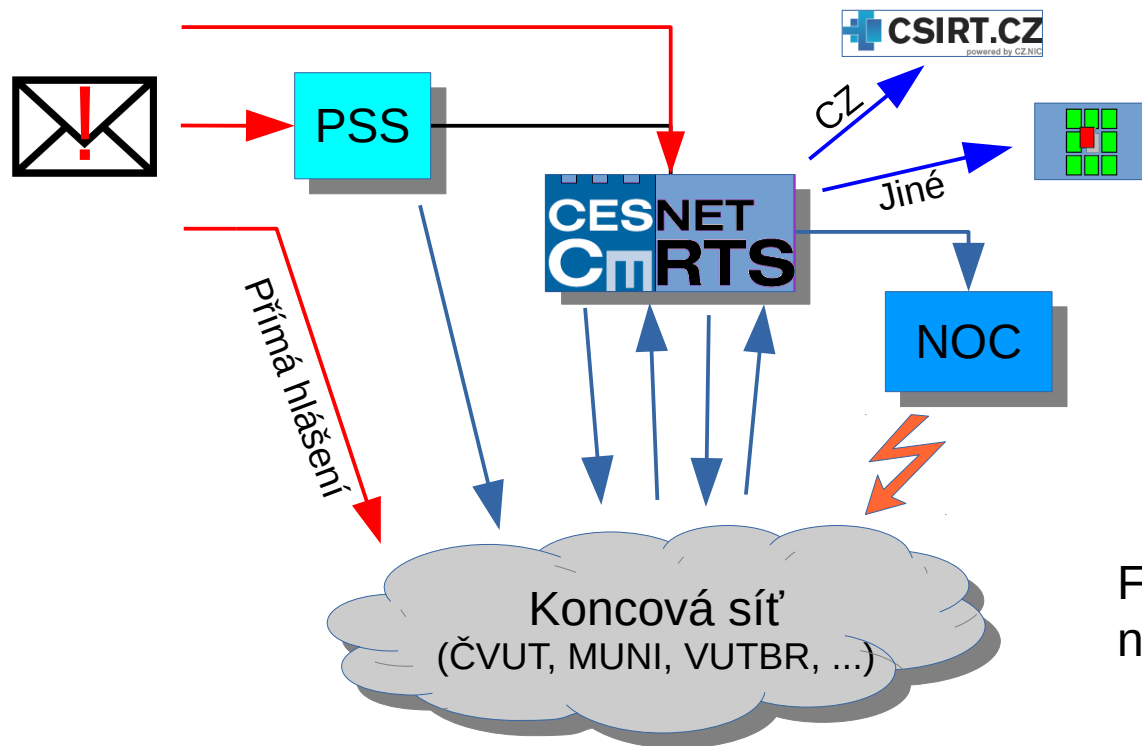


Plošný sběr, zpracování a distribuce bezpečnostních událostí





Funkce CSIRT týmu ale nemůže skončit pouze **reakcí**.





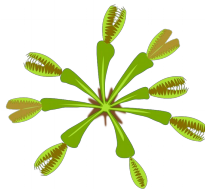
Sondy + Nemea



Cowrie



Dionaea



Fail2Ban



LaBrea



Shadowserver



network security incident exchange



NETWORK SECURITY HANDLING
AND RESPONSE PROCESS



- Platforma pro automatizované sdílení informací o incidentech
 - Zapisující konektory zasílají události do „fronty“
 - Čtoucí konektory odebírají vše, co se objevilo
- Kdo ostatním poskytuje data, dostane se k datům ostatních
- Jednotný formát

<https://warden.cesnet.cz>

<https://idea.cesnet.cz>



- Jednotné automatizované zpracování
- Zpřístupňuje informace lidským způsobem (bez nutnosti přístupu do Wardenu)
- Příklad: DDoS
 - Informace dorazí přes FTAS, sondy a LaBreu do Wardenu
 - Mentat zagreguje informace z různých zdrojů
 - ... a roztřídí podle zdrojů útoku
 - Jednotlivé organizace dostanou specifický report o svých IP

<https://mentat.cesnet.cz>

Date: Mon, 19 Apr 2021 21:20:06 +0200 (CEST)
 From: CESNET-CERTS Reporting <reporting@cesnet.cz>
 Subject: [M20210419SL-U4TEN] Nizká - Upozornění na možné problémy ve Vaší síti
 Reply-To: abuse@cesnet.cz

