DNS4EU

Co DNS4EU přinese uživatelům i poskytovatelům internetu?

Robert Šefr | CTO, Whalebone

whalebone

Co-funded by the European Union

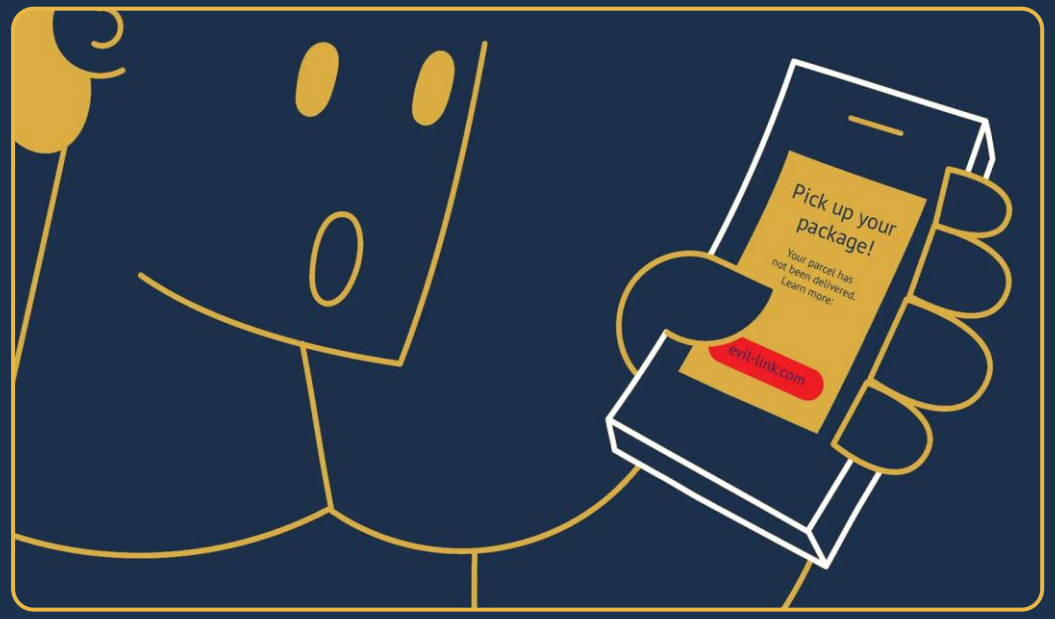
Agenda

1. Co je to Protective DNS
2. Projekt DNS4EU
3. Technologie
4. Právo a etika
5. Threat Intelligence
6. Q&A

DNS ∩ Kybernetická bezpečnost

15B

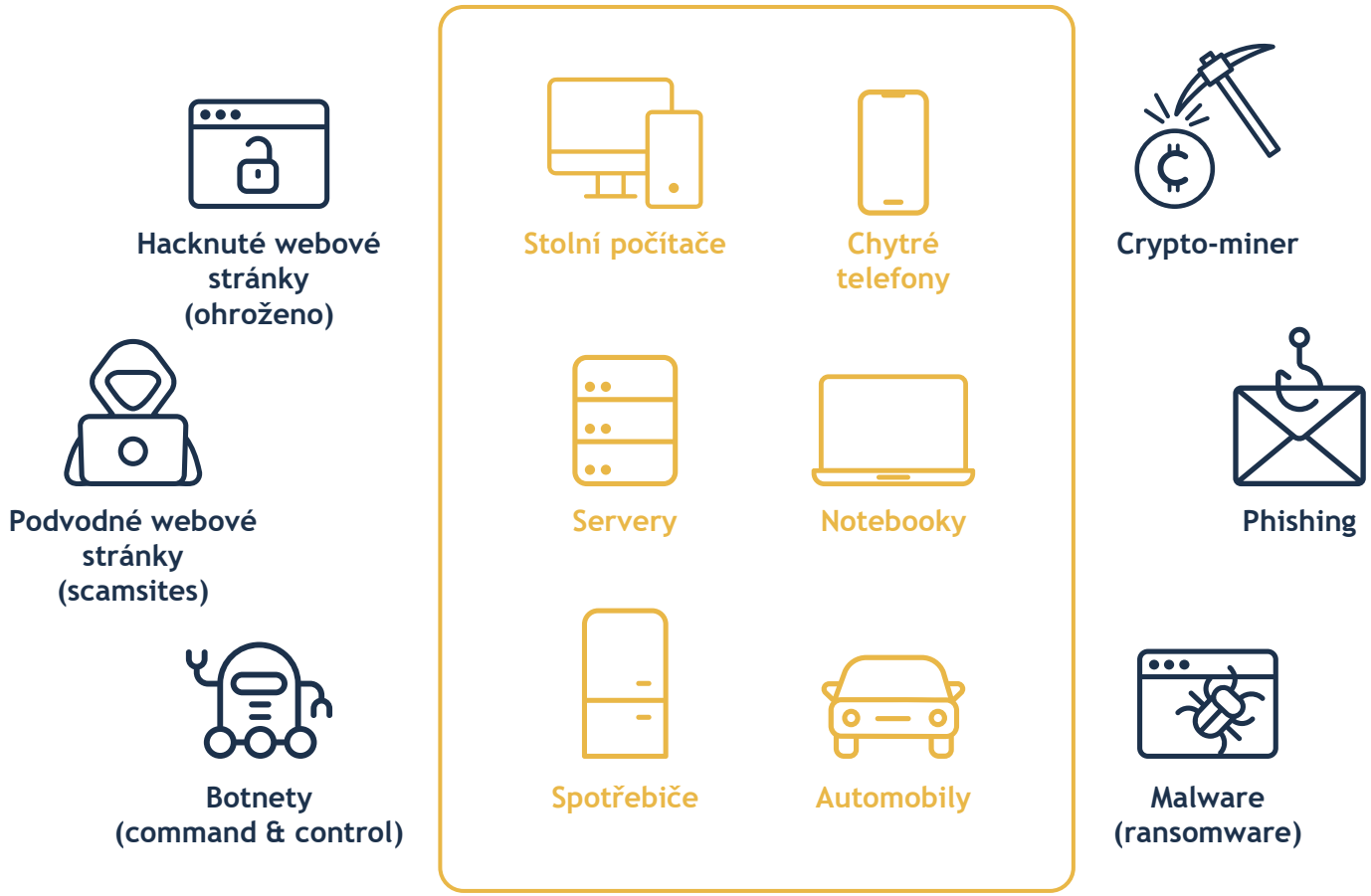
připojených zařízení



94%

útoků se opírá o DNS

Protective DNS (PDNS)



- Znemožnění útočníkům používat domény může **výrazně snížit** počet bezpečnostních incidentů a zlepšit jejich včasné odhalení.
  - phishing / smishing
  - hostování malwaru
  - Komunikace C&C

Projekt DNS4EU

Co-funded by
the European Union

DNS4EU

= bezpečný, stabilní a soukromý internet pro Evropu

Cíl agentury ENISA
Posílit digitální bezpečnost a nezávislost Evropské unie.

Výzva
Vládní instituce a občané EU nejsou dobře chráněni, protože reakce na hrozby jsou pomalé.

Řešení
Vytvoření nezávislé ochrany DNS na úrovni EU s reakcí na hrozby v reálném čase a snadnou distribucí občanům a institucím.

Konsorcium DNS4EU

Vedoucí projektu — CZ Whalebone, s.r.o.

