ioc2rpz

ioc2rpz community

here threat intelligence meets DNS

Vadim Pavlov, owner/developer/admin/maintainer etc

2023-06-15

Agenda

- Introduction
- WTH is ioc2rpz community and why I'm doing that?
- Behind the scenes
- Some cool statistics
- Roadmap (as usual not committed)
- Q & A

Introduction

- 30+ years in IT
  - my first PC - ZX Spectrum's clone
  - Masters degree in Computer Science
- 10.5 years deep dive in DNS & DNS Security
- B1TD & Ecosystem PM @ Infoblox
- Created Infoblox's DEX and SA portals
- Created ioc2rpz and related projects
- Like to travel, try local food and wear "stupid" t-shirts

WTH ioc2rpz and ioc2rpz community?

ioc2rpz - a technology, DNS server for Response Policy Zones (RPZ)* distribution. Open source, available on github (http://ioc2rpz.com).

ioc2rpz community - a service which was built based on the ioc2rpz technology. It provides OSINT RPZ/DNS Firewall feeds free of charge (https://ioc2rpz.net).

* - **D**omain **N**ame **S**ervice **R**esponse **P**olicy **Z**ones (DNS RPZ) is a method that allows a nameserver administrator to overlay custom information on top of the global DNS to provide alternate responses to queries. Another generic name for the DNS RPZ functionality is "DNS firewall".

RPZ was presented @ BlackHat & DefCon in 2010 by Paul Vixie and Vernon Schryver

What is ioc2rpz?

