

Bezpečnost bez kompromisů

Ochrana před phishingem pro každého

• 23.09.2026

O sdružení CZ.NIC

- správce domény .CZ od roku 1998
- sdružení právnických osob
- více než 100 členů, 3 komory
- pobočky: Praha, Brno, Plzeň, České Budějovice
- obecně prospěšné projekty
 - Infrastruktura (mojeID, DNS...)
 - Výzkum, open source software (Knot DNS, BIRD, Datovka...)
 - Osvěta (Akademie, Edice, TV seriály...)
 - Bezpečnost (CSIRT.CZ, Turris...)



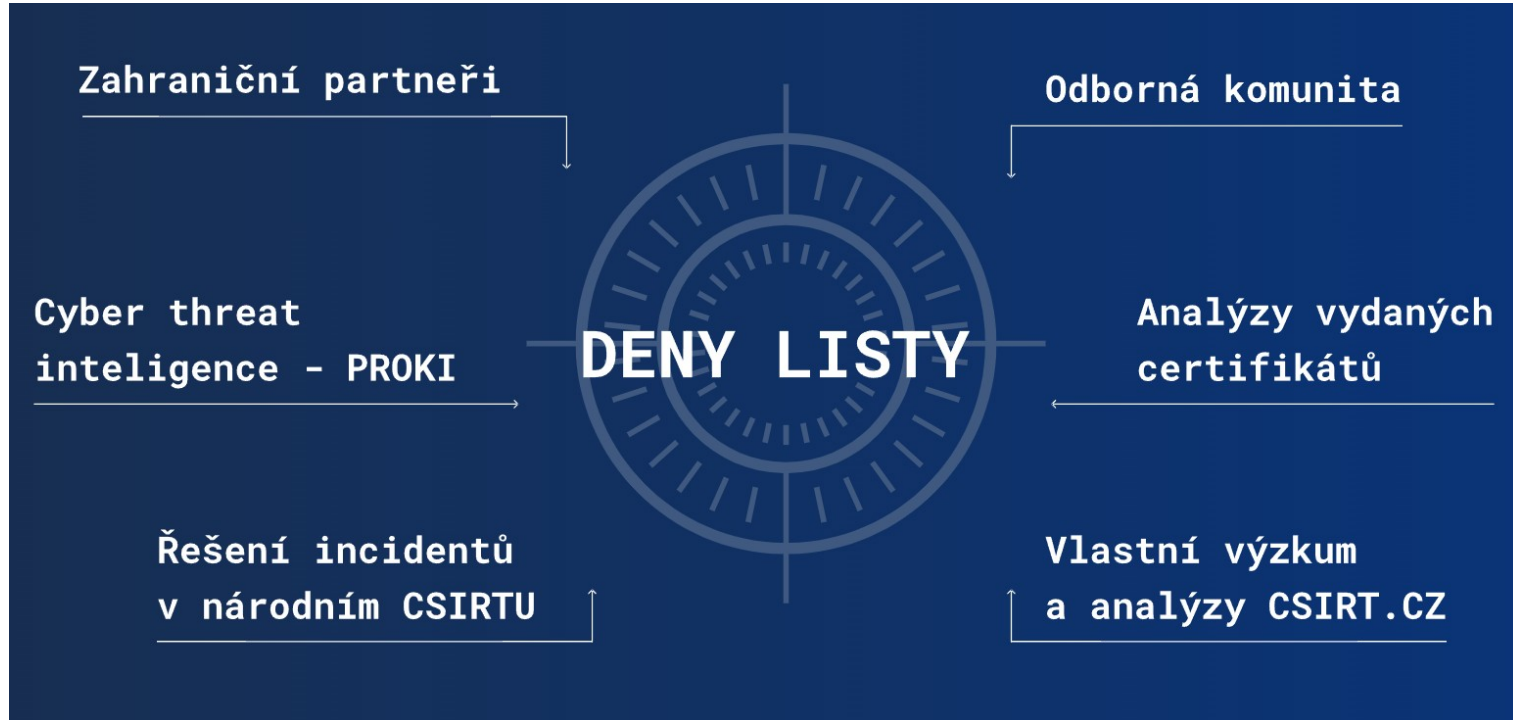
Naše projekty



CSIRT.CZ (Národní CSIRT České republiky)

