SOCIAL LINKS

HOW TO FIND INFORMATION USING DOMAIN RECORDS

6 August 2020

In Partnership With

Whois XML API
Domain Investigations

Jörn Weber
OSINT Expert at Corma

#1
Leading tool

HOW TO FIND INFORMATION USING DOMAIN RECORDS

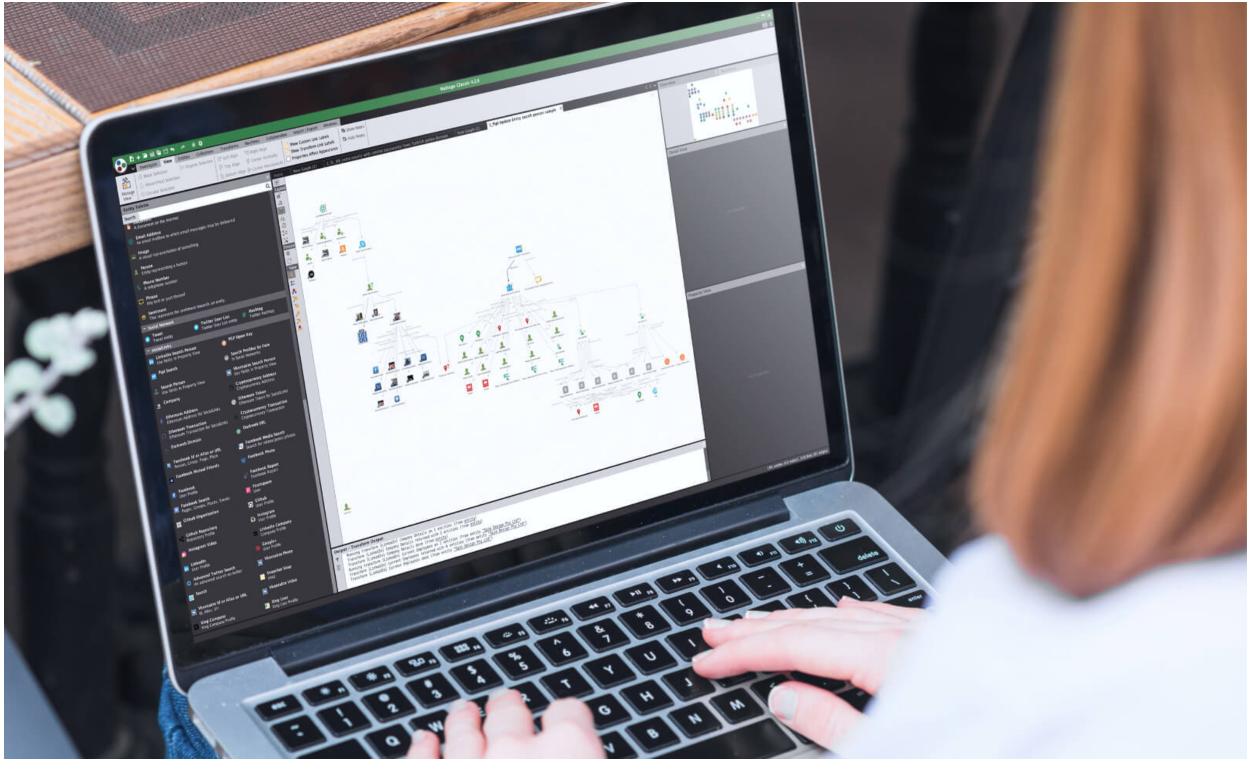
AGENDA

- Introduction:
  Social Links, WhoisXML API, and Jörn Weber.

- Introduction to the methods
- The Cryptoqueen – Where is Dr. Ruja?
- Q & A about the 1st case.
- Operation Bayonet – The Alphabay Case.
- Q & A about the 2nd case.

- Q & A.