ioc2rpz - DNS server

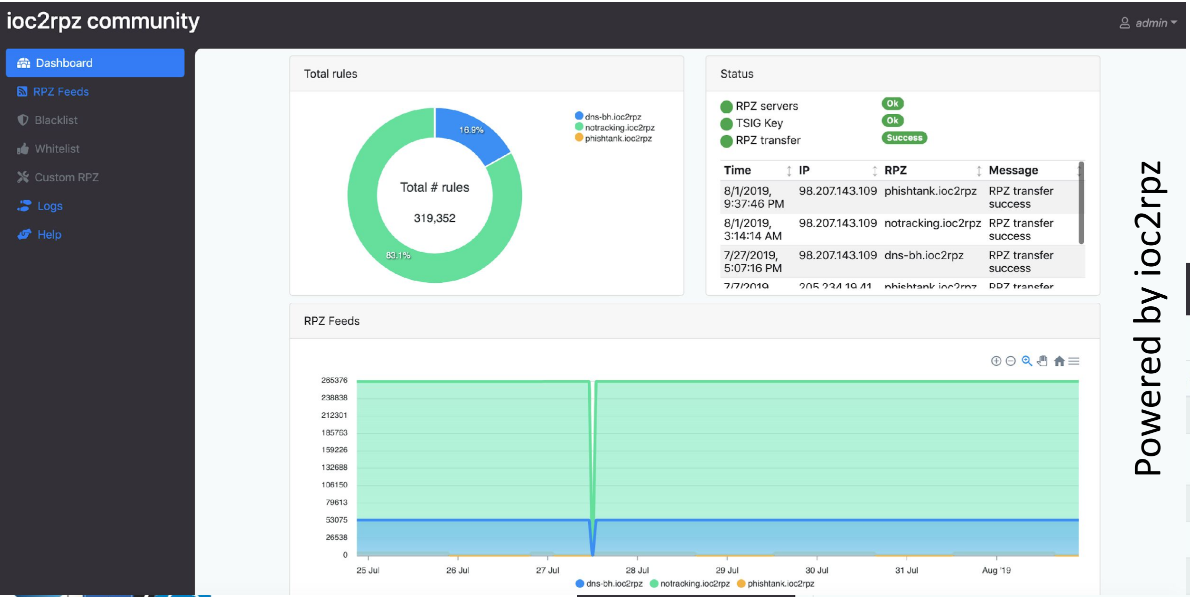
http://ioc2rpz.com

ioc2rpz.gui - Web interface

https://github.com/Homas/ioc2rpz.gui

ioc2rpz Community

https://ioc2rpz.net



ioc2rpz community

Total rules

Total # rules

319,352

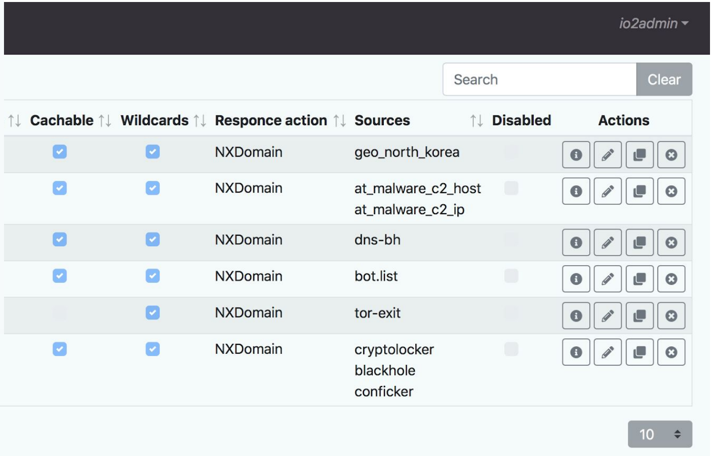
Status

● RPZ servers	Ok
● TSIG Key	Ok
● RPZ transfer	Success

Time	IP	RPZ	Message
8/1/2019, 9:37:46 PM	98.207.143.109	phishtank.ioc2rpz	RPZ transfer success
8/1/2019, 3:14:14 AM	98.207.143.109	notracking.ioc2rpz	RPZ transfer success
7/27/2019, 5:07:16 PM	98.207.143.109	dns-bh.ioc2rpz	RPZ transfer success
7/7/2019	205.234.19.41	phishtank.ioc2rpz	RPZ transfer

RPZ Feeds

Powered by ioc2rpz



				Cachable	Wildcards	Responce action	Sources	Disabled	Actions
				☑	☑	NXDomain	geo_north_korea	□	
				☑	☑	NXDomain	at_malware_c2_host at_malware_c2_ip	□	
				☑	☑	NXDomain	dns-bh	□	
				☑	☑	NXDomain	bot.list	□	
				□	☑	NXDomain	tor-exit	□	
□	dga.ioc2rpz	srv_1	fqdn	☑	☑	NXDomain	cryptolocker blackhole conficker	□	

TXT

REST API

Own TI

ioc2rpz

Response Policy Zones/DNS Firewall

Domain **N**ame **S**ervice **R**esponse **P**olicy **Z**ones (DNS RPZ) is a method that allows a nameserver administrator to overlay custom information on top of the global DNS to provide alternate responses to queries. Another generic name for the DNS RPZ functionality is "DNS firewall".

More info you can find at https://dnsrpz.info/ and in the following drafts: draft-vixie-dnsop-dns-rpz-00, draft-vixie-dns-rpz-04

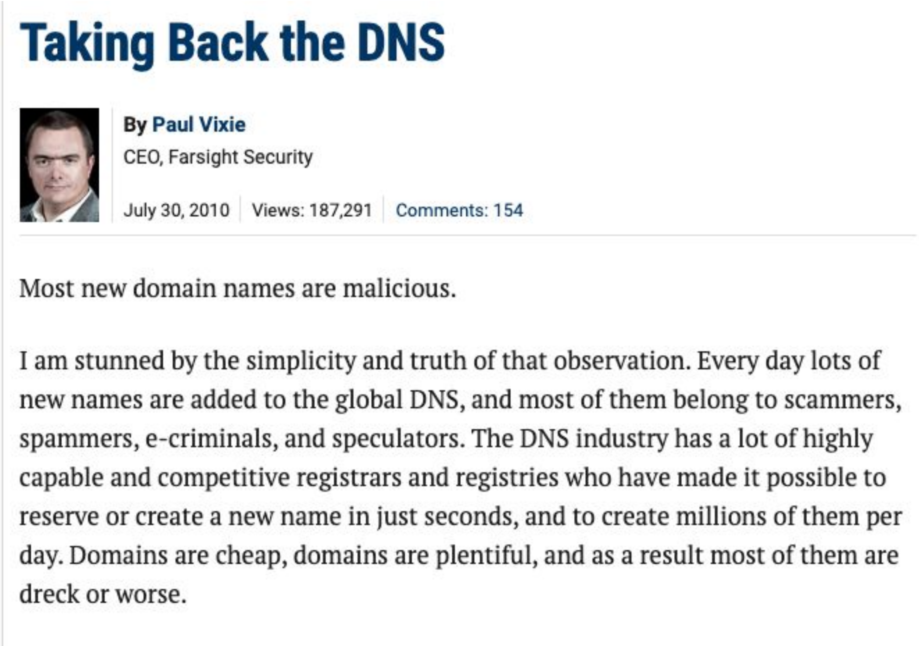
Open source DNS servers with RPZ support:

- ISC Bind
- Knot (partial support)
- PowerDNS

Commercial DNS servers with RPZ support:

- Akamai AnswerX
- BlueCat
- EfficientIP
- Infoblox

Celebrating 13 years of the RPZ technology



Taking Back the DNS

By Paul Vixie
CEO, Farsight Security

July 30, 2010 | Views: 187,291 | Comments: 154

Most new domain names are malicious.