Členové konsorcia

- CZ CZ.NIC
- CZ České vysoké učení technické v Praze
- BE Time.lex
- DE deSEC
- HU Sztaki
- IT ABI Lab Centro di Ricerca e Innovazione per la Banca
- PL Naukowa i Akademicka Sieć Komputerowa
- RO Directoratul Național de Securitate Cibernetică

Přidružení partneři

- BG Ministry of Electronic Governance
- CZ CESNET
- FI F-Secure
- PT Centro Nacional de Cibersegurança

Případy použití systému DNS4EU

Veřejnost

- Dostupné komukoli na veřejných IP adresách
- Přísná anonymizační opatření
- Může být také hostován telekomunikační společností na sdílené IP adrese

Telekomunikace

- Provoz DNS překladačů na vlastních IP adresách
- Využití technologie, Threat Intelligence a právních požadavků (státní blacklisty)

Vláda

- Využití Threat Intelligence k ochraně veřejných institucí
- Jednotný bod pro vyhledávání hrozeb a reakci na incidenty
- Není zamýšleno jako služba pro občany

Technologie

Knot Resolver / hlavní body vývoje

- Testování nástroje Knot Resolver 6.x
- Opatření proti D(DoS)

Knot Resolver / opatření proti D/DoS

1. Ochrana ostatních
    a. UDP reflection / amplification
    b. Omezení provozu směrem k autoritativním serverům
2. Ochrana sebe sama
    a. Spíše o stanovení priorit než o stanovení pevných limitů
    b. Ochrana RAM
    c. Ochrana CPU

Backend DNS4EU - funkce

- Control/Data plane pro všechny překladače DNS
- Monitorování, hlášení, upozorňování a řešení problémů
- Udržuje konfiguraci resolveru a zajišťuje, aby bylo vše synchronizováno.
- Distribuuje aktualizace Threat Intelligence v reálném čase.
- Zajišťuje veškeré autentizaci, autorizaci a audit.

Backend DNS4EU

- Zprovoznění produkčního backendu DNS4EU
- Datové centrum v EU a služba poskytovaná evropským cloud providerem
- Plánovaný další vývoj, hlavní oblasti:
  - Zabezpečení
  - Podpora nástroje Knot Resolver 6.x
  - Zlepšení výkonu zejména ve škálovatelnosti zpracování dat


Právo a etika

Data Management Plan

- Veřejnost + telekomunikační společnosti (sdílená IP DNS4EU)
  - Okamžitá anonymizace na úrovni resolveru
- Telekomunikační společnosti (využívající vlastní IP)
  - Telekomunikační společnost je správcem údajů a rozhoduje o tom, jak údaje zpracovávat.
- Vláda
  - Vláda je správcem údajů
  - Předpokládáme, že nebude použita žádná anonymizace, protože je nasazena jako bezpečnostní a analytická služba
  - Instituce, které se ke službě připojí, budou dobře obeznámeny se strategií zpracování údajů uplatňovanou vládou
  - Služba nebude využívána jednotlivými občany

Sdílení údajů třetím stranám

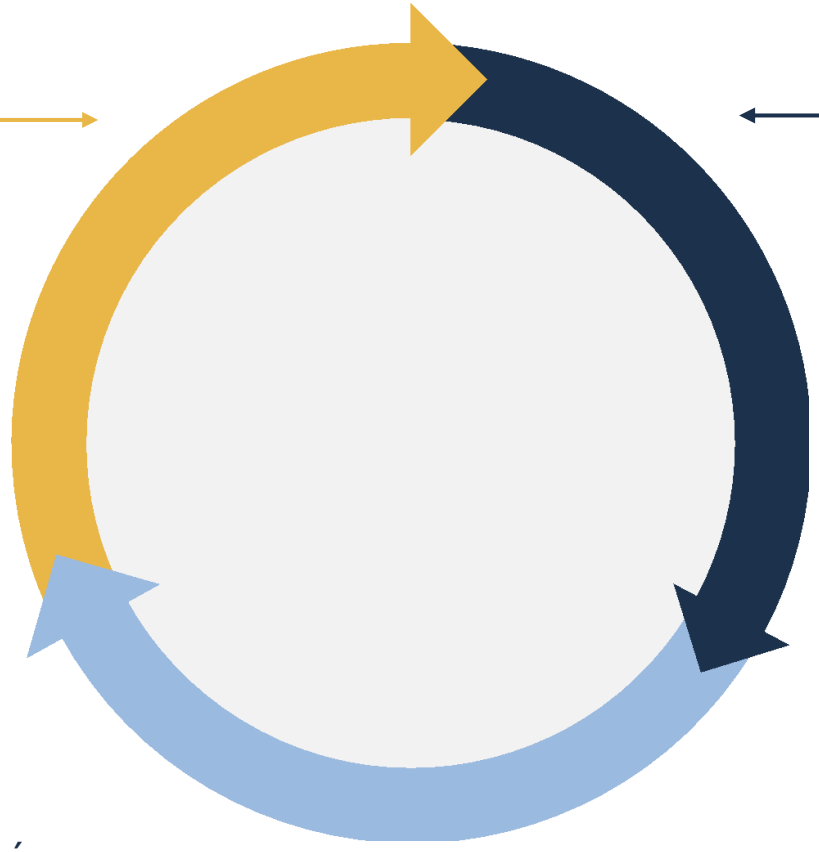
- Obecný přístup bude spočívat ve sdílení pouze souhrnných statistik
- Přístup ke zdrojovým datum lze poskytnout na základě následujících předpokladů
  - Formální žádost o sdílení údajů pod dohledem konsorcia
  - Splnění bezpečnostních opatření pro práci s daty
  - V úvahu budou brány pouze výzkumné činnosti prospěšné pro členské státy a občany EU
  - Budou dostačující pouze plně anonymizovaná data zejména z veřejného resolveru