Maltego: a Visualisation Tool



Key Social Links Facts

SOCIAL LINKS

6 Years of Open Source
Data Mining Tool Development

50+
Sources

700+
Transforms

9TB
Our own Social
Links database

50% EU Law Enforcement organizations already use Social Links for Open Source, Social Media and Dark Web Intelligence

Clients from all
around the world
from 55+ countries

TOP 5 Industries: Law Enforcement, Cyber Security, Finance and Banking, Consulting and Due Diligence

Social Links Allows You to Search and Investigate

- People and connections, including hidden data, activity analysis of pages and profiles
- Companies, employees, relations of employees with contractors, resumes of employees
- Geolocation — search by coordinates of events, people, photos and video materials
- Face recognition and identification of objects and people in the photo
- Dark Web – search by Keyword and Key Phrase, PGP key, location, product, contact information
- Companies leaks
- Messengers

Social Links is Already Used for

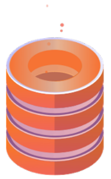
- Law Enforcement agencies
- Finance and Banking
- Consulting and Due Diligence
- Cyber Security companies
- Security Operation Centers in commercial companies
- Government organizations

The Who Behind Cyber Threat Intelligence

We deliver the most comprehensive domain, IP, DNS, and cyber threat intelligence data to enable a more secure and transparent Internet for all businesses.

Some of the headaches we solve:

- All sources of domain and IP data in one place
- Proper data parsing and formatting
- Working agreements with ISPs and registrars



Comprehensive & Updated Data Feeds

Readily Integratable APIs

Professional Research & Monitoring Tools

7.0 billion+
Historic WHOIS Records

1.2 billion+
Domains and subdomains

2,864+
TLDs & ccTLDs

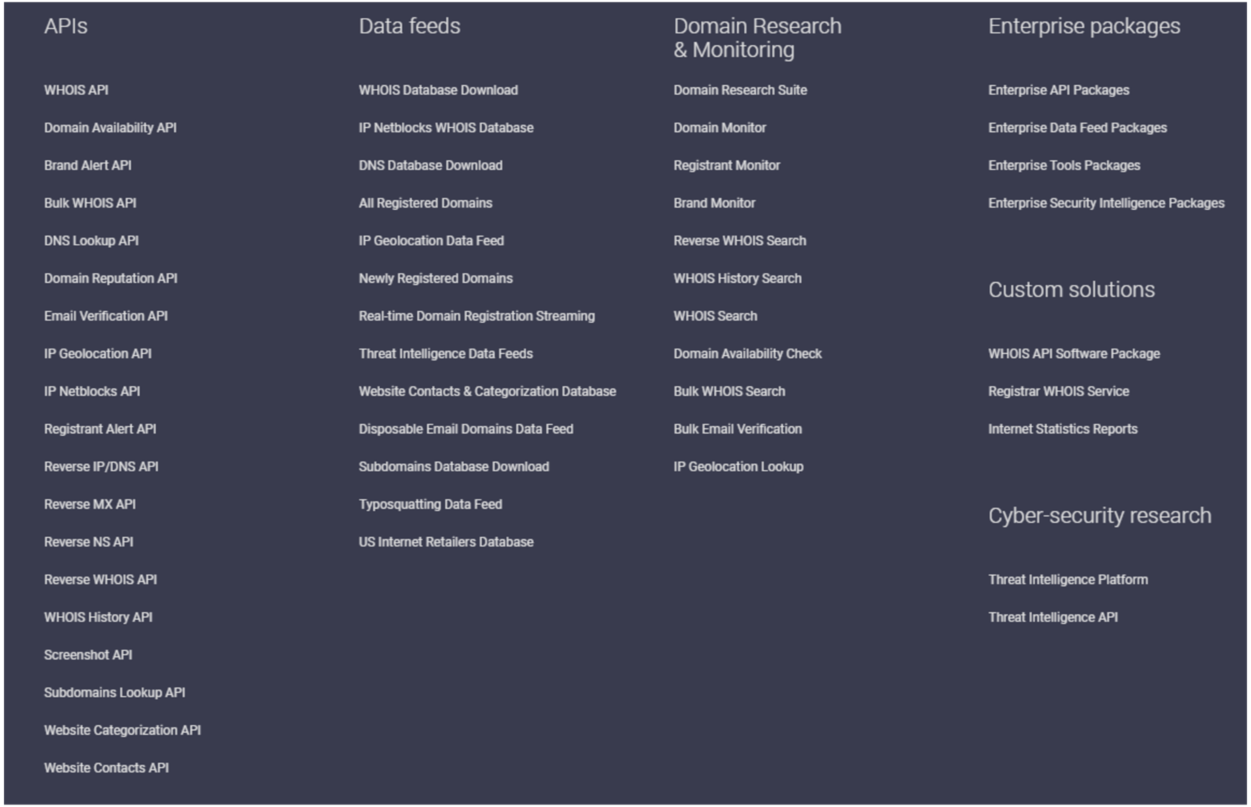
9.5 million+
IP netblocks

99.5%
IP addresses in use covered

330 million+
Registered websites

152 million+
Categorized websites

The Who Behind Cyber Threat Intelligence



APIs

- WHOIS API
- Domain Availability API
- Brand Alert API
- Bulk WHOIS API
- DNS Lookup API
- Domain Reputation API
- Email Verification API
- IP Geolocation API
- IP Netblocks API
- Registrant Alert API
- Reverse IP/DNS API
- Reverse MX API
- Reverse NS API
- Reverse WHOIS API
- WHOIS History API
- Screenshot API
- Subdomains Lookup API
- Website Categorization API
- Website Contacts API