I am stunned by the simplicity and truth of that observation. Every day lots of new names are added to the global DNS, and most of them belong to scammers, spammers, e-criminals, and speculators. The DNS industry has a lot of highly capable and competitive registrars and registries who have made it possible to reserve or create a new name in just seconds, and to create millions of them per day. Domains are cheap, domains are plentiful, and as a result most of them are dreck or worse.

The first public announcement of DNS RPZ was at **Black Hat on 29 July 2010** and then at DefCon on 30 July 2010

Thanks to:

- Paul Vixie
- Vernon Schryver

But why?

10.5 years ago when I joined Infoblox - no free RPZ feeds were available

6 years ago when I built ioc2rpz Infoblox didn't offer custom feeds

ioc2rpz community was built for:

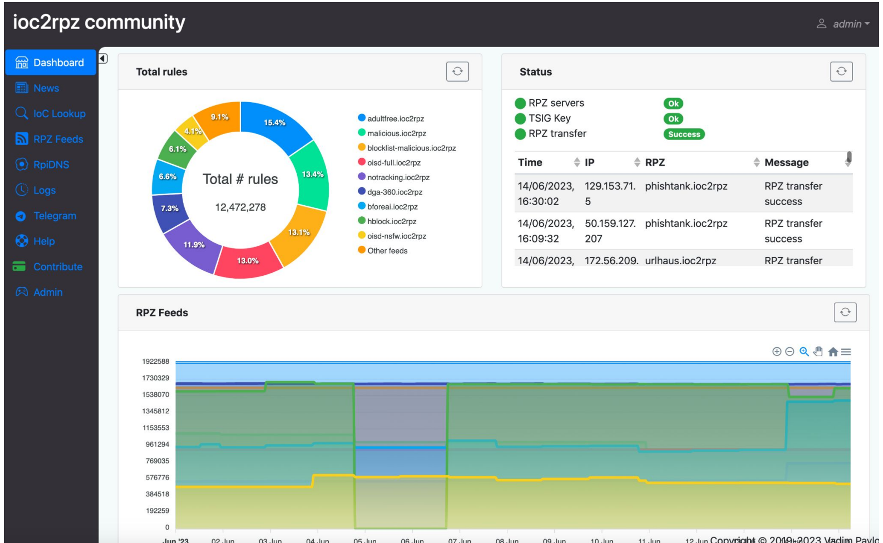
- base level security for everyone (by reducing threat surface, you reduce your threats)
- promote DNS Firewall technology
- promote ioc2rpz technology (was presented @ DefCon and BlackHat)
- and just for fun (to run own DNS server in production, except Infoblox's SA portal)

Do Good, And Then Throw It Into The Sea

Architecture

ioc2rpz community is kind of GDPR compliant - all data processed and stored in EU (except S3 :)

- ioc2rpz community site:
    - the portal;
    - ioc2rpz for community feeds;
    - ioc2rpz for custom feeds;
    - ioc2rpz.gui;
    - monitoring & reporting
- For AWS Route53 DNS Firewall
    - S3 + Lambdas
- OSINT and donated feeds "as is"



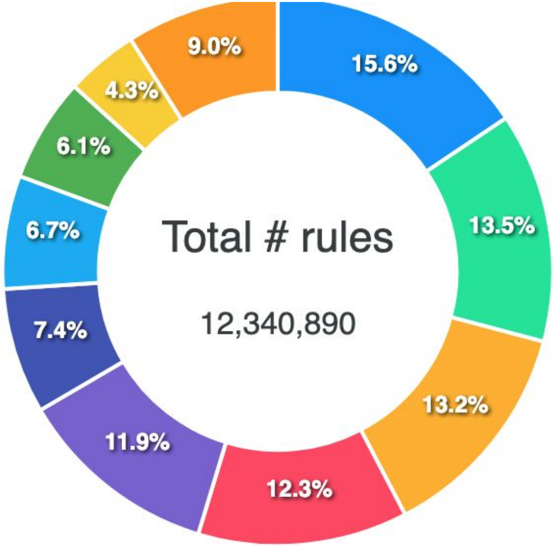
● RPZ servers Ok
● TSIG Key Ok
● RPZ transfer Success

