

Website owners identification

@gspdnsobaka

@AlphariusLegion



OUR COMPANY



01

Clowns and faggots

*Whoever doesn't want to work as a clown for
a faggot will work as a faggot for a clown. For
the same small price. Victor Pelevin.*



Оговорка по Фрейсу или Гей-скандал в окружении Дерипаски

Главное / Шоу-Бизнес Опубликовал(а): dima.bedusenko 10-02-2018, 11:44 👁 11 641



Main mission

Identify the owner of the website with picrelated article [compromat.group](#)

Enumerating similar domains

We started looking for the websites mirroring content from compromat.group website.

Successfully identified:

- *<http://kompromat.group/>*
- *<https://compromat.pro/>*
- *<http://Compromat.ws>*



Томский меценат с двойным дном КОМПРОМАТ

Не простая фигура. Это очень богатый человек, сложнохарактерный, волевой и жесткий
05 МАЙ 2022

Александр Дементьев любил виски



ПОСЛЕДНИЕ НОВОСТИ

05.05.2022

- 16:20 Банду несовершеннолетних неонацистов задержали за осквернение Вечного огня
- 16:00 Четыре человека погибли в ДТП на российской трассе
- 16:00 Сын экс-министра обороны России избил беременную девушку в Подмоскowie
- 15:48 Лидер ячейки теробороны Украины ликвидирован Росгвардией
- 15:35 Путина попросили провести открытый урок для детей
- 15:27 Двое подростков предстанут перед судом за убийство россиянина и разбой
- 15:00 Россиянка нашла останки человека в парке на севере Петербурга
- 15:00 В Госдуме ответили на информацию об отправленных Украине разведанных

ЧИТАЮТ КОММЕНТИРУЮТ

- РОСТРАНСНАДЗОР и надзиратели за миллиардами **5 515 392**
- Кристина Асмус в фильме Текст - постельная сцена **1 748 304**
- Алексей Абасов и Виталий Абасов: на кого работали гении коррупционных схем **800 925**
- Проводится проверка из-за видео с женщиной, давшей на ужин маленькому мальчику использованную жвачку и избившей его **533 420**
- Добивал. Опубликовано видео убийства «воров в законе» Астика и Хасика **478 475**
- Расстрелянный в Москве чемпион Ашот Болян был причастен к организации убийства брата Терещука **459 447**



Томский меценат с двойным дном КОМПРОМАТ

Не простая фигура. Это очень богатый человек, сложного характера, волевой и жесткий
05 МАЙ 2022

Александр Дементьев любил виски



ПОСЛЕДНИЕ НОВОСТИ

05.05.2022

- 16:20 Банду несовершеннолетних неонацистов задержали за осквернение Вечного огня
- 16:00 Четыре человека погибли в ДТП на российской трассе
- 16:00 Сын экс-министра обороны России избил беременную девушку в Подмоскovie
- 15:48 Лидер ячейки теробороны Украины ликвидирован Росгвардией
- 15:35 Путина попросили провести открытый урок для детей
- 15:27 Двое подростков предстанут перед судом за убийство россиянина и разбой
- 15:00 Россиянка нашла останки человека в парке на севере Петербурга
- 15:00 В Госдуме ответили на информацию об отп...
- 14:49 В Госдуме рассуждали о сроках завершения

ЧИТАЮТ

КОММЕНТИРУЮТ

- РОСТРАНСНАДЗОР и надзиратели за миллиардами **5 515 392**
- Кристина Асмус в фильме Текст - постельная сцена **1 748 304**
- Алексей Абасов и Виталий Абасов: на кого работали гении коррупционных схем **800 926**
- Проводится проверка из-за видео с женщиной, давшей на ужин маленькому мальчику использованную жвачку и избившей его **533 420**
- Добивал. Опубликовано видео убийства «воров в законе» Астика и Хасика **478 475**

Lightshot
Screenshot is saved to Screenshot_56.png. Click here to open in the folder.