- Provozované služby
 - Řešení incidentů (abuse@csirt.cz) – nejen subjekty dle zákona, ale v těchto případech i ostatní:
 - bezpečnostní incident přetrvává, na hlášení bezpečnostního incidentu nikdo nereaguje, na hlášení bezpečnostního incidentu jste obdrželi zamítavou odpověď, jste přesvědčeni o tom, že problém by se mohl týkat více sítí, které by bylo záhodno zkontaktovat a vyrozumět
 - Prevence
 - Honeypoty, PROKI, Adhoc akce (ROM-0, neaktuální CMS)
 - Vzdělávání a osvěta
 - Školení, články, AZB, pracovní skupina CSIRT.CZ
 - STOPONLINE
- Komerční aktivity
 - Deny listy
 - Penetrační testování
 - Skener webu
 - Zátěžové testy





DNS filtering

- Umožňuje pozměnit odpověď na konkrétní DNS dotaz
- Nasazení na rekurzivní DNS
- Responze policy zone (RPZ)
- Přesměruje uživatele na administrátorem definovanou stránku

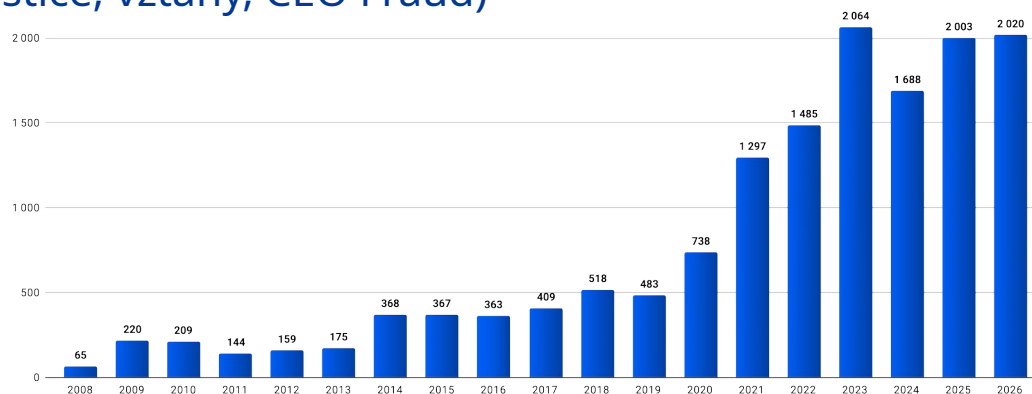


```
$TTL 3600
@ SOA rpz.firma.cz. hostmaster.rpz.firma.cz. 2609011547 60 60 432000 60
  NS localhost.
;
; Firma s.r.o. Response Policy Zones (RPZ)
; Last updated: 2026-09-01 15:47:40 (UTC)
;
; Terms Of Use: https://infoophishingu.isp.sk
; For questions please contact infoophishingu@isp.sk
;
p0rtal.eg0v.sk CNAME infoophishingu.isp.sk.
mojedatovka-prihlaseni.example-badness.net CNAME infoophishingu.isp.sk.
```