Time	IP	RPZ	Message
14/06/2023, 16:30:02	129.153.71.5	phishtank.ioc2rpz	RPZ transfer success
14/06/2023, 16:09:32	50.159.127.207	phishtank.ioc2rpz	RPZ transfer success
14/06/2023,	172.56.209.	urlhaus.ioc2rpz	RPZ transfer

Copyright © 2019-2023 Vadim Pavlo

ioc2rpz Community Feeds

- Feeds provided "as is" (not curated)
- OSINT and donated feeds with focus on:
  - No ads, no tracking
  - Malware & Phishing protection
  - Adult content filtration
  - Immediate response (including no registration access)
    - COVID-19 - deprecated
    - War in Ukraine - replaced by Infoblox malicious
    - Earthquake in Türkiye - replaced by Infoblox malicious
  - Donated: Infoblox (malicious & phishing), before.ai (predicted), shresta.it (NRD)
- Custom Feeds:
  - Country & TLD block
  - Source*



Some statistics - feeds

19 community feeds

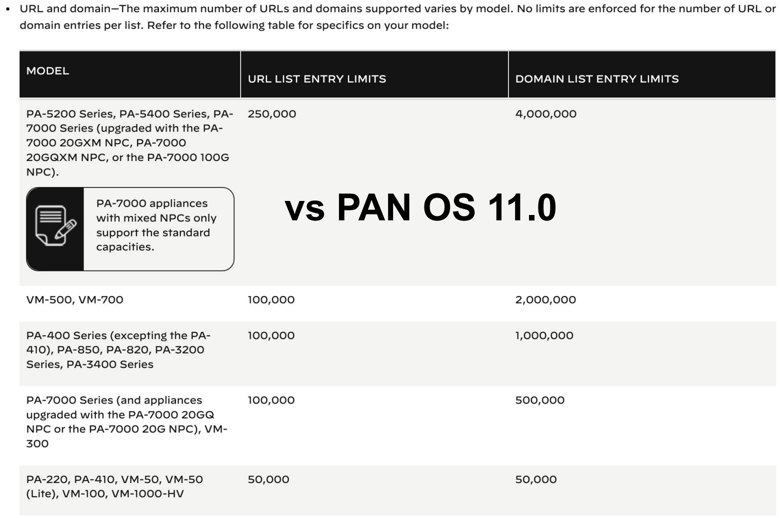
11 custom feeds (country & TLD)

TOP 5 feeds (by popularity):

1. dga-360.ioc2rpz - 900k rules
2. phishtank.ioc2rpz - 35k rules
3. blocklist-malicious.ioc2rpz - 1.6m rules
4. urlhaus.ioc2rpz - 1.5k rules
5. doh.ioc2rpz - 170 rules

TOP 5 feeds (by size):

1. adultfree.ioc2rpz - 1.9m rules
2. malicious.ioc2rpz - 1.7m rules
3. blocklist-malicious.ioc2rpz - 1.6m rules
4. notracking.ioc2rpz - 1.5m rules
5. oisd-full.ioc2rpz - 1.5m rules



- URL and domain—The maximum number of URLs and domains supported varies by model. No limits are enforced for the number of URL or domain entries per list. Refer to the following table for specifics on your model:

MODEL	URL LIST ENTRY LIMITS	DOMAIN LIST ENTRY LIMITS
PA-5200 Series, PA-5400 Series, PA-7000 Series (upgraded with the PA-7000 20GXM NPC, PA-7000 20GQXM NPC, or the PA-7000 100G NPC). PA-7000 appliances with mixed NPCs only support the standard capacities.	250,000	4,000,000
VM-500, VM-700	100,000	2,000,000
PA-400 Series (excepting the PA-410), PA-850, PA-820, PA-3200 Series, PA-3400 Series	100,000	1,000,000
PA-7000 Series (and appliances upgraded with the PA-7000 20GQ NPC or the PA-7000 20G NPC), VM-300	100,000	500,000
PA-220, PA-410, VM-50, VM-50 (Lite), VM-100, VM-1000-HV	50,000	50,000

vs PAN OS 11.0

Some statistics - my household

Top 5 Feeds	Count
notracking.ioc2rpz	124,903
oisd-full.ioc2rpz	94,152
doh.ioc2rpz	11,194
bogons-ipv4.ioc2rpz	83
local.ioc2rpz	71