он Ашот
ации
443

ГОРЯЧЕЕ

в Израиль, лишают КАК УГОЛОВНИК КУЗНЕЦОВ ПОЛУЧИЛ СТАТУС БЕЖЕНЦА? <>

КОМПРОМАТ

весь сор в одной избе

- ГЛАВНАЯ
- РЕДКОЛЕГИЯ
- ЛЕНТА
- ОЛИГАРХИ
- МИНИСТРЫ
- ДЕПУТАТЫ
- ПОЛИЦИЯ
- ЧИНОВНИКИ
- СПЕЦСЛУЖБЫ
- ПРОКУРОРЫ
- БРАТВА
- РАЗНОЕ



Выбор редакции 1 of 5 < >

**РОДСТВЕННИЦУ
ЭКС-СОВЛАДЕЛЬЦА
ГК "ЯШМА",
СБЕЖАВШЕГО ОТ
КРЕДИТОРОВ В
ИЗРАИЛЬ**



ВСЕ ИНСАЙДЫ В
НАШЕМ TELEGRAM

Lightshot
Screenshot is saved to Screenshot_57.png. Click here to open in the folder.

Пишите нам

КОМПРОМАТ^{WS}



Статьи [Расследования](#) [Слухи](#)

[Россия](#) [Украина](#) [Теги](#)

29.03.2019	23:17	Очередная «война» Потанина	40427	1
15.03.2019	05:34	Загогулина Потанина	238452	0
13.03.2019	05:34	Олигархический авиапарк — 2019	27253	0
01.11.2018	05:34	Бельгийская пицца от Олерского	59564	0
03.08.2018	05:34	Многостаночник Ильдар Узбеков выводит все, что можно	27853	0
14.06.2018	05:34	«Решала» от барина Александр Грановский	26643	0
10.10.2017	05:34	Мурманская побирушка	25392	1
12.02.2016	05:34	Красивая жизнь в Лондоне закончилась Интерполом	27163	0
01.05.2022	10:06	Как в Санкт-Петербурге канализация растеклась по жилым домам, и почему чиновники винят жителей и пандемию	3983	0
30.04.2022	14:52	Что изменится в жизни россиян с 1 мая 2022 года?	2326	0
30.04.2022	13:06	Как Олег Бойко из банального ростовщика дорос до «пионера финтеха»	3055	0
30.04.2022	13:06	Плесень и антибиотики в кефире «Коровка из Кореновки» и «Б.Ю.	4993	0

Преступная Россия

- Расстрел двух «воров в законе» произошел на глазах у ребенка
- «Я вела себя как нормальный горожанин». Чиновница из Петрозаводска прокомментировала свои угрозы мусорящим в ее дворе людям
- Путин призвал терзать и трясти чиновников
- Бывший оперативник ингушского Центра «Э», осужденный за пытки, вышел на свободу
- О глуме над детским спортом рассказал уволенный из школы олимпийского резерва тренер по боксу в Волгограде

Viewdns.info

Tools API Research Data

Reverse IP Lookup

Find all sites hosted on a given server.

Domain / IP
 GO

Reverse Whois Lookup

Find domain names owned by an individual or company.

Registrant Name or Email Address
 GO

IP History

Show historical IP addresses for a domain.

Domain (e.g. domain.com)
 GO

DNS Report

Provides a complete report on your DNS settings.

Domain (e.g. domain.com)
 GO

Reverse MX Lookup

Find all sites that use a given mail server.

Mail server (e.g. mail.google.com)
 GO

Reverse NS Lookup

Find all sites that use a given nameserver.

Nameserver (e.g. ns1.example.com)
 GO

IP Location Finder

Find the geographic location of an IP Address.

IP
 GO

Chinese Firewall Test

Checks whether a site is accessible from China.

URL / Domain
 GO

DNS Propagation Checker

Check whether recent DNS changes have propagated.

Domain (e.g. domain.com)
 GO

Is My Site Down

Check whether a site is actually down or not.

Domain (e.g. domain.com)
 GO

Iran Firewall Test

Check whether a site is accessible in Iran.

Site URL / Domain
 GO

Domain / IP Whois

Lookup information on a Domain or IP address.

Domain / IP
 GO

VIEWDNS.INFO

Framework for technical OSINT. Reverse IP Lookup, Whois lookup, IP History etc.

