Система доменных имен как источник информации

Евгений Сухов
2022

Данные

Доменные имена

Ресурсные записи

Результат резолва

Тип хостинга

Время и частота обращений

Источник запросов

Whois/время регистрации

Whois/владелец

Whois/регистратор

Сертификаты

Синкхол

Регистрация известных вредоносных доменов

«Направление» на подконтрольные сервера

Мониторинг

Аналитика

Оповещение

Мониторинг чужих синкхолов

Всего ~ 500к

Активны ~ 70к

005304d1ec3c417642a81b5b96d2231b.info	TI_SINKHOLED_microsoftinternetsafety
005581064db5f9eedb3e14082282c3d1.info	TI_SINKHOLED_microsoftinternetsafety
0058ae46c08b3be037189c5184689734.info	TI_SINKHOLED_microsoftinternetsafety
00599.be-24.ru	TI_SINKHOLED_honeybot_whois
005a7ff3b3b5f0262b28bc868ba7477c.info	TI_SINKHOLED_microsoftinternetsafety
005c59e2b70e304a0ac4a08e2629bec1.info	TI_SINKHOLED_microsoftinternetsafety
005ed7545de4a69fec20fd0fae92a94c.info	TI_SINKHOLED_microsoftinternetsafety
006094bc374ac8e39bc0af4fdb2c3fbd.info	TI_SINKHOLED_microsoftinternetsafety
0062000333e1d28ff6986188cdb7da59.info	TI_SINKHOLED_microsoftinternetsafety
0065d409938224543a0cc9453e8ae8c5.info	TI_SINKHOLED_microsoftinternetsafety
0066872129739617f19ecb975ba73d68.info	TI_SINKHOLED_microsoftinternetsafety
006815c8d93bd05ac902ded06dc0a5f4.info	TI_SINKHOLED_microsoftinternetsafety
006912bce46d7e9af769e966e0fdec84.info	TI_SINKHOLED_microsoftinternetsafety
0069285d146f8e60663ee3090605e0e1.info	TI_SINKHOLED_microsoftinternetsafety
006b92a381d4.com	TI_SINKHOLED_shadowserver
006bee3a8f0cf2ba3386e5ae439af0d3.info	TI_SINKHOLED_microsoftinternetsafety
006ef85f6e47.com	TI_SINKHOLED_sinkhole_fkie
007652730d54.net	TI_SINKHOLED_shadowserver
0076ffc.be-24.ru	TI_SINKHOLED_honeybot_whois
0077127d34cd630e9bfdad10ec1fa11c.info	TI_SINKHOLED_microsoftinternetsafety
007966f64323067577b290928705b9d2.info	TI_SINKHOLED_microsoftinternetsafety