Threat Intelligence

Životní cyklus Threat Intelligence

Zmírnění falešně pozitivních výsledků
Vyhodnocování detekce a průběžná optimalizace procesu s cílem minimalizovat výskyt falešně pozitivních detekcí.

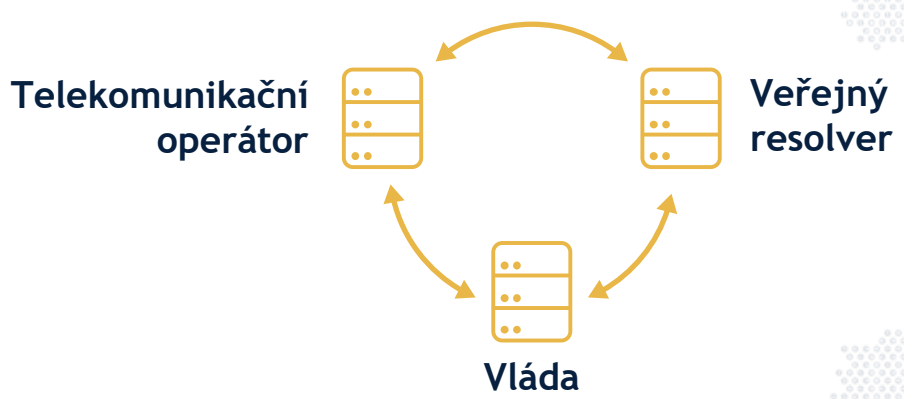
Analýza provozu
Sledování vzorů v provozu za účelem odhalení neznámých škodlivých domén, DGA a tunelování DNS.



Včasná detekce
Sledování registrace domén a certifikátů pro zachycení domény před jejím použitím.

Kanály pro sdílení Threat Intelligence
Zprávy a kanály o pozorovaných škodlivých doménách od členů konsorcia a připojených institucí.

Regionální Threat Intelligence



DNS4EU

- Banky
- Ministerstvo sociálních věcí
- Služba doručování balíků
- Sdílení informací & Analytické centrum
- Poštovní služby