IP history results for compromat.pro.
=====

IP Address	Location	IP Address Owner	Last seen on this IP
188.114.97.2	United States	CloudFlare	2022-02-07
188.114.96.2	United States	CloudFlare	2022-02-07
172.67.134.84	United States	Cloudflare, Inc.	2022-02-05
104.21.25.150	United States	Cloudflare, Inc.	2022-02-05
188.114.97.2	United States	CloudFlare	2022-02-04
188.114.96.2	United States	CloudFlare	2022-02-04
172.67.134.84	United States	Cloudflare, Inc.	2022-02-03
104.21.25.150	United States	Cloudflare, Inc.	2022-02-03
194.85.61.76	Russia	JSC "RU-CENTER"	2019-12-26
109.70.26.37	Russia	RU-CENTER	2019-12-26
109.70.26.36	Russia	RU-CENTER	2011-11-07

 @JalStarcenter

IP History results

*For compromat.pro
website*

*Russian IP addresses is a
win for law enforcement,
but we needed to go
deeper*

Bypassing Cloudflare IP protection

*Most of the websites we have
identified used Cloudflare IP
protection. So we came up with using
WAF Bypass tool*

<https://github.com/vincentcox/bypass-firewalls-by-DNS-history>


```
b4cksp4ce@bksp-acer-2:~/Downloads/bypass-firewalls-by-DNS-history-master$ bash bypass-fi  
rewalls-by-DNS-history.sh -d compromat.group
```

```
-----  
WAF Bypass  
-----
```

```
Via DNS history. ( @vincentcox_be | vincentcox.com )  
-----
```

```
jq: error (at <stdin>:0): Cannot index string with string "dns_names"  
jq: error (at <stdin>:5): Cannot iterate over null (null)  
parse error: Invalid numeric literal at line 3, column 0
```

```
[-] 1 Domains collected...  
[-] Scraping IP's from (sub)domains (100%)  
[-] 12 IP's gathered from DNS history...  
[-] Launching requests to origin servers...  
[-] Waiting on replies from origin servers...  
[+] Bypass found!
```

[IP]	[Confidence]	[Organisation]
https://5.45.64.21	100 %	AS58061 Scalaxy B.V.
http://83.243.68.157	85 %	AS42065 ZAO ElectronTelecom
http://5.45.64.21	85 %	AS58061 Scalaxy B.V.

```
b4cksp4ce@bksp-acer-2:~/Downloads/bypass-firewalls-by-DNS-history-master$
```

WAF Bypass

This script will try to find:

- *the direct IP address of a server behind a firewall like Cloudflare, Incapsula, SUCURI ...*
- *an old server which still running the same (inactive and unmaintained) website, not receiving active traffic because the A DNS record is not pointing towards it*



Whois Domain Bot

bot

<https://reg.ru/link/WYT/ccx>

11:07 AM

/whois [politobzor.net](https://reg.ru/link/WYT/ccx) 11:08 AM ✓

[politobzor.net](https://reg.ru/link/WYT/ccx) - [5.8.79.230](https://reg.ru/link/WYT/ccx)

Domain name: [politobzor.net](https://reg.ru/link/WYT/ccx)

Registry Domain ID: 1770408572_DOMAIN_NET-VRSN

Registrar WHOIS Server: [whois.reg.com](https://reg.ru/link/WYT/ccx)

Registrar URL: [https://www.reg.com](https://reg.ru/link/WYT/ccx)

Registrar URL: [https://www.reg.ru](https://reg.ru/link/WYT/ccx)

Updated Date: 2021-03-21T04:34:43Z

Creation Date: 2013-01-02T04:09:00Z

Registrar Registration Expiration Date: 2023-01-02T04:09:00Z

Registrar: Registrar of domain names [REG.RU](https://reg.ru/link/WYT/ccx) LLC

Registrar IANA ID: 1606

Registrar Abuse Contact Email: abuse@reg.ru

Registrar Abuse Contact Phone: +7.4955801111

Status: clientTransferProhibited <http://www.icann.org>

[/epp#clientTransferProhibited](http://www.icann.org)

Registry Registrant ID:

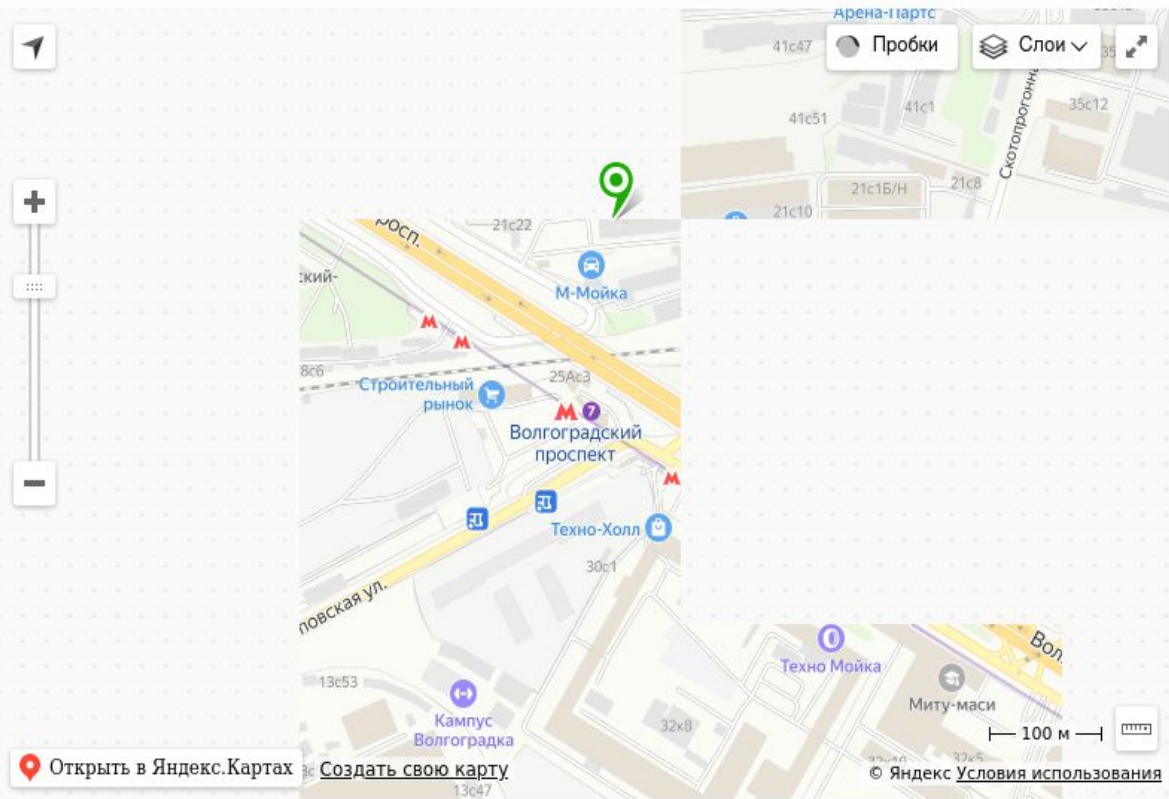
Registrant Name: Andrei Ermilov

Registrant Organization: VO-media, LLC

Whois Domain Bot

Whois information about IP address or domain in pocket format

Заказы на сайте nike-store-online.ru принимаются круглосуточно



**GO STUPID
GO CRAZY**

огрнпн 316222500123032

огрнп 316222500123032



Все

Картинки

Карты

Новости

Видео

Ещё

Инструменты

Результатов: примерно 28 (0,29 сек.)

<https://www.rusprofile.ru> > Проверка ИП ▾

ИП Павлов Алексей Святославович - Rusprofile

ОГРНИП: 316222500123032: от 14 октября 2016 г. ИНН: 222400320279. Дата регистрации: 14.10.2016. Адрес: Алтайский край, город Барнаул.

<https://checko.ru> > pavlov-aleksey-316222500123032 ▾

ИП Павлов Алексей Святославович - Чекко

ИП Павлов Алексей Святославович - **ОГРН 316222500123032** - ИНН 222400320279 - Регион не указан - Реквизиты - Контакты - Сведения о...

**GO STUPID
GO CRAZY**

URL: <http://giveaway-eth.com/>Submission: On April 30 via manual (April 30th 2018, 9:11:44 pm UTC) from 
[Summary](#)
[HTTP 15](#)
[Redirects](#)
[Behaviour !\[\]\(c3d993ca47bfe2a953c700506ce31fa0_img.jpg\)](#)
[Indicators](#)
[Similar](#)
[DOM](#)
[Content](#)
[API](#)
[Verdicts](#)

Summary

This website contacted **6 IPs** in **1 countries** across **5 domains** to perform **15 HTTP transactions**. The main IP is **207.174.214.239**, located in **United States** and belongs to **PUBLIC-DOMAIN-REGISTRY - PDR, US**. The main domain is **giveaway-eth.com**.