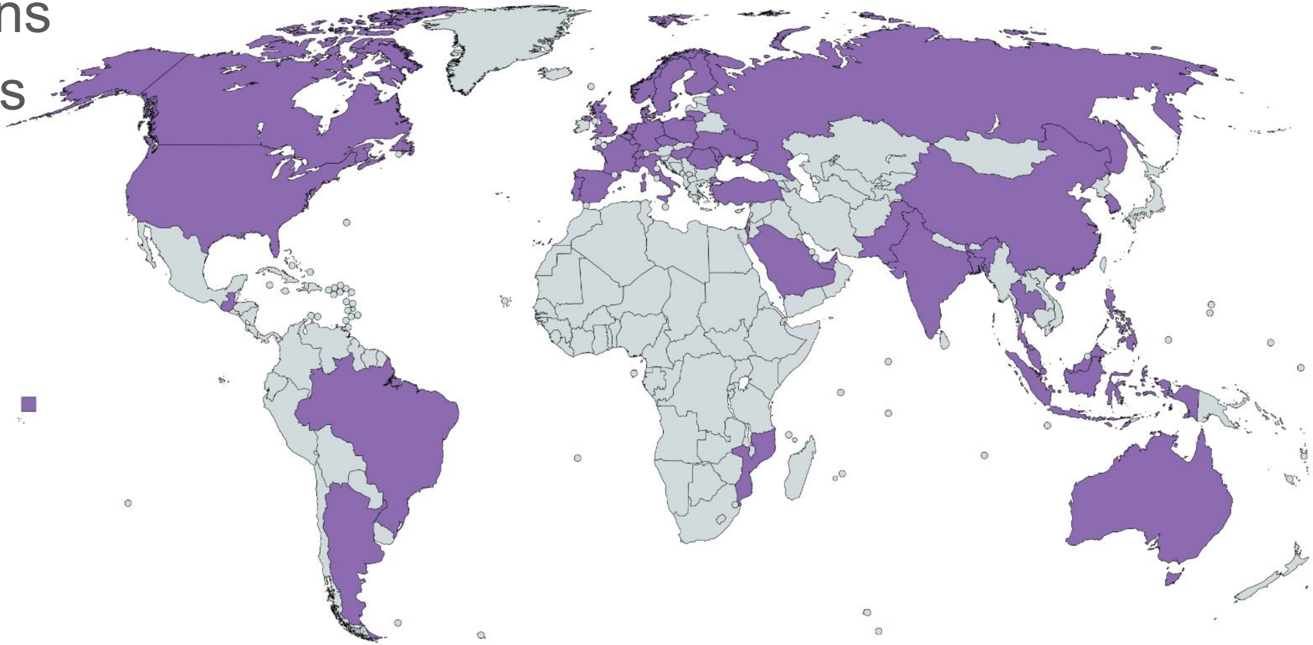
Top 5 blocked devices	Count
Sony TV	75,542
Amazon Fire HD 8	44,666
Samsung TV	43,019
Samsung S22	23,696
Apple iPhone	16,617

Top 5 blocked requests	Count
sanalytics.disneyplus.com	31,263
lcprd1.samsungcloudsolution.net	27,400
ephemeralcounters.api.roblox.com	14,564
ecsv2.roblox.com	14,344
ssl.google-analytics.com	13,045

Top 5 request types	Count
A	826,953
AAAA	680,945
PTR	441,434
TYPE65	254,310
SOA	4,945

Some statistics - accounts

- protected users - unknown
- 120 active accounts (pull feeds daily)
- from 155 locations
- from 47 countries