DGA

Реверс-инжиниринг

Машинное обучение

Статистический анализ

~ 300к доменов

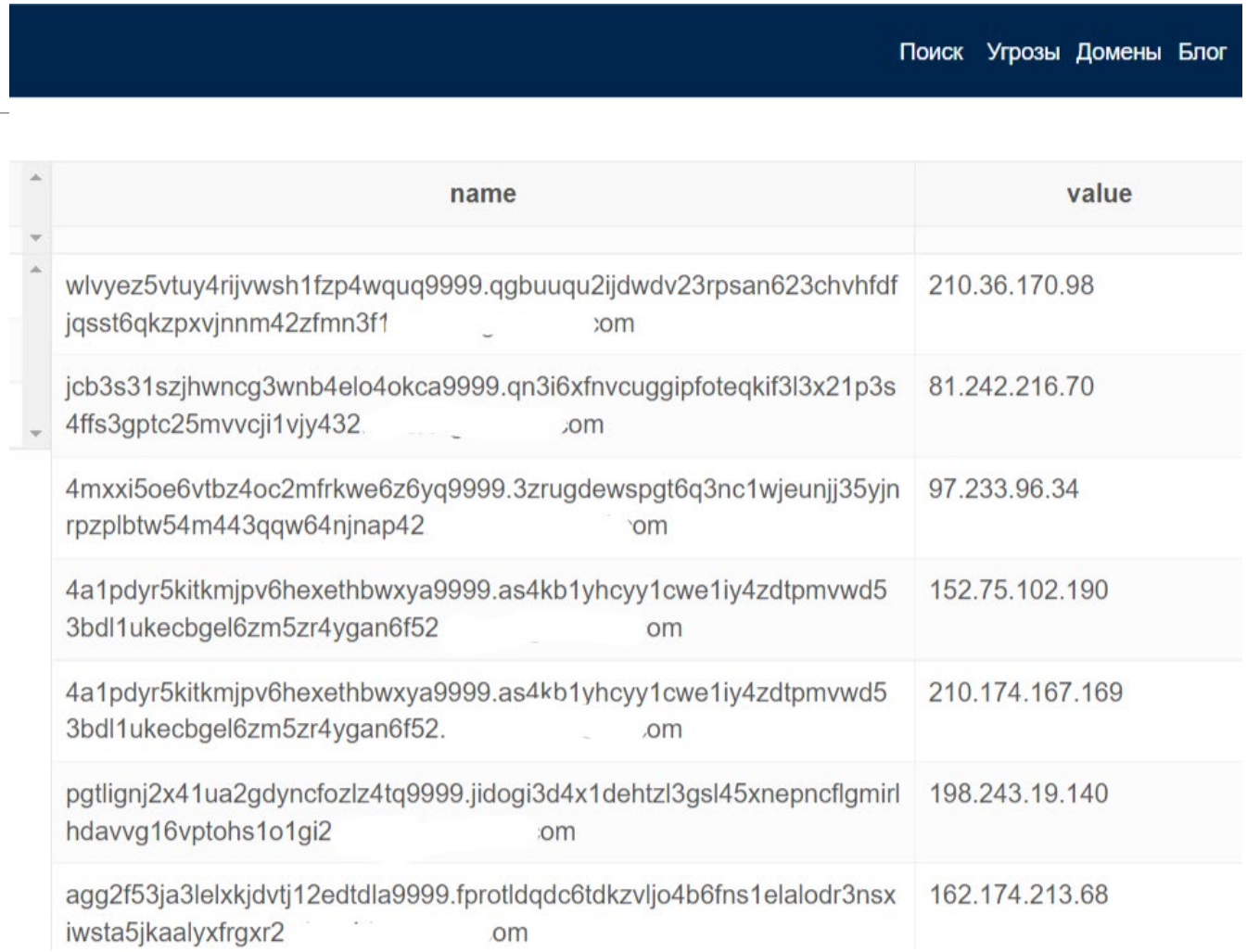
aqrqnaxc.info	TI_DGA_Pykspa
aqsaua.biz	TI_DGA_Pykspa
aqsgieiq.info	TI_DGA_Pykspa
aqsgooyy.org	TI_DGA_Pykspa
aqsqcyeoya.biz	TI_DGA_Pykspa
aqsweueoya.biz	TI_DGA_Pykspa
aqsxhunvwrgp.net	TI_DGA_Pykspa
aqsyiw.org	TI_DGA_Pykspa
aqthxkhlprfidxmyj.net	TI_DGA_Ranbyus
aqtoblarcbfqch.net	TI_DGA_Ranbyus
aqtwrpbrjvqeafyno.net	TI_DGA_Ranbyus
aquaisiugkeq.net	TI_DGA_Pykspa
aquoyusgqy.org	TI_DGA_Pykspa
aquykyeoya.info	TI_DGA_Pykspa
aqwdtfwacecj.net	TI_DGA_Pykspa
aqweey.net	TI_DGA_Pykspa
aqwqig.com	TI_DGA_Pykspa
aqwryk.info	TI_DGA_Pykspa
aqwzca.net	TI_DGA_Pykspa
aqxiuapam.biz	TI_DGA_Pitou
aqxiuapap.biz	TI_DGA_Pitou
aqxiuapaq.biz	TI_DGA_Pitou
aqxiuapas.biz	TI_DGA_Pitou