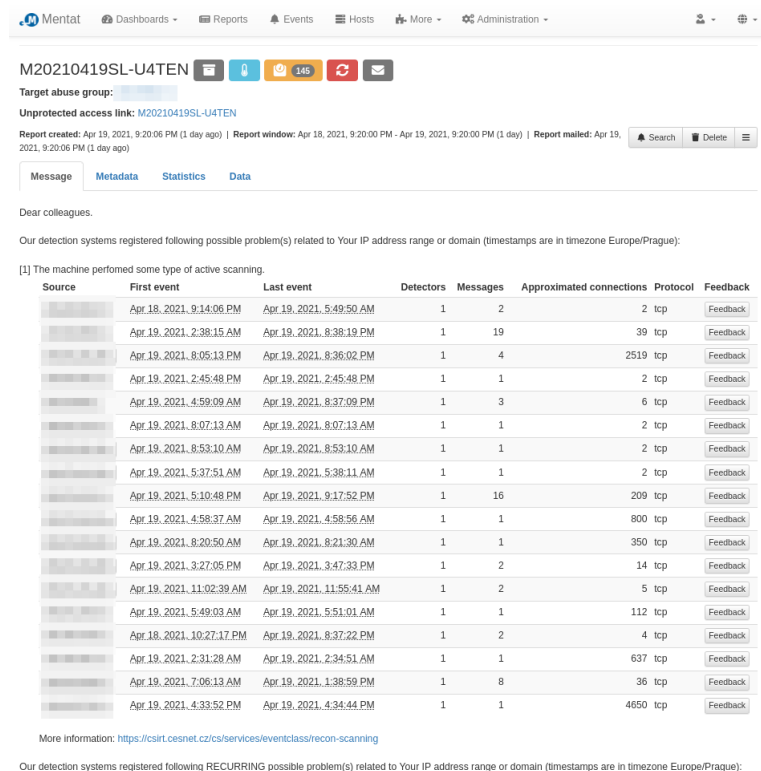
Vážení kolegyně.

Naše detekční systémy zaznamenaly následující možné problém(y) související s Vaším rozsahem IP adres nebo Vaší doménou (uvedené časy jsou v časové zóně Europe/Prague):

[1] Stroj se pokoušel o nějakou formu aktivního skenování.

Zdroj	První událost	Poslední událost	Detekt	Zpráva	Protokol
	18.04. 21:14:06	19.04. 05:49:50	1	2	tcp
	19.04. 02:38:15	19.04. 20:38:19	1	19	tcp
	19.04. 20:05:13	19.04. 20:36:02	1	4	tcp
	19.04. 14:45:48	19.04. 14:45:48	1	1	tcp
	19.04. 04:59:09	19.04. 20:37:09	1	3	tcp
	19.04. 08:07:13	19.04. 08:07:13	1	1	tcp
	19.04. 08:53:10	19.04. 08:53:10	1	1	tcp
	19.04. 05:37:51	19.04. 05:38:11	1	1	tcp
	19.04. 17:10:48	19.04. 21:17:52	1	16	tcp
	19.04. 04:58:37	19.04. 04:58:56	1	1	tcp
	19.04. 08:20:50	19.04. 08:21:30	1	1	tcp
	19.04. 15:27:05	19.04. 15:47:33	1	2	tcp
	19.04. 11:02:39	19.04. 11:55:41	1	2	tcp
	19.04. 05:49:03	19.04. 05:51:01	1	1	tcp
	18.04. 22:27:17	19.04. 20:37:22	1	2	tcp
	19.04. 02:31:28	19.04. 02:34:51	1	1	tcp
	19.04. 07:06:13	19.04. 13:38:59	1	8	tcp
	19.04. 16:33:52	19.04. 16:34:44	1	1	tcp

Více informací: <https://csirt.cesnet.cz/cs/services/eventclass/recon-scanning>



M20210419SL-U4TEN

Target abuse group: [M20210419SL-U4TEN](#)

Unprotected access link: [M20210419SL-U4TEN](#)

Report created: Apr 19, 2021, 9:20:06 PM (1 day ago) | Report window: Apr 18, 2021, 9:20:00 PM - Apr 19, 2021, 9:20:00 PM (1 day) | Report mailed: Apr 19, 2021, 9:20:06 PM (1 day ago)

Message Metadata Statistics Data

Dear colleagues,

Our detection systems registered following possible problem(s) related to Your IP address range or domain (timestamps are in timezone Europe/Prague):