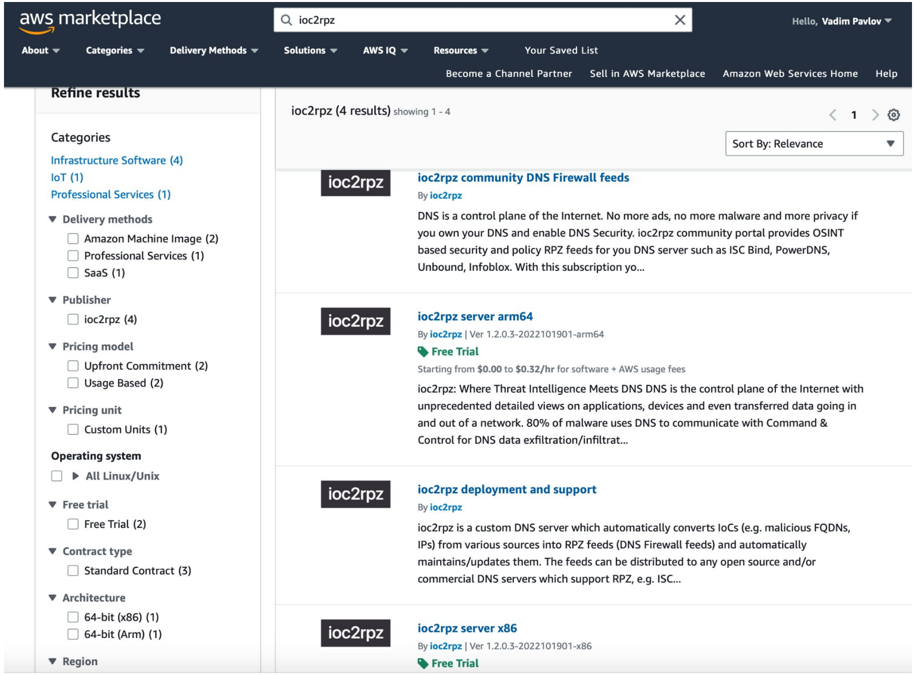


Not committed roadmap

- RpiDNS:
  - Docker container image
  - Ubuntu 22 support
  - RPZ feeds management from UX/UI
  - Service notifications
- ioc2rpz community - remove account
- PiHole support
- Custom feeds by source

Want to run yourself?

- Docker container
  - https://github.com/Homas/ioc2rpz.dc
- AWS Marketplace
  - https://aws.amazon.com/marketplace/search/results?searchTerms=ioc2rpz
- ioc2rpz & ioc2rpz.gui on bare metal



Refine results

Categories

Infrastructure Software (4)
IoT (1)
Professional Services (1)

Delivery methods
- □ Amazon Machine Image (2)
- □ Professional Services (1)
- □ SaaS (1)

Publisher
- □ ioc2rpz (4)

Pricing model
- □ Upfront Commitment (2)
- □ Usage Based (2)

Pricing unit
- □ Custom Units (1)

Operating system
- □ All Linux/Unix

Free trial
- □ Free Trial (2)

Contract type
- □ Standard Contract (3)

Architecture
- □ 64-bit (x86) (1)
- □ 64-bit (Arm) (1)

Region

ioc2rpz (4 results) showing 1 - 4

Sort By: Relevance

ioc2rpz community DNS Firewall feeds
By ioc2rpz
DNS is a control plane of the Internet. No more ads, no more malware and more privacy if you own your DNS and enable DNS Security. ioc2rpz community portal provides OSINT based security and policy RPZ feeds for you DNS server such as ISC Bind, PowerDNS, Unbound, Infoblox. With this subscription yo...

ioc2rpz server arm64
By ioc2rpz | Ver 1.2.0.3-2022101901-arm64
Free Trial
Starting from **$0.00** to **$0.32/hr** for software + AWS usage fees
ioc2rpz: Where Threat Intelligence Meets DNS DNS is the control plane of the Internet with unprecedented detailed views on applications, devices and even transferred data going in and out of a network. 80% of malware uses DNS to communicate with Command & Control for DNS data exfiltration/infiltrat...

ioc2rpz deployment and support
By ioc2rpz
ioc2rpz is a custom DNS server which automatically converts IoCs (e.g. malicious FQDNs, IPs) from various sources into RPZ feeds (DNS Firewall feeds) and automatically maintains/updates them. The feeds can be distributed to any open source and/or commercial DNS servers which support RPZ, e.g. ISC...

ioc2rpz server x86
By ioc2rpz | Ver 1.2.0.3-2022101901-x86
Free Trial

Q & A

ioc2rpz

Thank YOU!

Vadim Pavlov

ioc2rpz[at]gmail.com
https://www.linkedin.com/in/vadim-pavlov/