DNS туннели

Скрытый обмен данными

Коммуникации с C2

Статистический анализ



Cybersquatting

Мониторинг регистрируемых доменов

Сбор и мониторинг поддоменов

Анализ(ML, Regexp, Links)

Оповещение

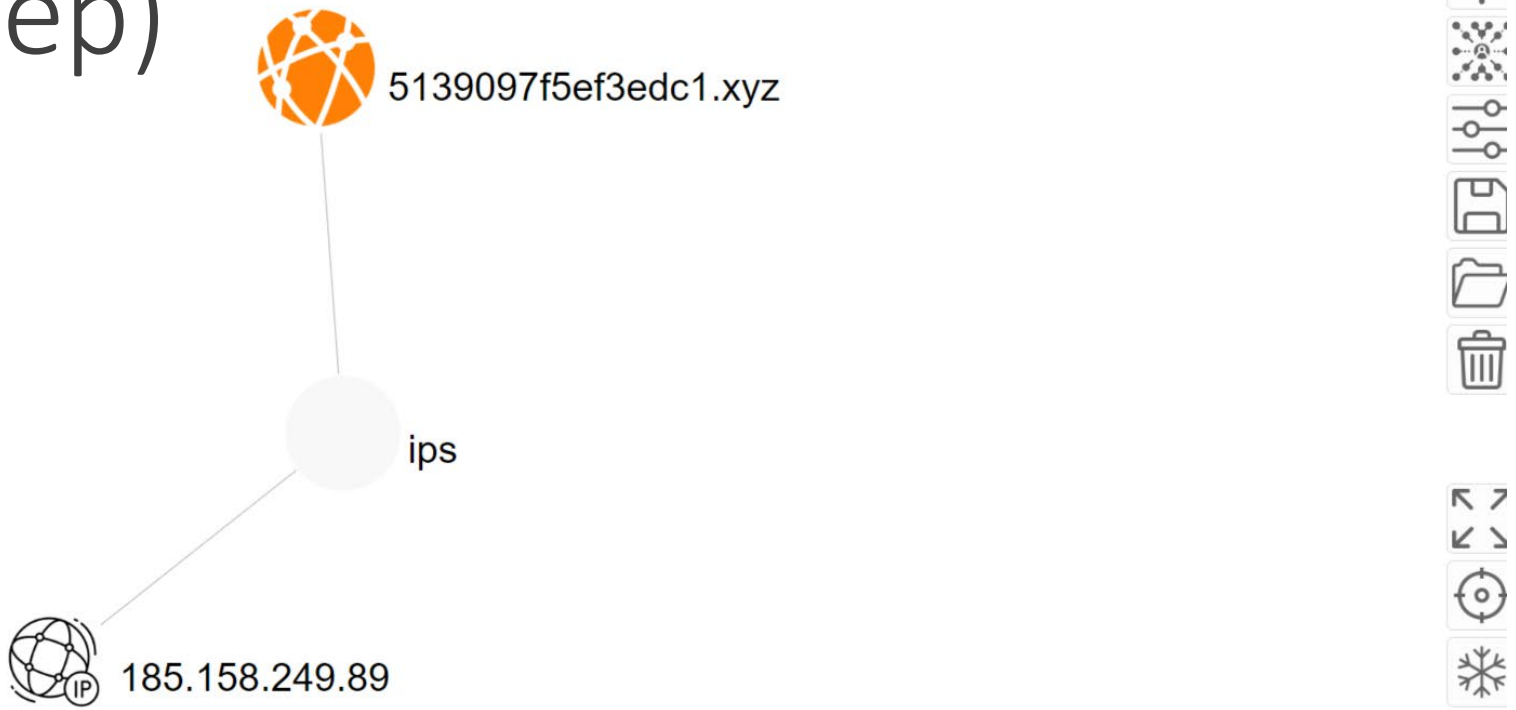
До 100 новых имен в день в Российском сегменте

