europe

What is DNS4EU

DNS4EU is an initiative by the European Commission with the goal of providing a private, safe and independent DNS resolution for European citizens, governments, and institutions.

DNS4EU aligns with the EU's vision of digital independence by providing an alternative to the existing public DNS services offered by major non-EU tech companies.



DNS4EU Consortium leader



Whalebone, s.r.o.

Whalebone is a cybersecurity company that brings next-generation DNS security to T1 Telcos, regional ISPs, and enterprises all over the world.

Their products already protect more than **400 companies** and millions of their customers from malware, phishing schemes, and other malicious attacks targeted at all types of internet-connected devices.

Whalebone's mission is to bring cybersecurity to 1 billion internet users by the end of the decade.

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

Public resolvers comparison

Feature	DNS4EU	Google	Cloudflare	Quad 9	AdGuard <i>(commercial)</i>
DNSSEC	Yes	Yes	Yes	Yes	Yes
DNS over HTTPS/TLS	Yes	Yes	Yes	Yes	Yes
DNS over QUIC	in 2025	No	No	No	Yes
Private data anonymization	Yes	No	No	Yes	No
Filtering options	Pure Protective Child protection Advertisement	Pure	Pure Protective Child protection	Pure Protective	Pure Protective Child protection Advertisement

DNS4EU Threat Intelligence

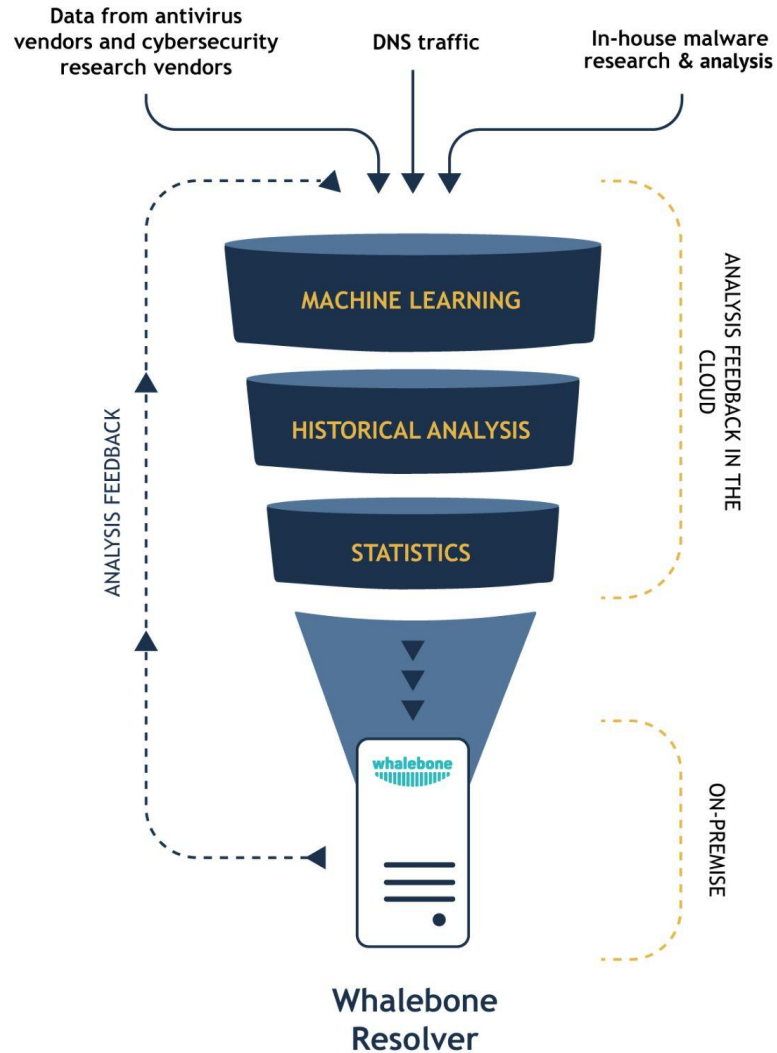
INTRODUCTION: Threat intelligence exchange is one of the key pillars of the DNS4EU project.

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.