[giveaway-eth.com](#) scanned **4 times** on urlscan.io

[Show Scans 4](#)

urlscan.io Verdict: **Potentially Malicious **

Targeting these brands:  **Generic Crypto (Crypto Exchange)**







Live information

Google Safe Browsing:  No classification for [giveaway-eth.com](#)

Domain created: August 25th 2021, 16:27:11 (UTC)

Domain registrar: Wild West Domains, LLC

Domain & IP information

IP/ASNs	IP Detail	Domains	Domain Tree	Links	Certs	Frames
	IP Address	AS Autonomous System				
1	207.174.214.239 	394695 (PUBLIC-DOMAIN-REGISTRY - PDR)				
1	209.197.31.15 	20446 (HIGHWINDS3 - Highwinds Network Group)				
7	104.16.54.3 	13335 (CLOUDFLARENET - Cloudflare)				
1	172.217.22.46 	15169 (GOOGLE - Google LLC)				
1	151.101.12.193 	54113 (FASTLY - Fastly)				

15

6

Screenshot



Detected technologies

 **Ruby** (Programming Languages)

 **Ruby on Rails** (Web Frameworks)

 **Apache** (Web Servers)

 **jQuery** (JavaScript Libraries)

Twitter Bootstrap ()

Page Statistics

15	0 %	0 %	5	5
Requests	HTTPS	IPv6	Domains	Subdomains
6	1	302 kB	734 kB	0
IPs	Countries	Transfer	Size	Cookies


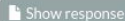









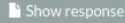














URL: http://giveaway-eth.com/

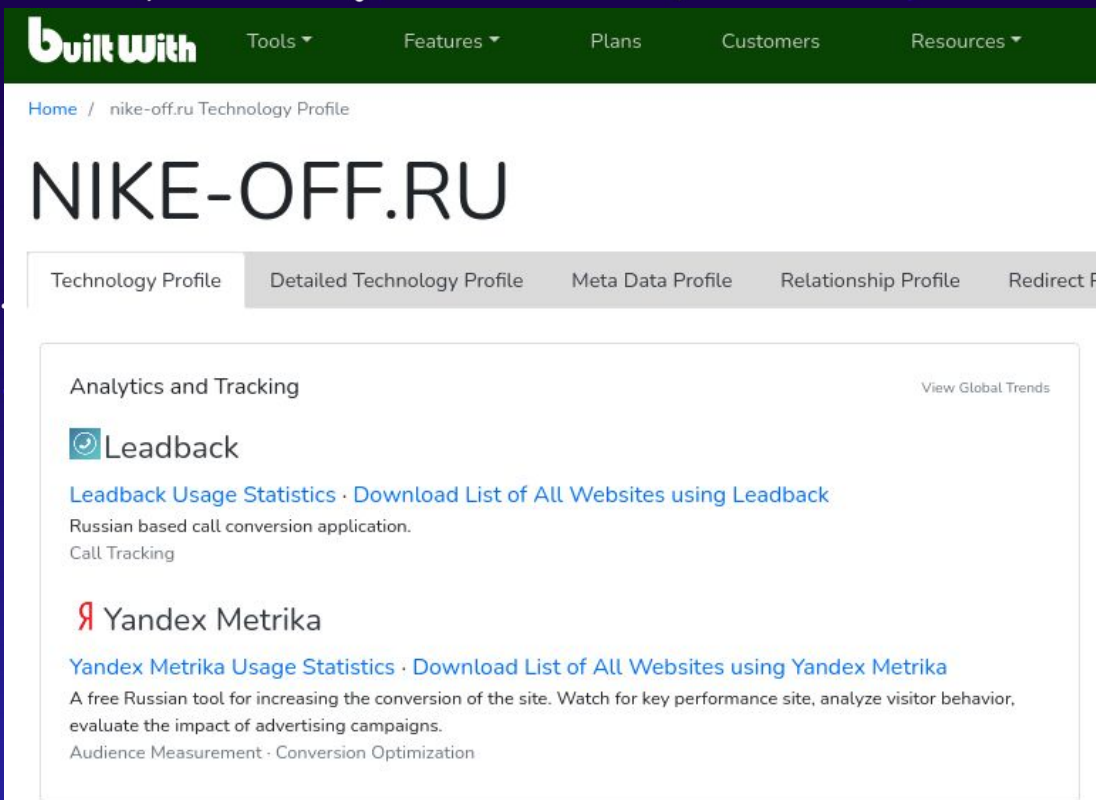
Submission: On April 30 via manual (April 30th 2018, 9:11:44 pm UTC) from 
[Summary](#)
[HTTP 15](#)
[Redirects](#)
[Behaviour 6](#)
[Indicators](#)
[Similar](#)
[DOM](#)
[Content](#)
[API](#)
[Verdicts](#)