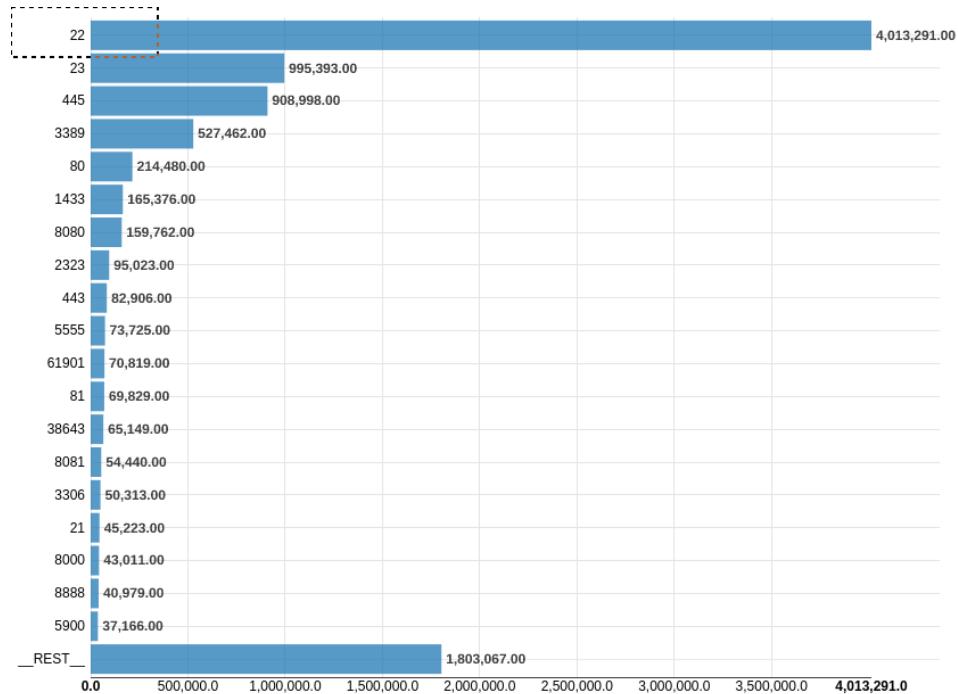
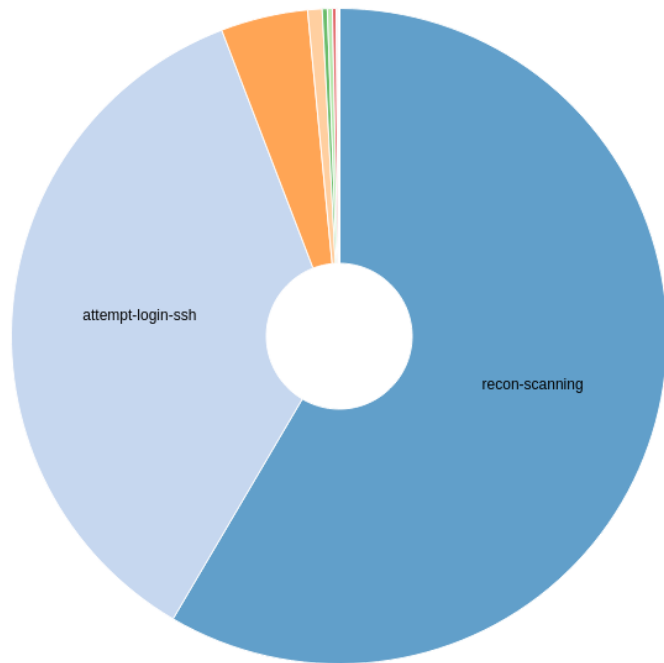
[1] The machine performed some type of active scanning.