Threat Intelligence



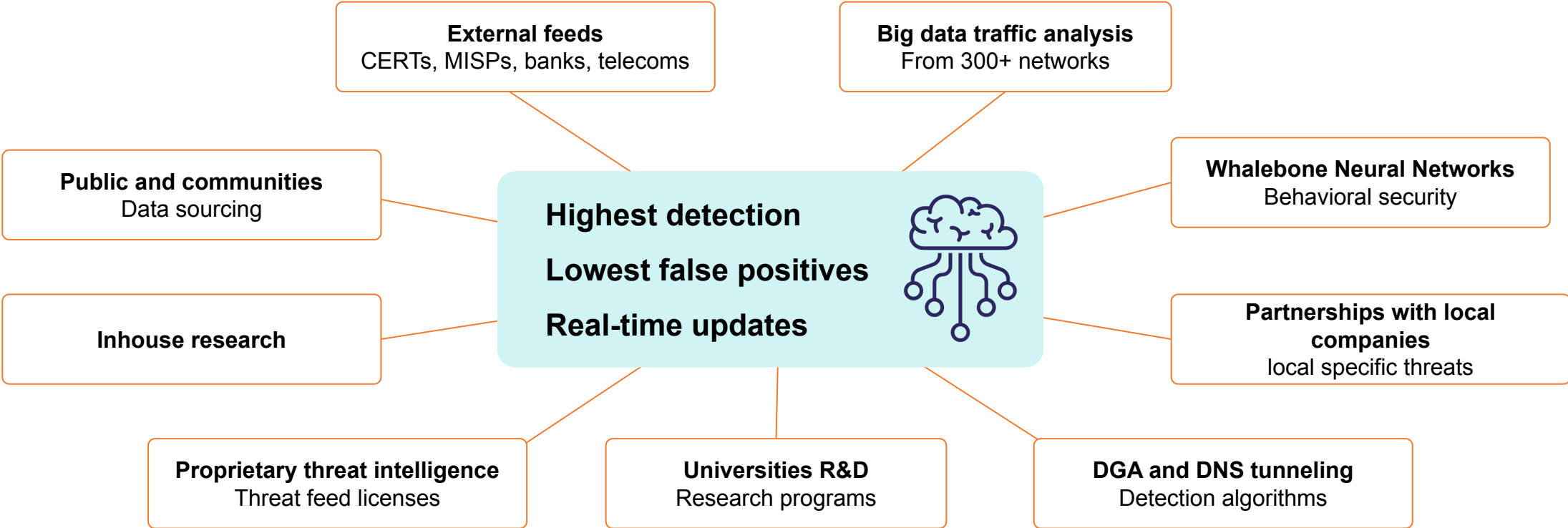
- We combine in-house research with data from external partnerships
- Every minute we are detecting possible online threats in the network and pass the data to the resolvers
- We combine machine learning techniques and statistics to refine the Threat Intelligence and avoid false positives

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

<input type="checkbox"/> Date ↑	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events
2023-09-07	Object name: domain-ip [↗]					185.68.16.147 domain		
	References: 1 [↗]							
<input type="checkbox"/> 2023-09-07	Network activity	domain: domain	3108mp-sv-cz.online			Phishing page	<input checked="" type="checkbox"/>	
<input type="checkbox"/> 2023-09-19	Network activity	ip: ip-dst	185.68.16.147			Resolving IP	<input checked="" type="checkbox"/>	
<input type="checkbox"/> 2023-09-07	Network activity	domain: domain	31-08mpasv-cz.online			Phishing page	<input checked="" type="checkbox"/>	
<input type="checkbox"/> 2023-09-07	Network activity	domain: domain	31-08-mp-sv-cz.online			Phishing page	<input checked="" type="checkbox"/>	

Whalebone Threat Intelligence sources



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



Whalebone Global Threat Intelligence Overview



whalebone
"WORLDWIDE"

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

110% higher blocking rate than the second-best competitor (AV-Test)

Maintained low false positive ratio

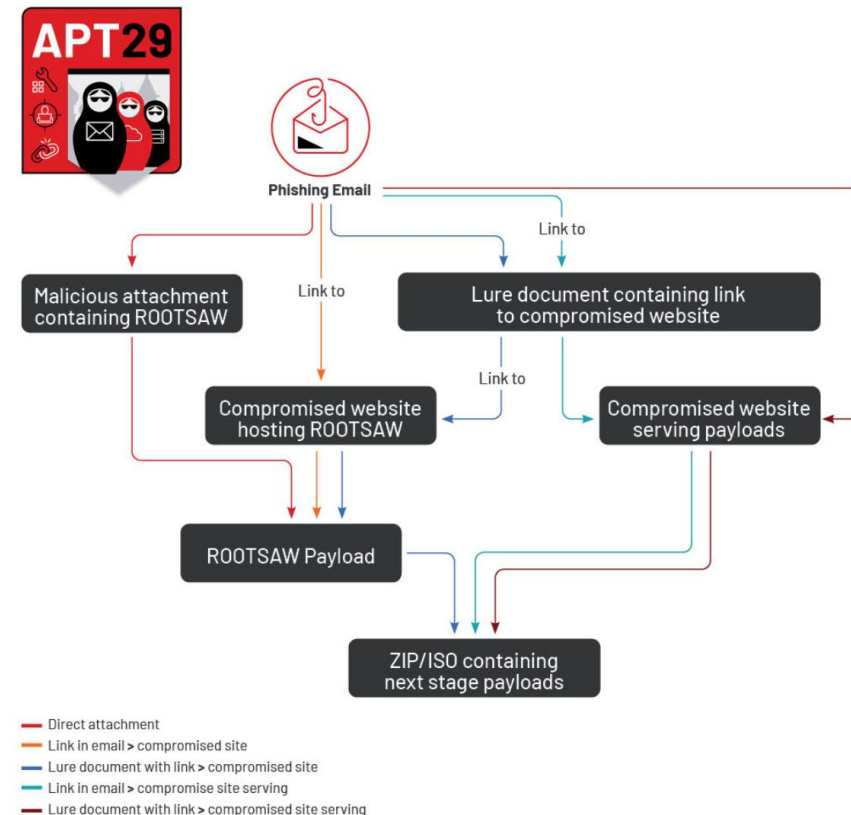
Case study: Attack by APT29 group targeting political parties in Germany