Hrozby, IoC

CERT Portugalsko

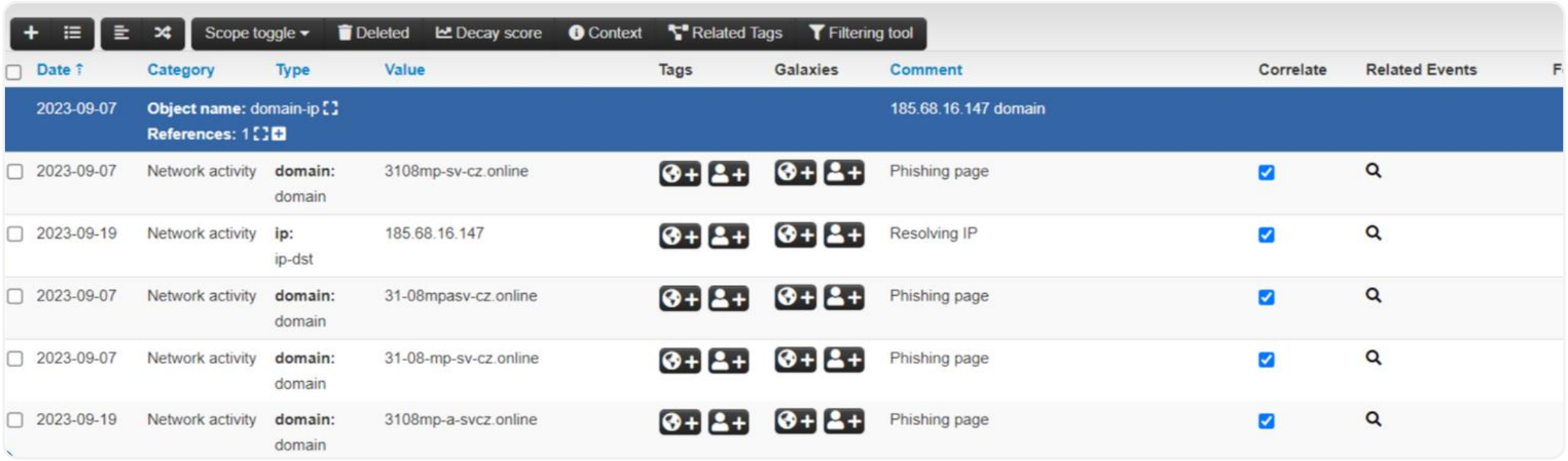
CERT Polsko

CERT Česká republika

CERT Rumunsko

Malware Information Sharing Platform

- Open-source Threat Intelligence a platforma pro sdílení informací
- Distribuované servery, které mohou vytvářet, spotřebovávat nebo předávat Threat Intelligence o škodlivých doménách, IP adresách a dalších.
  - Každý CERT, CSIRT nebo komerční subjekt může spustit vlastní instanci.
- Umožňuje zadávat mnoho typů hrozeb s kontextem, značkami, komentáři a dalšími informacemi.



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	☑	
2023-09-19	Network activity	**domain:** domain	3108mp-a-svcz.online			Phishing page	☑	

Co DNS4EU přinese uživatelům i poskytovatelům internetu?

- Technologické novinky
  - Novinky ve způsobech konfigurace resolveru
  - Další možnosti monitoringu
  - Zvýšení výkonu
  - Podpora nových protokolů a standardů
- Ochrana proti hrozbám
  - Rychlejší pokrytí hrozeb mířených na daný region
  - Automatizace v odstraňování falešných detekcí

DNS4EU / Časová osa

2023

Zahájení a přípravy

- Návrhy technologií, zabezpečení a dodržování norem
- Nasazení backendu EU
- Rozšíření výzkumu
- Oslovení telekomunikačních operátorů a vlád

2024

Nasazení v telekomunikacích a státní správě

- Nastavení regionální výměny Threat Intelligence
- Dosažení souladu s právními předpisy a bezpečnostními požadavky

2025

Koncoví uživatelé

- Dokumentace a podpora
- Propagace mezi koncovými uživateli
- Škálování nasazení podle potřeby

2026+

Pokračování po ukončení projektu

- Udržitelnost a neustálé zlepšování služeb

Podrobnější informace?

joindns4.eu

linkedin.com/showcase/dns4eu/

twitter.com/dns4eu

facebook.com/dns4eu

Máte otázky?
Děkujeme.

Robert Šefr

whalebone.io

robert.sefr@whalebone.io

linkedin.com/in/robertsefr