Data feeds

- WHOIS Database Download
- IP Netblocks WHOIS Database
- DNS Database Download
- All Registered Domains
- IP Geolocation Data Feed
- Newly Registered Domains
- Real-time Domain Registration Streaming
- Threat Intelligence Data Feeds
- Website Contacts & Categorization Database
- Disposable Email Domains Data Feed
- Subdomains Database Download
- Typosquatting Data Feed
- US Internet Retailers Database

Domain Research & Monitoring

- Domain Research Suite
- Domain Monitor
- Registrant Monitor
- Brand Monitor
- Reverse WHOIS Search
- WHOIS History Search
- WHOIS Search
- Domain Availability Check
- Bulk WHOIS Search
- Bulk Email Verification
- IP Geolocation Lookup

Enterprise packages

- Enterprise API Packages
- Enterprise Data Feed Packages
- Enterprise Tools Packages
- Enterprise Security Intelligence Packages

Custom solutions

- WHOIS API Software Package
- Registrar WHOIS Service
- Internet Statistics Reports

Cyber-security research

- Threat Intelligence Platform
- Threat Intelligence API

7.0 billion+
Historic WHOIS Records

1.2 billion+
Domains and subdomains

2,864+
TLDs & ccTLDs

9.5 million+
IP netblocks

99.5%
IP addresses in use covered

330 million+
Registered websites

152 million+
Categorized websites

The Who Behind Cyber Threat Intelligence

Common use cases:

- Build better cybersecurity platforms
- Strengthen managed security services
- Assess and improve security postures
- Conduct meaningful cyber investigations
- Protect domains from brand abuses
- Enrich business data