Source	First event	Last event	Detectors	Messages	Approximated connections	Protocol	Feedback
	Apr 18, 2021, 9:14:06 PM	Apr 19, 2021, 5:49:50 AM	1	2	2	tcp	Feedback
	Apr 19, 2021, 2:38:15 AM	Apr 19, 2021, 8:38:19 PM	1	19	39	tcp	Feedback
	Apr 19, 2021, 8:05:13 PM	Apr 19, 2021, 8:36:02 PM	1	4	2519	tcp	Feedback
	Apr 19, 2021, 2:45:48 PM	Apr 19, 2021, 2:45:48 PM	1	1	2	tcp	Feedback
	Apr 19, 2021, 4:59:09 AM	Apr 19, 2021, 8:37:09 PM	1	3	6	tcp	Feedback
	Apr 19, 2021, 8:07:13 AM	Apr 19, 2021, 8:07:13 AM	1	1	2	tcp	Feedback
	Apr 19, 2021, 8:53:10 AM	Apr 19, 2021, 8:53:10 AM	1	1	2	tcp	Feedback
	Apr 19, 2021, 5:37:51 AM	Apr 19, 2021, 5:38:11 AM	1	1	2	tcp	Feedback
	Apr 19, 2021, 5:10:48 PM	Apr 19, 2021, 9:17:52 PM	1	16	209	tcp	Feedback
	Apr 19, 2021, 4:58:37 AM	Apr 19, 2021, 4:58:56 AM	1	1	800	tcp	Feedback
	Apr 19, 2021, 8:20:50 AM	Apr 19, 2021, 8:21:30 AM	1	1	350	tcp	Feedback
	Apr 19, 2021, 3:27:05 PM	Apr 19, 2021, 3:47:33 PM	1	2	14	tcp	Feedback
	Apr 19, 2021, 11:02:39 AM	Apr 19, 2021, 11:55:41 AM	1	2	5	tcp	Feedback
	Apr 19, 2021, 5:49:03 AM	Apr 19, 2021, 5:51:01 AM	1	1	112	tcp	Feedback
	Apr 18, 2021, 10:27:17 PM	Apr 19, 2021, 8:37:22 PM	1	2	4	tcp	Feedback
	Apr 19, 2021, 2:31:28 AM	Apr 19, 2021, 2:34:51 AM	1	1	637	tcp	Feedback
	Apr 19, 2021, 7:06:13 AM	Apr 19, 2021, 1:38:59 PM	1	8	36	tcp	Feedback
	Apr 19, 2021, 4:33:52 PM	Apr 19, 2021, 4:34:44 PM	1	1	4650	tcp	Feedback

More information: <https://csirt.cesnet.cz/cs/services/eventclass/recon-scanning>

Our detection systems registered following RECURRING possible problem(s) related to Your IP address range or domain (timestamps are in timezone Europe/Prague):

- recon-scanning
- attempt-login-ssh
- attempt-login-rdp
- avail-ddos
- None
- attempt-exploit
- attempt-login-telnet
- attempt-exploit-http
- anomaly-traffic
- intrusion-botnet-bot
- abusive-spam-spammer
- vulnerable-config-ne...
- vulnerable-config-nt...
- vulnerable-config-sn...
- vulnerable-config-do...
- vulnerable-config-ip...
- vulnerable-config-qo...



- Informace někdy nelze získat hromadně...
- ... nebo je vhodné do zpracování zařadit i jiné typy informací

GeoIP BGP+ASN whois



www.blocklist.de



Caida



CIRCL
BGP Rank



- Databáze škodlivých IP adres
 - Seznam (nám) známých zdrojů škodlivých aktivit
... a všeho, co o nich víme
(Primární zdroje – Warden, MISP)
- Data jsou obohacena o další informace z externích zdrojů
- Shrnutí všech informací do reputačního skóre
 - Predikce míry hrozby entity pro následující den
(strojové učení z dostupných dat)

<https://nerd.cesnet.cz>



IP search | IP detail | Data | Map

Timezone: local

Log in using: Local account EducAIN

Known IP addresses

IP prefix & Hostname suffix & Country code & ASN

Event category

Blacklist & Tag Min tag confidence

Sort by Reputation score ☐ Ascending

Max number of addresses

Results (20)