15 HTTP transactions

[Everything](#)
[HTML](#)
[Script](#)
[AJAX](#)
[CSS](#)
[Image](#)
[Expand all](#)


0 data transactions


Method	Resource	Size	Time	Type	IP
Protocol	Status Path	x-fer	Latency	MIME-Type	Location
 GET	200 Primary Request / giveaway-eth.com/	 63 KB	256ms	Document	207.174.214.239
H/1.1	OK	63 KB	130ms	text/html	 PDR
 GET	200 bootstrap.min.css maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/	141 KB	26ms	Stylesheet	209.197.3.15
H/1.1	OK	20 KB	8ms	text/css	 Highwinds Network...
 GET	200 overrides.min.css?18005c9c8eb43636 blockchain.info/Resources/	4 KB	57ms	Stylesheet	104.16.54.3
S		2 KB	30ms	text/css	 Cloudflare
 GET	200 jquery.min.js blockchain.info/Resources/js/	 94 KB	51ms	Script	104.16.54.3
S		33 KB	24ms	application/javascript	 Cloudflare
 GET	200 bootstrap.min.js?18005c9c8eb43636 blockchain.info/Resources/js/	 36 KB	45ms	Script	104.16.54.3
S		10 KB	19ms	application/javascript	 Cloudflare
 GET	200 shared.min.js?18005c9c8eb43636 blockchain.info/Resources/js/	 13 KB	57ms	Script	104.16.54.3
S		5 KB	31ms	application/javascript	 Cloudflare
 GET	200 blockchain.css?18005c9c8eb43636 blockchain.info/Resources/css/	253 KB	71ms	Stylesheet	104.16.54.3
S		40 KB	45ms	text/css	 Cloudflare
 GET	200 payment-request.css?18005c9c8eb43636 blockchain.info/Resources/	734 B	78ms	Stylesheet	104.16.54.3
S		430 B	52ms	text/css	 Cloudflare
 GET	200 app-overrides.css?18005c9c8eb43636 blockchain.info/Resources/	2 KB	56ms	Stylesheet	104.16.54.3
S		792 B	29ms	text/css	 Cloudflare
 GET	200 chart?cht=qr&chs=300x300&chl=0xD289Bc0A919E75B824F4Dfc376E9F24C119E3D3F3&chld=H%7C0 chart.apis.google.com/	2 KB	61ms	Image	172.217.22.46
H/1.1	OK	2 KB	55ms	image/png	 Google LLC
 GET	200 T1X5ZPT.gif i.imgur.com/	126 KB	32ms	Image	151.101.12.193
S		126 KB	7ms	image/gif	 Fastly



The screenshot shows the BuiltWith.com website profile for NIKE-OFF.RU. The page has a green header with the BuiltWith logo and navigation links for Tools, Features, Plans, Customers, and Resources. Below the header, the breadcrumb trail reads 'Home / nike-off.ru Technology Profile'. The main title is 'NIKE-OFF.RU'. A navigation bar contains tabs for 'Technology Profile', 'Detailed Technology Profile', 'Meta Data Profile', 'Relationship Profile', and 'Redirect P'. The main content area is titled 'Analytics and Tracking' and includes a 'View Global Trends' link. Two technology entries are listed: 'Leadback' and 'Yandex Metrika'. Each entry includes a logo, a title, a link to usage statistics and a download list, a brief description, and associated keywords.