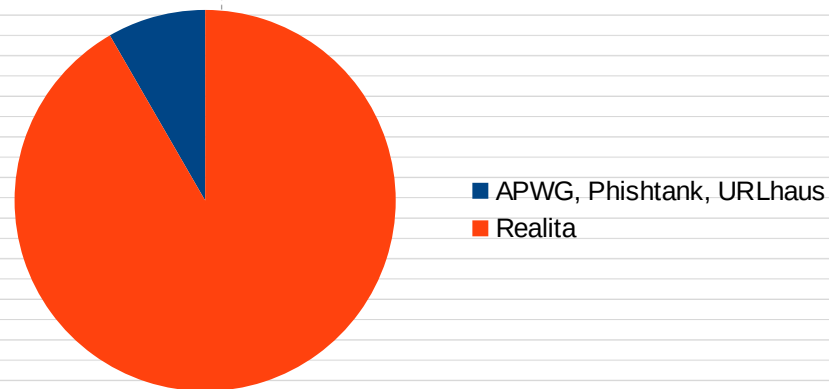
Proč to řešit

- Obrovský nárůst případů sociálního inženýrství
 - Phishing
 - Smishing
 - Vishing
 - Podvody všeho druhu (bazary, investice, vztahy, CEO Fraud)
 - Kampaně šířící malware
- V roli CSIRT.CZ nárůst od 2020



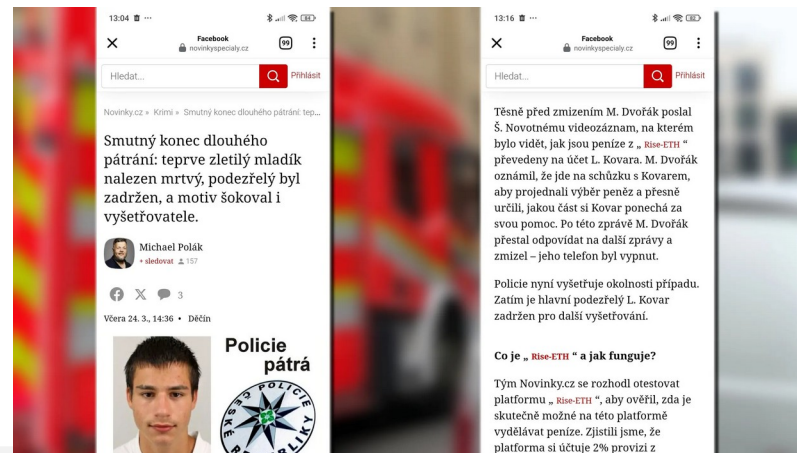
Rozdíl je v detailu

Datum	Naše detekce	Datum	Phishtank, APWG, a URLHaus	URL
1.3.	idcsszmpasv.cz	2023-03-01 22:05:01	com-ee.cz	https://secure.oldschool.com-ee.cz/m=weblogin/loginform.ws825,295,688,41525479,2938
1.3.	cssz-mp-sv.cz	2023-03-05 11:20:01	crocsky.cz	http://crocsky.cz/
1.3.	eportal-cssz.cz	2023-03-07 04:10:02	com-ea.cz	https://secure.oldschool.com-ea.cz/m.weblogin./loginform241,162,617,33878163,2916,4843
1.3.	onlineportalcssz.cz			
1.3.	24eportal-csas.cz			
3.3.	ideportalcssz.cz			
3.3.	mp-sv-eportal.cz			
3.3.	onlinecssz.cz			
3.3.	eporatal-online.cz			
3.3.	sluzby-idcssz.cz			
3.3.	ideportal-online.cz			
6.3.	csszeportalonline.cz			
6.3.	prihlasit-cssz.cz			
6.3.	pojistenceonline.cz			
6.3.	sluzbyeportal.cz			
6.3.	spustiteportal.cz			
6.3.	prihlasit-eportal.cz			
7.3.	prihlasitcsszid.cz			
7.3.	mpasv24eportal.cz			
7.3.	pojistence-online.cz			
7.3.	sluzby-eportal.cz			
7.3.	mpasv24-eportal.cz			
16.3.	ceskaposta-id.cz			
16.3.	ceska-posta-psani.cz			
16.3.	eportal24-cssz.cz			
16.3.	mp-sv-psani.cz			
16.3.	mp-sv-onlinepsani.cz			
16.3.	propojistenceccssz.cz			
16.3.	lceskapostaonline.cz			
16.3.	prejit-prijimat.cz			
16.3.	akceptovat.cz			
16.3.	eportalcssz.cz			
16.3.	prejit-na-platby.cz			