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.

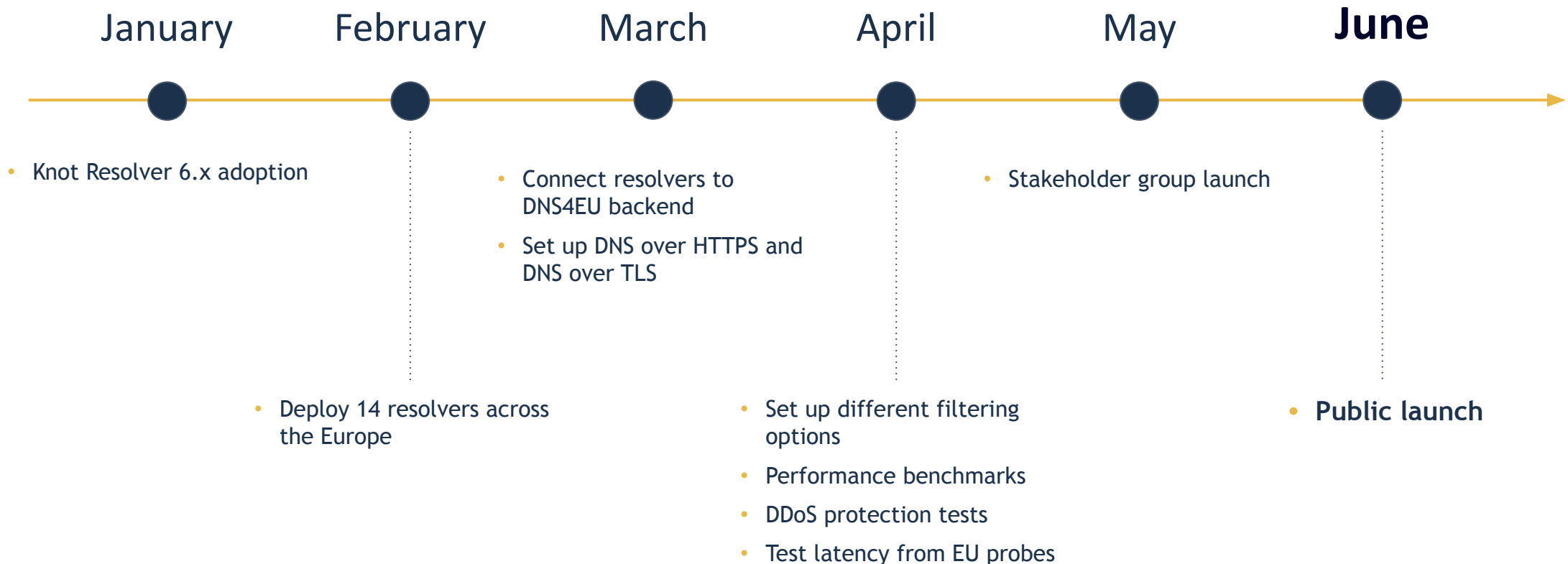
- Attack by APT29 - **Cozy Bear**
- A known threat group linked to Russia's Foreign Intelligence Service, which has been active since at least 2008.
- In 2023 They targeted **German embassy in ICEBEAT Campaign**.
- They compromised WordPress sites to redirect unsuspecting victims to a malware installer called **ROOTSAW**.
- These sites were cleverly disguised as invitations to a fake event hosted by the **CDU (Christian Democratic Union)**.



A background image of space showing the Earth's horizon from space. The sky is dark blue with a few stars. A bright comet with a long tail is visible in the upper left. The Earth's horizon is a thin line of light blue and white, with a bright sun or star on the right side.

When can I use **◆ DNS4EU**

Public resolvers **timeline**



Public resolvers map



**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