До 500 новых имен в международном

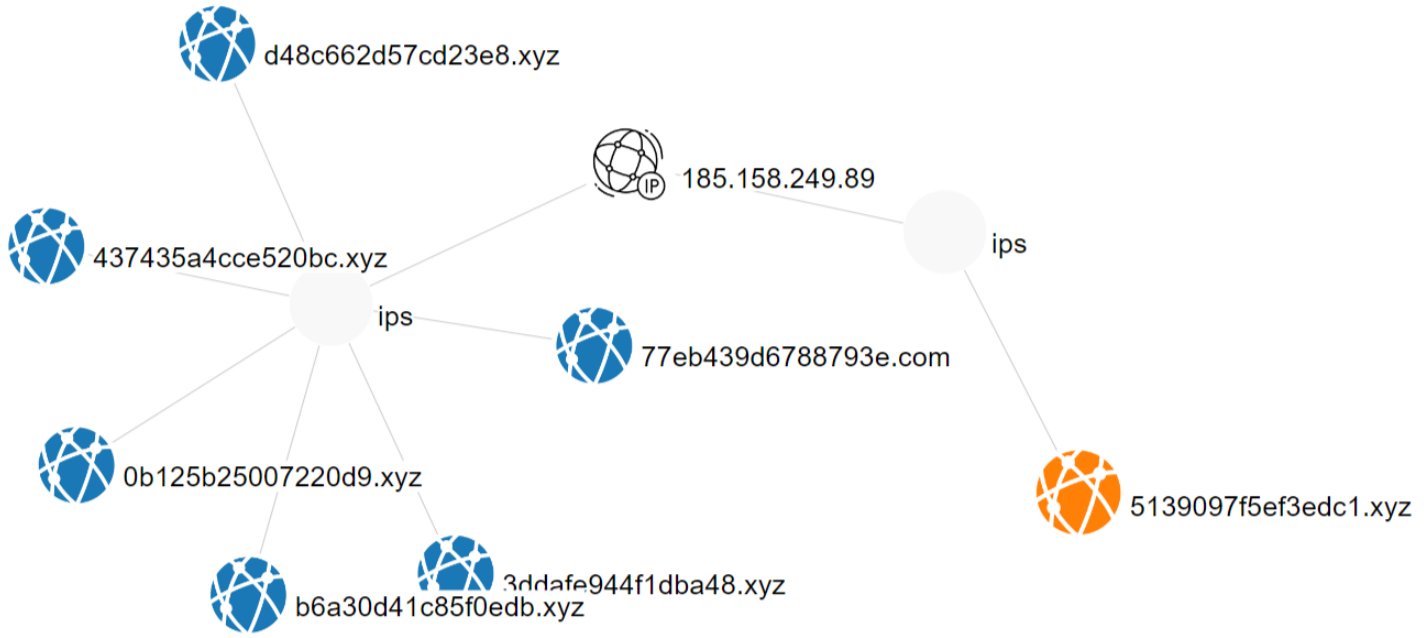
first_date	name
2022-09-27	avito.id8422.ru
2022-09-27	order5574205.xyz
2022-09-27	id645453.xyz
2022-09-27	id5323.xyz
2022-09-27	order969432.xyz
2022-09-27	order5881787.xyz
2022-09-27	id2161346.xyz
2022-09-27	order-0442.xyz
2022-09-27	id64839.xyz
2022-09-27	id345345.xyz
2022-09-27	yandex.id7333.ru
2022-09-27	boxberry.id4744565.ru
2022-09-27	ozon.id9195.ru
2022-09-27	avito.id853123.ru
2022-09-27	id9578195.xyz
2022-09-27	sberbank.id6375.ru
2022-09-27	www.test.id-773621.top
2022-09-27	blablacar-ru.id5323.xyz
2022-09-27	avito.id9197.ru
2022-09-27	youla.id9195.ru
2022-09-27	www.www.staging.id-773621.top