Před čím nás to ochrání

- Generické útoky
 - Mailboxy, Google, MS účty, Facebook, Booking.com...
- Cílené útoky na české a slovenské uživatele
 - Zdravotní pojišťovny, parkování, pokuty a body, Portál občana, městská doprava, ESTA, dálniční známky, investice...
- Limity služby
 - Nejde blokovat konkrétní URL
 - Zneužívané veřejné služby (Google sheets)



Hlavní komponenty

CT-Watch

- Dashboard
- Search
- Domains
- Queries
- Ignored Domains
- Tags
- Users
- Denylists
- API key

Monitor > Domains 24869 results (25129 total)

Type to search

/

Filters

☐ Uri	Reason link	Created at	Whois registered	
> ☐ easy-spark-3228.chatgpt.site  	domain:*easy* AND domain:*park* AND -registerable_domain:easypark.com	2026-09-18 15:53:15	3 years ago	...
> ☐ easy-park-3935.chatgpt.site  	domain:*easy* AND domain:*park* AND -registerable_domain:easypark.com	2026-09-18 15:23:36	3 years ago	...
> ☐ easyparknlservademis.com  	domain:*easy* AND domain:*park* AND -registerable_domain:easypark.com	2026-09-18 15:03:24	5 months ago	...
> ☐ easy-spark-2018.chatgpt.site  	domain:*easy* AND domain:*park* AND -registerable_domain:easypark.com	2026-09-18 14:21:34	3 years ago	...
> ☐ gov-infoevzp-cz.casa  	domain: *vzp* AND domain: *cz* AND tld:casa	2026-09-18 14:20:32	an hour ago	...
> ☐ slovaktech-6244.chatgpt-team.site  	domain: *slovensk* OR domain: *slovak* AND -registerable_domain:*sk	2026-09-18 14:07:49	4 months ago	...

CT-Watch

- Dashboard
- Search
- Domains
- Queries
- Ignored Domains
- Tags
- Users
- Denylists
- API key

Monitor > Queries 23 results (82 total)

Type to search

/

Filters

☐ Query	Last run	Tags	End date
☐ (e?znamk* OR eznamk*) AND -registerable_domain:eznamka.sk	2026-09-18 16:00:16		-
☐ domain_tokens:primabanka AND domain_tokens:sk AND -registerable_domain:primabanka.sk	2026-09-18 16:00:08		-
☐ domain_tokens:minv AND domain_tokens:sk AND -registerable_domain:minv.sk	2026-09-18 16:00:10		-
☐ domain_tokens:mfsr AND -registerable_domain:mfsr.sk	2026-09-18 16:00:07		-
☐ domain: *slovensk* OR domain: *slovak* AND -registerable_domain:*.sk	2026-09-18 16:00:15	sk	-
☐ domain_tokens:posta AND domain_tokens:sk AND -registerable_domain:posta.sk	2026-09-18 16:00:06	sk	-



Hlavní komponenty



Pavel Bašta [↗](#)

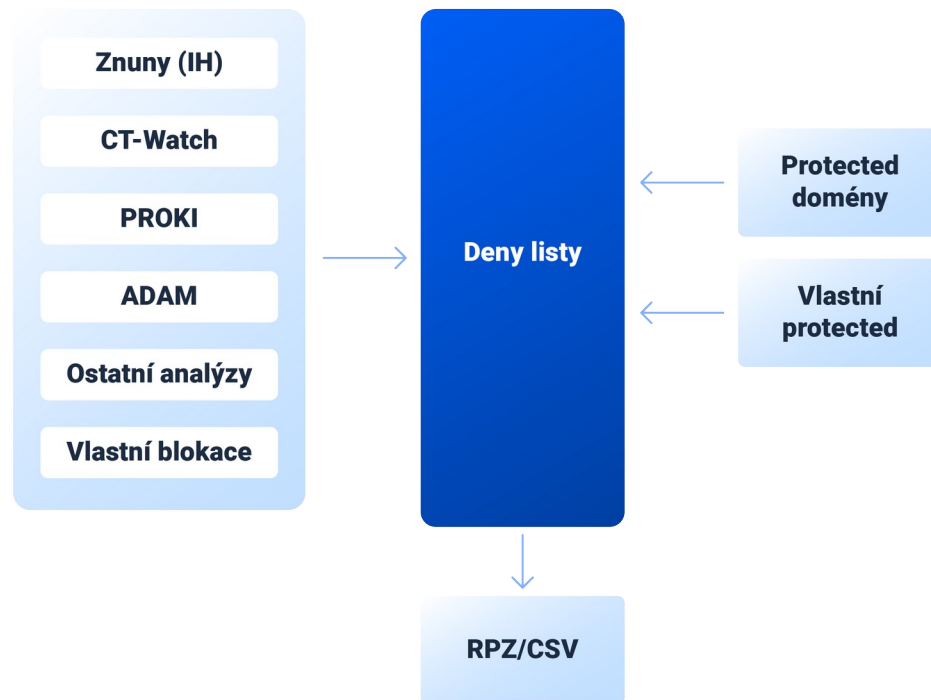
Domény Incidents Protectlist Statistika Historie změn