50K satisfied customers

Top Inc. 5000 fastest growing since 2016

7.0 billion+
Historic WHOIS Records

1.2 billion+
Domains and subdomains

2,864+
TLDs & ccTLDs

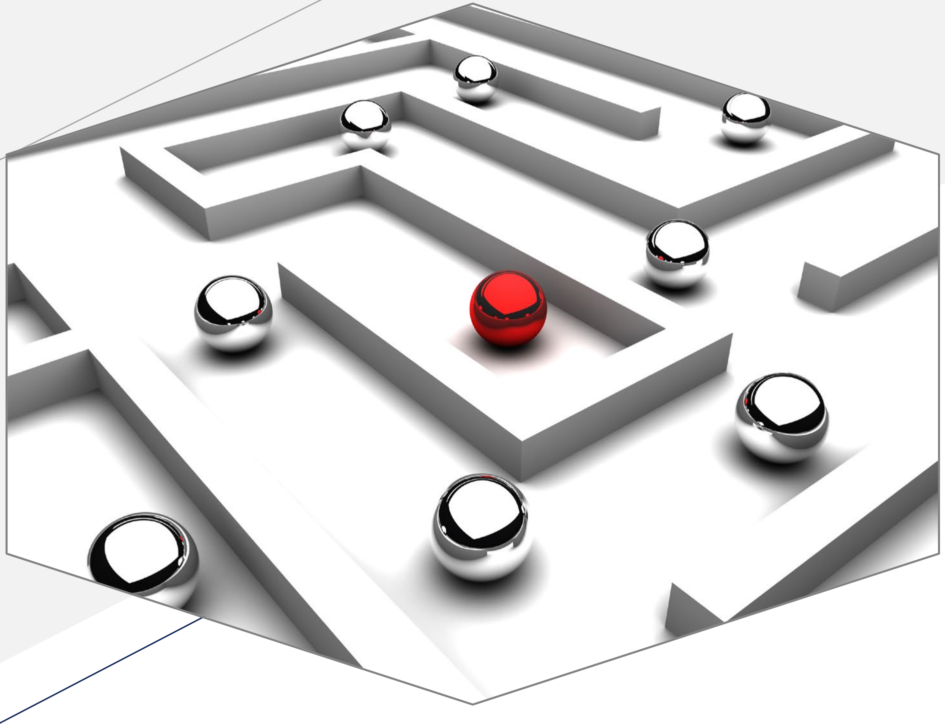
9.5 million+
IP netblocks

99.5%
IP addresses in use covered

330 million+
Registered websites

152 million+
Categorized websites

CASES

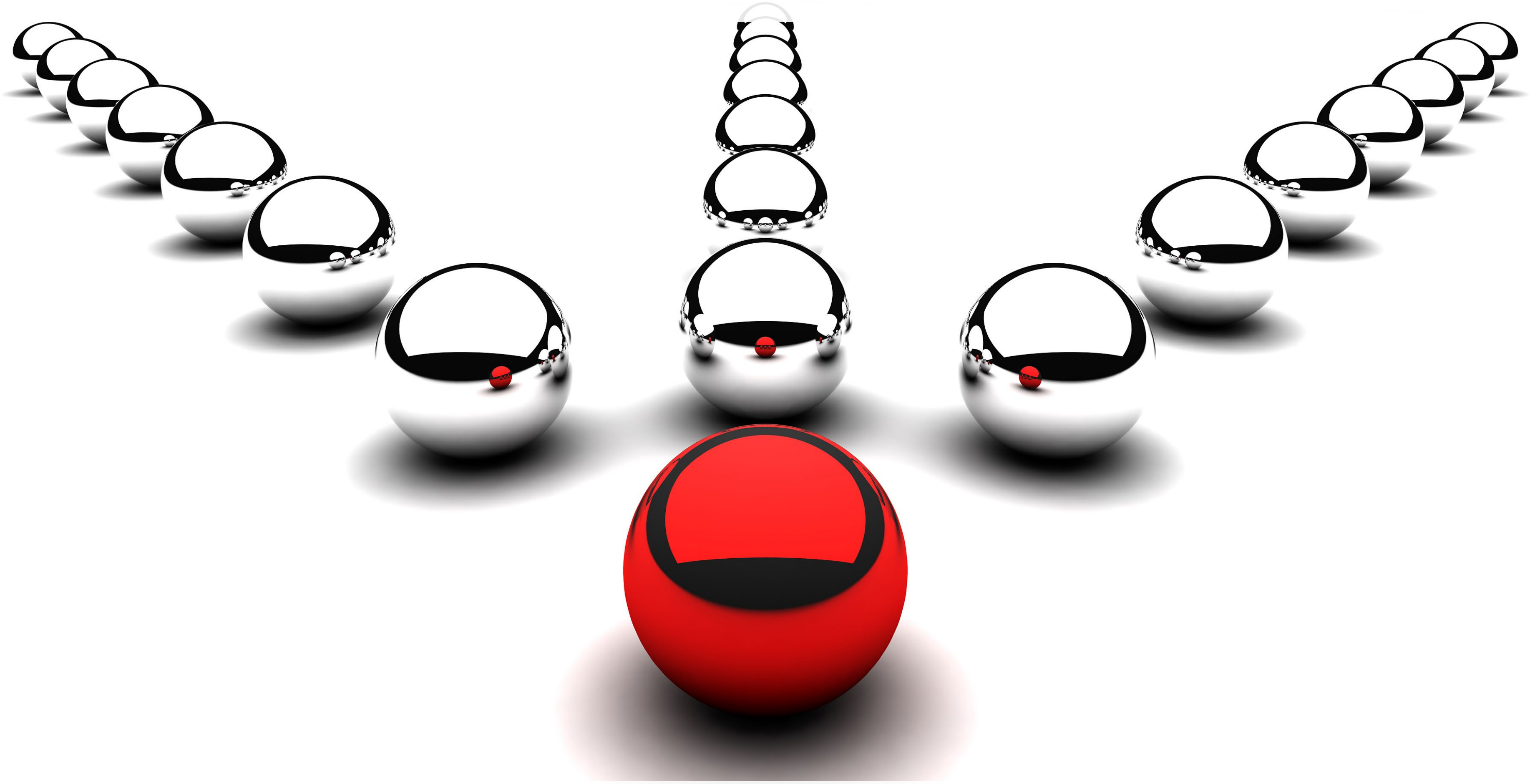


Social Links & WhoisXML API Webinar 06. August 2020

Jörn Weber
corma GmbH

https://corma.de / https://www.corma.training

Entities

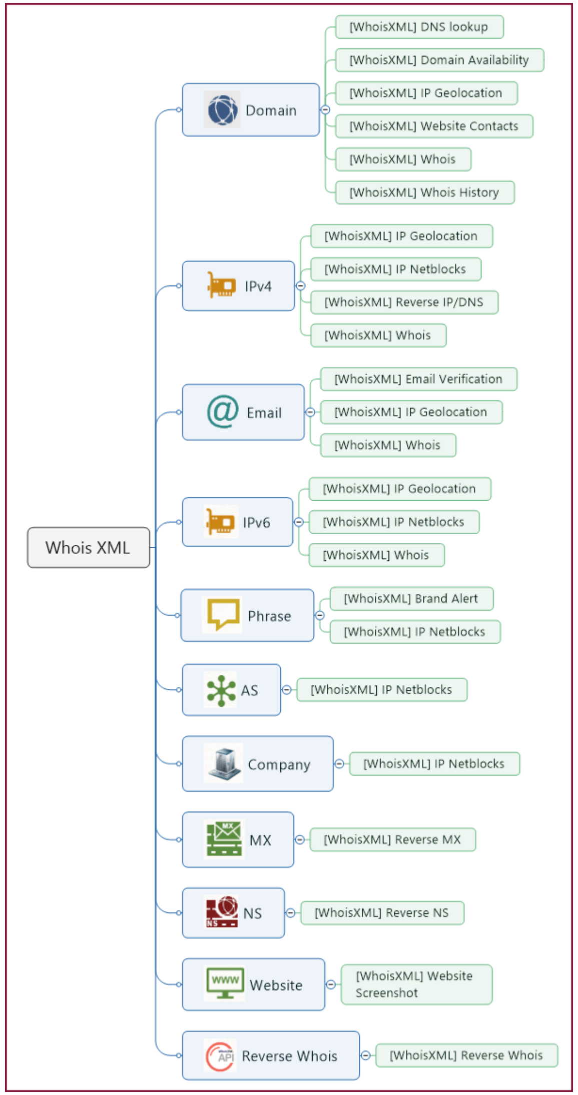


WhoisXML API

Entities for WhoisXML

Entity	Icon	Example
Domain	paterva.com	maltego.com
IPv4 Address	74.207.243.85	112.233.45.56
Email Address	@ info@paterva.com	support@maltego.com
IPv6 Address	::ffff:68c8:12cd	2a00:6020:15d0:8200:3026:3e52:3660:5655
Phrase	Some phrase	some text
AS	63949	6349
Company	Black Label Ltd.	Black Label Ltd.
NS (Name Server)	NS ns59.domaincontrol.com	lily@cloudflare.com
MX (Mail Server)	MX mx.protection.outlook.com	mx1.paterva.com
WhoIsXML Reverse	WhoisXML API Reverse Whois	Please use fields in Property View
Website	WWW	www.corma.training