IP address	Hostname	ASN	Country	Events	Rep.	Other properties	Time added	Last event	Links
194.165.16.67	--	AS48721	MC	5839 8 3	0.992	Scanner blacklist_de-ssh abuseipdb	2021-03-19 06:48:57	2021-04-21 13:24:05	↗
194.165.16.42	--	AS48721	MC	11536 8 4	0.982	Scanner	2021-02-16 18:57:15	2021-04-21 13:19:31	↗
81.161.63.253	--	AS202984	CN	3061 6 4	0.961	Scanner Login attempts DShield uceprotect blacklist_de-ssh abuseipdb ciarmy	2020-11-07 14:01:19	2021-04-21 11:50:17	↗
171.67.71.100	research.esrg.stanford.edu	AS32	US	19689 6 2	0.953	Scanner ciarmy abuseipdb	2021-03-05 19:07:44	2021-04-21 14:00:50	↗
156.96.113.109	--	AS46664	US	1333 5 2	0.944	Scanner spamhaus-sbl spamhaus-drop spamhaus-pbl-isp abuseipdb	2021-03-09 00:28:14	2021-04-20 06:48:05	↗
89.248.165.134	recyber.net	AS202425	GB	30588 5 2	0.943	Scanner dshield ciarmy abuseipdb	2021-03-02 20:34:25	2021-04-21 13:59:28	↗
23.148.145.7	--	AS46664	US	4145 5 2	0.942	Scanner ciarmy	2021-03-01 17:21:55	2021-04-21 03:33:44	↗
81.161.63.100	--	AS202984	CN	3567 6 4	0.942	Scanner DShield Login attempts uceprotect blacklist_de-ssh abuseipdb ciarmy bruteforceblocker	2020-11-09 17:41:05	2 hours ago 13:28:51	↗
89.248.168.176	security.criminalip.com	AS29073 AS202425	NL	5821 5 2	0.937	Scanner DShield Research scanner dshield ciarmy abuseipdb	2019-05-21 07:09:03	2021-04-21 11:51:08	↗
221.181.185.19	--	AS56046	CN	3806 7 3	0.937	Scanner Login attempts DShield blacklist_de-ssh abuseipdb spamhaus-xbl-cbl uceprotect	2020-12-07 14:28:54	2021-04-21 08:22:25	↗
222.187.232.205	--	AS4134	CN	2038 4 2	0.937	Login attempts Scanner spamhaus-pbl sorbs-dul uceprotect blacklist_de-ssh abuseipdb spamhaus-xbl-cbl	2021-03-10 10:23:46	2021-04-21 13:56:49	↗
221.181.185.135	--	AS56046	CN	4370 7 3	0.937	Login attempts Scanner DShield blacklist_de-ssh abuseipdb spamhaus-xbl-cbl uceprotect	2020-12-07 14:46:24	2021-04-21 07:26:24	↗
81.161.63.103	--	AS202984	CN	2368 5 3	0.937	Scanner DShield Login attempts blacklist_de-ssh uceprotect bruteforceblocker abuseipdb ciarmy	2020-11-09 13:38:08	2021-04-21 12:21:59	↗
221.181.185.153	--	AS56046	CN	1271 4 2	0.937	Scanner Login attempts uceprotect blacklist_de-ssh abuseipdb spamhaus-xbl-cbl	2021-03-26 04:05:03	2021-04-21 07:31:33	↗
45.148.10.50	--	AS48090	NL	2743 6 4	0.937	Scanner abuseipdb ciarmy uceprotect spamhaus-xbl-cbl	2021-04-07 13:14:25	2021-04-21 14:00:03	↗
118.126.65.27	--	AS45090	CN	2863 5 2	0.936	Scanner ciarmy uceprotect	2021-02-05 09:12:49	2021-04-21 14:00:19	↗
209.141.45.200	joseph.kreed.org	AS53667	US	5016 7 3	0.935	Scanner abuseipdb ciarmy spamhaus-xbl-cbl uceprotect bruteforceblocker	2021-04-06 19:43:35	2021-04-20 17:03:36	↗
89.248.169.12	security.criminalip.com	AS202425	NL	2958 5 2	0.934	Scanner DShield Research scanner uceprotect ciarmy spamhaus-xbl-cbl	2019-05-10 09:15:28	2021-04-21 10:16:08	↗
92.63.197.71	--	AS60307 AS12695 AS204655 AS44446	RU	18353 5 2	0.933	Scanner DShield ciarmy dshield abuseipdb	2020-07-27 18:33:29	2021-04-21 13:57:29	↗
222.187.239.109	--	AS4134	CN	1142 4 2	0.932	Login attempts Scanner spamhaus-pbl sorbs-dul uceprotect blacklist_de-ssh abuseipdb spamhaus-xbl-cbl	2021-03-26 03:50:03	2021-04-21 12:27:12	↗