Analytics and Tracking [View Global Trends](#)

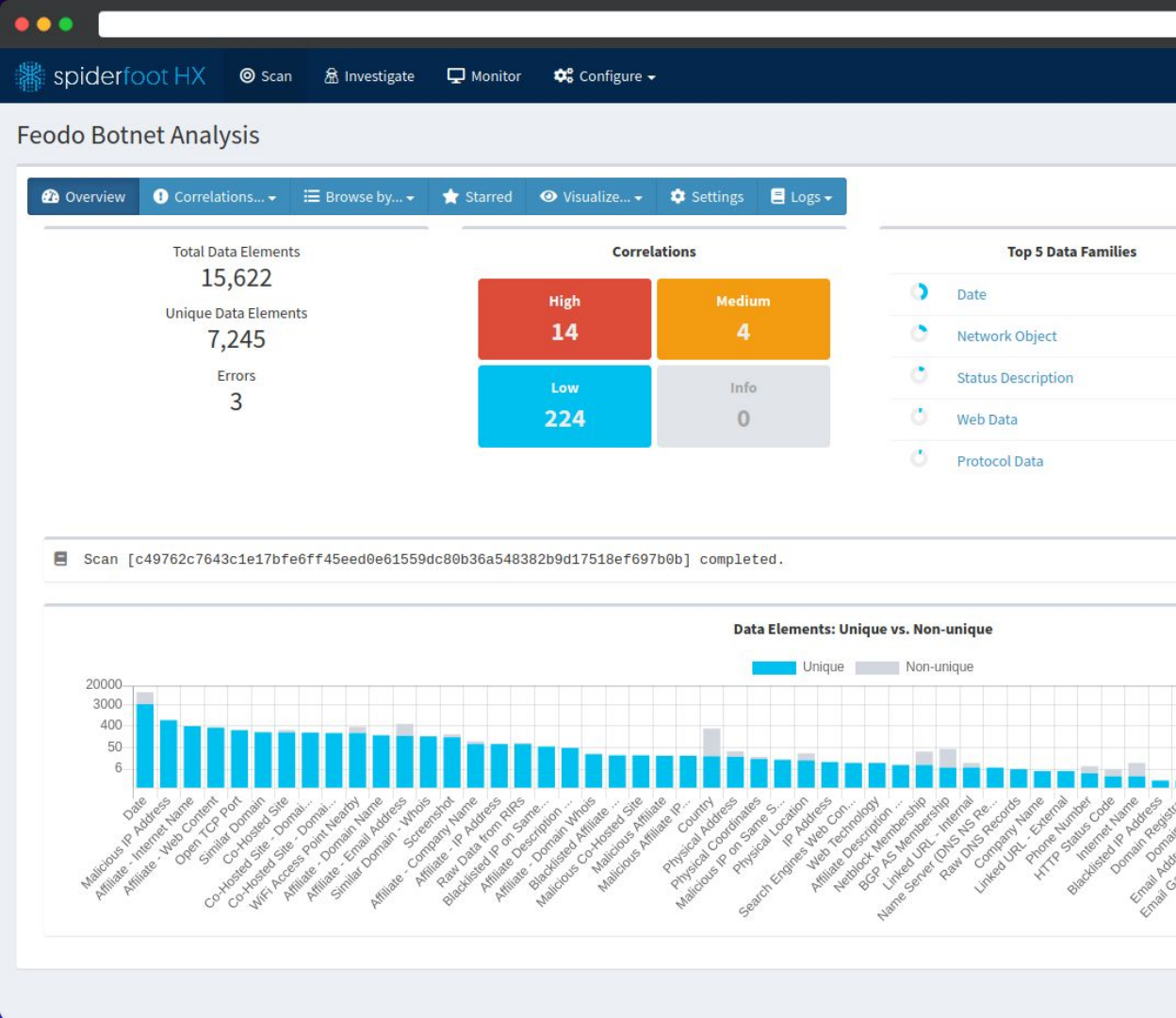
 **Leadback**
[Leadback Usage Statistics](#) · [Download List of All Websites using Leadback](#)
Russian based call conversion application.
Call Tracking

 **Yandex Metrika**
[Yandex Metrika Usage Statistics](#) · [Download List of All Websites using Yandex Metrika](#)
A free Russian tool for increasing the conversion of the site. Watch for key performance site, analyze visitor behavior, evaluate the impact of advertising campaigns.
Audience Measurement · Conversion Optimization

Builtwith.com

Find out what websites are built with

- *Analytics and Tracking*
- *JavaScript Libraries and Functions*
- *Webmaster Registration*



SpiderFoot HX

Framework for
 website, IP,
 human names
 etc. OSINT