DNS data (3) | Certificates (0) | Subdomains (0) | Map

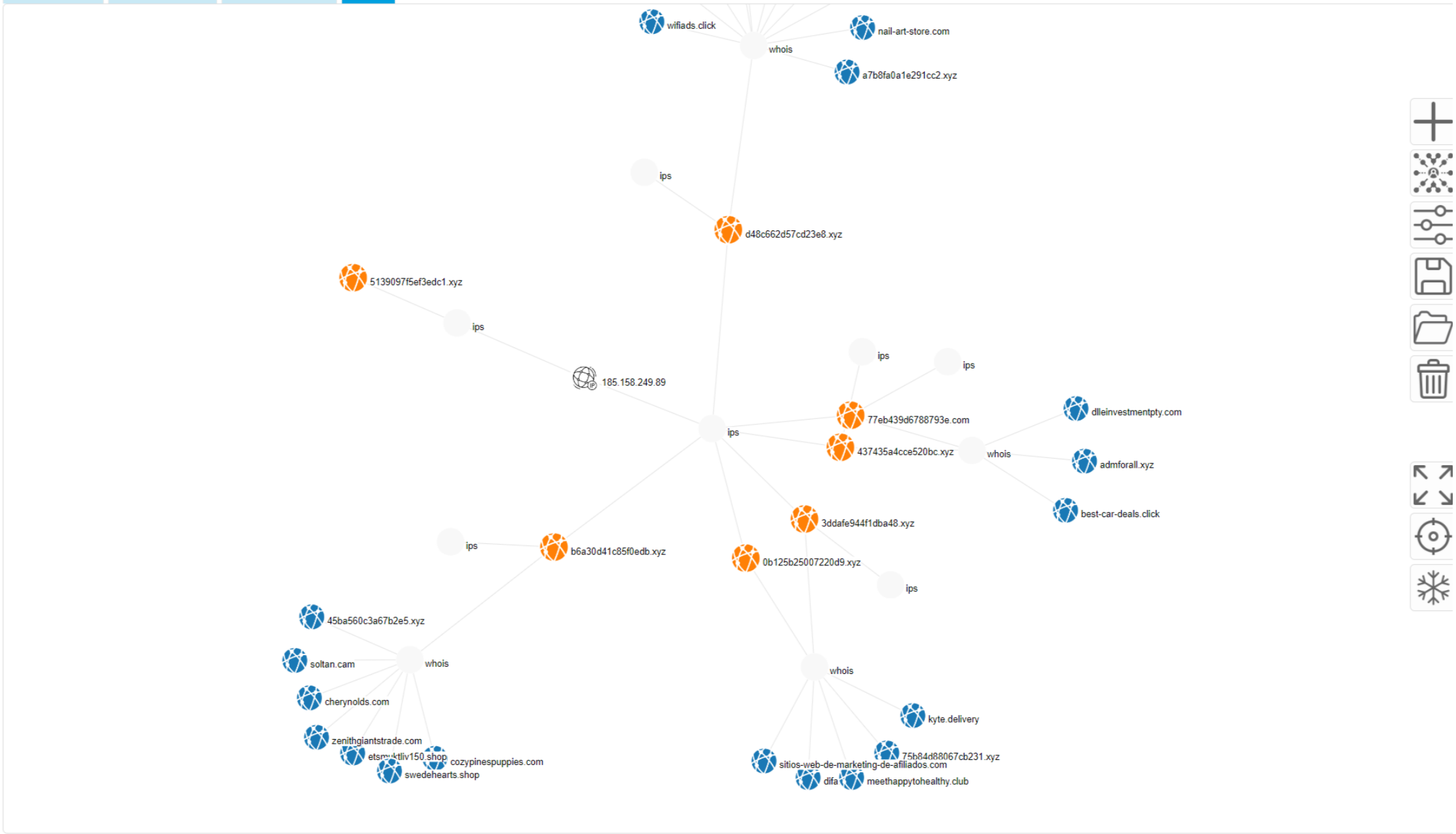
Связи(пример)



DNS data (3) | Certificates (0) | Subdomains (0) | Map



DNS data (3) | Certificates (0) | Subdomains (0) | Map



Сервисы

Фиды

Безопасный DNS

Открытые данные

https://t.me/dga_domains

https://t.me/CyberSquattingChannel

Спасибо!

Евгений Сухов

Ростелеком-Солар

e.sukhov@rt-solar.ru