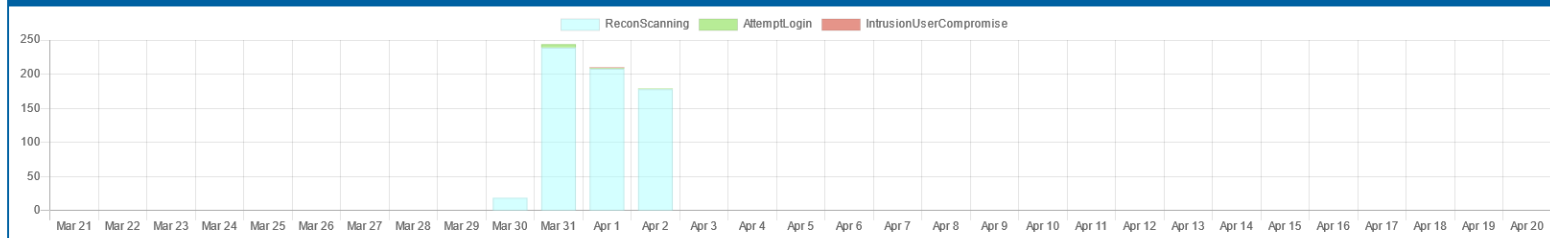
IP address 194.165.1 Odeslat dotaz

.432 194,165.1

Search at other sites:

Tags: **Scanner**

Event timeline ▲



Record time data	Geolocation	Blacklists	Network info	DShield	Shodan (more info)	Passive DNS (7)
ts_added 2021-03-30 23:04:11	 Monaco, Monaco	IP blacklists	Origin AS AS48721 - ADM-SERVICE-AS	N/A	Ports: 3389	PTR NODATA 2021-04-07 – 2021-04-07 (1x)
last_activity 2021-04-02 21:57:19	 Europe/Monaco	blocklist_de-ssh abuseipdb uceprotected bruteforceblocker	Address block (?) 194.165.		OS: Debian	PTR NODATA 2021-03-30 – 2021-04-20 (10230x)
ts_last_update 2021-04-02 21:57:28		Domain blacklists (?) none	BGP Prefix 194.165.			PTR NODATA 2021-04-01 – 2021-04-01 (1x)

All attributes ▼

Event details (≥100, only latest 100 shown)

AttemptLogin+Test  2021-04-20 13:24:35	Multiple unsuccessful login attempts on SSH Source(s): [194.165.1.1], Proto: [tcp], "ssh"; Target(s): Port: [22], Proto: [tcp], "ssh"; "CreateTime": "2021-04-20T11:25:09Z", "FlowCount": 12, "_CESNET": { "EventClass": "attempt-login-ssh", "EventSeverity": "medium", "SourceResolvedASN": [48721], "SourceResolvedCountry": ["MC"], "StorageTime": "2021-04-20T11:25:13.856865Z" }	1 cz. 1 cz.	[Nemea, brute_force_detector]
AttemptLogin+Test  2021-04-20 13:19:32	Multiple unsuccessful login attempts on SSH Source(s): [194.165.1.1], Proto: [tcp], "ssh"; Target(s): Port: [22], Proto: [tcp], "ssh"; "CreateTime": "2021-04-20T11:20:07Z", "FlowCount": 28, "_CESNET": { "EventClass": "attempt-login-ssh", "EventSeverity": "medium", "SourceResolvedASN": [48721], "SourceResolvedCountry": ["MC"], "StorageTime": "2021-04-20T11:20:17.385352Z" }	1 cz. 1 cz.	[Nemea, brute_force_detector]

- DNS odráží okamžitý stav – Passive DNS udržuje historii
 - Sleduje DNS transakce a staví databázi
- Příklady
 - Jaké všechny jmenné záznamy ukazují na IP a.b.c.d?
 - Jaké záznamy známe v doméně cesnet.cz?
 - Jak se měnilo doménové jméno v čase? Není to fast-flux?
 - Není příliš podobné existujícímu jménu? Nejde o phishing?

<https://passivedns.cesnet.cz>



PassiveDNS Search

Query:

Query type:

☒ IP
 ☐ domain
☐ domain & subdomains

Date limit:

Since: 03 / 29 / 2021

Until: 03 / 30 / 2021

Search

Elapsed time: 0.039217s

Page 1

IP	Domain	RTYPE	First seen	Last seen	Count	Source
78.128.211.46	www.cesnet.cz	A	2021-03-29 00:10:02.344920	2021-03-29 23:55:02.227642	256	ns.cesnet
78.128.211.46	www.cesnet.cz	A	2021-03-29 00:03:44.595298	2021-03-29 23:44:05.743237	170	adns2.cesnet.cz
78.128.211.46	www.cesnet.cz	A	2021-03-29 00:08:23.365356	2021-03-29 23:59:32.152469	202	adns1.cesnet.cz
78.128.211.46	cesnet.cz	A	2021-03-29 00:05:03.948795	2021-03-29 23:55:03.869946	157	adns1.cesnet.cz
78.128.211.46	cesnet.cz	A	2021-03-29 01:57:39.927095	2021-03-29 21:14:09.949594	20	ns.cesnet
78.128.211.46	cesnet.cz	A	2021-03-29 10:45:44.954685	2021-03-29 22:48:07.111438	6	adns2.cesnet.cz
46.211.128.78.in-addr.arpa	www.cesnet.cz	PTR	2021-03-29 00:52:25.640564	2021-03-29 22:32:58.246510	25	adns1.cesnet.cz
46.211.128.78.in-addr.arpa	www.cesnet.cz	PTR	2021-03-29 00:56:14.486300	2021-03-29 23:30:15.149114	15	adns2.cesnet.cz
NODATA	46.211.128.78.in-addr.arpa	A	2021-03-29 00:56:14.485409	2021-03-29 21:41:20.626957	10	adns2.cesnet.cz
NODATA	46.211.128.78.in-addr.arpa	A	2021-03-29 00:52:25.640190	2021-03-29 23:27:03.394540	16	adns1.cesnet.cz

[Previous page](#) [Next page](#)

celanet.cz
z2.cesnet-ca.cz
cesl.cz
ocsp.cesnet-ca.cz
net-cz.cz
net.cz
rvsnet.cz
expresnet.cz
cesnet.cz.lampanet.net
cesnet.ca.cz
fedra.cesnet-ca.cz
r150.cesne.cz
cesnet-ca.cz
cesnet-gw1.hknet.cz

wsnet.cz
cernet.cz
hsnet.cz
tik.cesnet.net
cesnz.net
tul.cesnet.net
du.cesnet.cf
wisnet.cz
crsnet.cz
ceznet.cz
casnet.cz
cesnet-gw2.hknet.cz
notesnet.cz
cesnet.cf
ocsp1.cesnet-ca.cz
cesnet.cz.didata.cz

caas.cesne.cz
bvsnet.cz
crt.cesnet-ca.cz
cesnet.pki.cz
cesnet-certs.cz
vesnet.cz
cesnet.hk
notify.cesnet-ca.cz
itsnet.cz
cesr.cz
cesnet2.cz
lai.cesnet-ca.cz
cesnet-gw3.hknet.cz
cesnet.co.za



- **Warden**
 - ~ **1.6** milionu událostí za den
 - (pouze **0.4 %** CESNET + partneři)
 - **26** zdrojů
- **Mentat**
 - ~ **30** reportů za týden
 - pro ~ **300** organizací
- **NERD**
 - ~ **800 000** IP
 - ~ **115 000** BGP
 - ~ **16 000** ASN
 - ~ **38 000** CIDR
 - ~ **16 000** organizací
- **PassiveDNS**
 - ~ **129** milionů záznamů za den



- Většina služeb je dostupná veřejně
 - Některé jen pro členy bezpečnostních týmů
mentat-info@cesnet.cz
 - Některé s podmínkami („dejte, dáme“ :))
warden-info@cesnet.cz

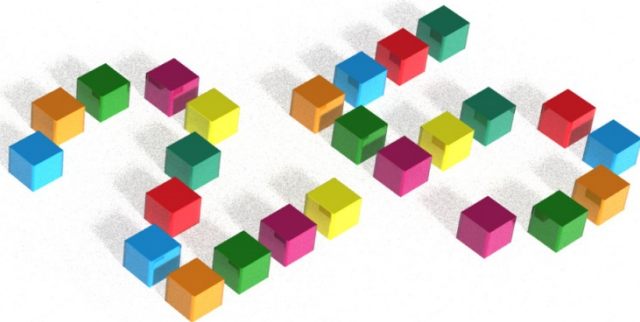
- Většina dat je také přístupná přes API

- Rádi pohovoříme o požadavcích, zvážíme zakomponování úprav, nebojte se ozvat



- **Zapojte se do Wardenu**
- Máte honepot? IDS/IPS?
- Máte logy a fail2ban?
- Podívejte se na <https://warden.cesnet.cz> a ozvěte se na warden-info@cesnet.cz





Děkuji za pozornost!