☐ Pouze vlastní záznamy organizace

[+ Přidat incidenty](#)

	Stav ▲	Domain ▲	Typ incidentu ▲	První výskyt ▼	
	blocked	ritualscosmetics.club		2026-09-18 15:29:37	
	blocked	z9opcf.top	Financial	2026-09-18 15:14:03	
	blocked	v4k9rx.lat	Financial	2026-09-18 15:14:03	
	blocked	h7qveb.sbs	Financial	2026-09-18 15:14:03	
	blocked	fr4kpz.casa	Financial	2026-09-18 15:14:03	
	blocked	d8wkmc.qpon	Financial	2026-09-18 15:14:03	
	blocked	b5y2qm.lat	Financial	2026-09-18 15:14:03	
	blocked	gls-grop.mgczechia.cz		2026-09-18 15:00:22	
	blocked	gov-infoevzp-cz.casa		2026-09-18 14:26:30	
	blocked	manager-wedos-service-id927527.artistadell...		2026-09-18 13:59:51	
	blocked	oakam.agrivoltaicoelevatodaterra.it		2026-09-18 13:59:03	
	blocked	easypark3.com		2026-09-18 13:59:00	
	blocked	easypark.yachts		2026-09-18 13:56:33	
	blocked	easypark.yachts		2026-09-18 13:56:33	

Jak to funguje



Kde dává nasazení smysl

- Internetový provider/operátor
- Úřady a státní instituce
- Privátní firmy

Ostatní bezpečnostní řešení

DNS Patrol

- Pokročilá ochrana na úrovni DNS
- Více než 30 detekčních modulů pro identifikaci hrozeb včetně phishingu, malwaru, DGA a DNS tunelování
- Individuální nastavení každého detekčního modulu v režimu Pass, Audit nebo Block
- Threat Intelligence a Deny Listy pro aktuální ochranu před známými škodlivými doménami
- Administrační portál, přehledný monitoring a pokročilé logování
- Aplikace pro ochranu zařízení mimo domácí síť (Android, iOS, Windows)
- Snadná integrace do SIEM
- Postaveno na výkonném open-source DNS serveru Knot resolver

Penetrační testování

- Realizuje tým CSIRT.CZ
 - Penetrační testování
 - Skener webu – testování webové aplikace na nejčastější zranitelnosti
 - Vulnerability scan s ručním testováním
 - Zátěžové testy
 - Testování odolnosti na různé typy DoS/DDoS útoků

VIP doména

- Anycast infrastruktura .CZ domény
- Robustní ochrana proti DDoS útokům
- Rychlá odezva kdekoliv na světě
 - 15 států na všech kontinentech
- Ochrana domény proti krádeži i lidské chybě

Router Turris Omnia

- Omnia NG
 - Distribuovaný dynamický firewall
 - Automatické aktualizace
 - Založeno na linuxu
 - WiFi 7
 - Porty SFP+ (10 Gbps) a RJ45 (2.5 Gbps)
 - Open Source
 - Děti ho milují :-)
 - Tombola!



Děkuji vám za pozornost!

Pavel Bašta

• 23.09.2026