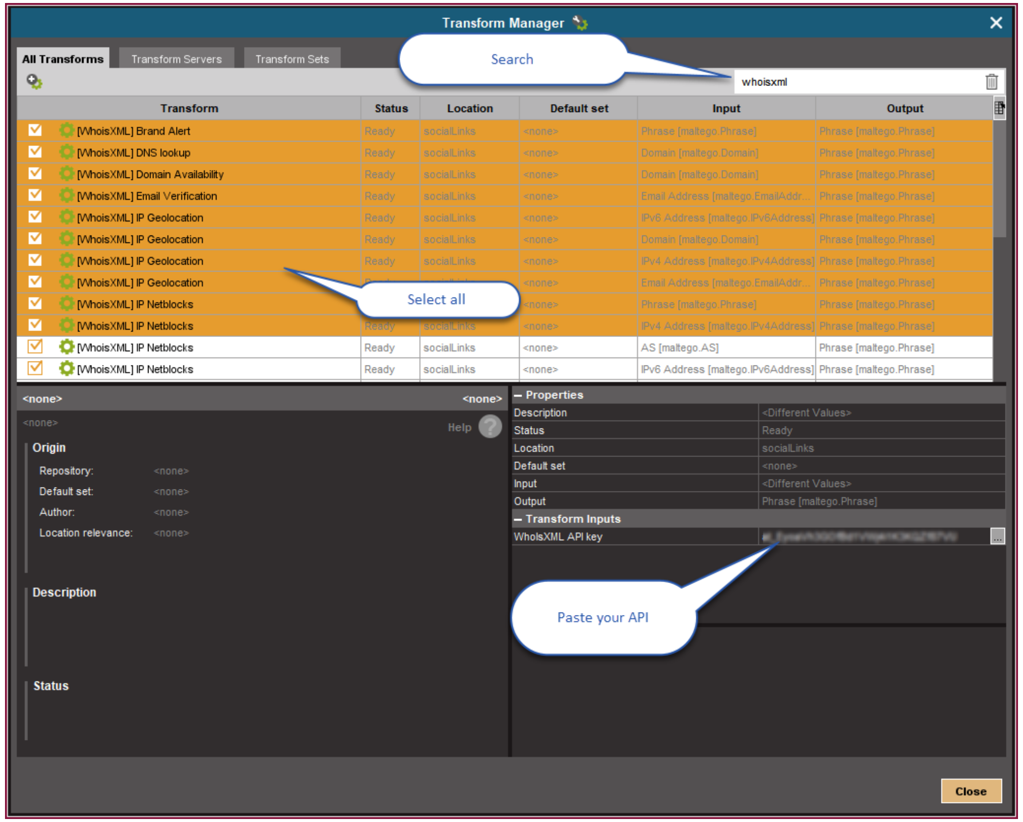
WhoisXML API Transforms -Overview



- Whois XML
  - Domain
    - [WhoisXML] DNS lookup
    - [WhoisXML] Domain Availability
    - [WhoisXML] IP Geolocation
    - [WhoisXML] Website Contacts
    - [WhoisXML] Whois
    - [WhoisXML] Whois History
  - IPv4
    - [WhoisXML] IP Geolocation
    - [WhoisXML] IP Netblocks
    - [WhoisXML] Reverse IP/DNS
    - [WhoisXML] Whois
  - Email
    - [WhoisXML] Email Verification
    - [WhoisXML] IP Geolocation
    - [WhoisXML] Whois
  - IPv6
    - [WhoisXML] IP Geolocation
    - [WhoisXML] IP Netblocks
    - [WhoisXML] Whois
  - Phrase
    - [WhoisXML] Brand Alert
    - [WhoisXML] IP Netblocks
  - AS
    - [WhoisXML] IP Netblocks
  - Company
    - [WhoisXML] IP Netblocks
  - MX
    - [WhoisXML] Reverse MX
  - NS
    - [WhoisXML] Reverse NS
  - Website
    - [WhoisXML] Website Screenshot
  - Reverse Whois
    - [WhoisXML] Reverse Whois

How to enter the API

- Get the API Key here: https://main.whoisxmlapi.com/signup



whoisxml

	Transform	Status	Location	Default set	Input	Output
☑	[WhoisXML] Brand Alert	Ready	socialLinks	<none>	Phrase [maltego.Phrase]	Phrase [maltego.Phrase]
☑	[WhoisXML] DNS lookup	Ready	socialLinks	<none>	Domain [maltego.Domain]	Phrase [maltego.Phrase]
☑	[WhoisXML] Domain Availability	Ready	socialLinks	<none>	Domain [maltego.Domain]	Phrase [maltego.Phrase]
☑	[WhoisXML] Email Verification	Ready	socialLinks	<none>	Email Address [maltego.EmailAddr...	Phrase [maltego.Phrase]
☑	[WhoisXML] IP Geolocation	Ready	socialLinks	<none>	IPv6 Address [maltego.IPv6Address]	Phrase [maltego.Phrase]
☑	[WhoisXML] IP Geolocation	Ready	socialLinks	<none>	Domain [maltego.Domain]	Phrase [maltego.Phrase]
☑	[WhoisXML] IP Geolocation	Ready	socialLinks	<none>	IPv4 Address [maltego.IPv4Address]	Phrase [maltego.Phrase]
☑	[WhoisXML] IP Geolocation			<none>	Email Address [maltego.EmailAddr...	Phrase [maltego.Phrase]
☑	[WhoisXML] IP Netblocks			<none>	Phrase [maltego.Phrase]	Phrase [maltego.Phrase]
☑	[WhoisXML] IP Netblocks	Ready	socialLinks	<none>	IPv4 Address [maltego.IPv4Address]	Phrase [maltego.Phrase]
☑	[WhoisXML] IP Netblocks	Ready	socialLinks	<none>	AS [maltego.AS]	Phrase [maltego.Phrase]
☑	[WhoisXML] IP Netblocks	Ready	socialLinks	<none>	IPv6 Address [maltego.IPv6Address]	Phrase [maltego.Phrase]

<none> <none>

<none>

Origin

Repository: <none>

Default set: <none>

Author: <none>

Location relevance: <none>

Description

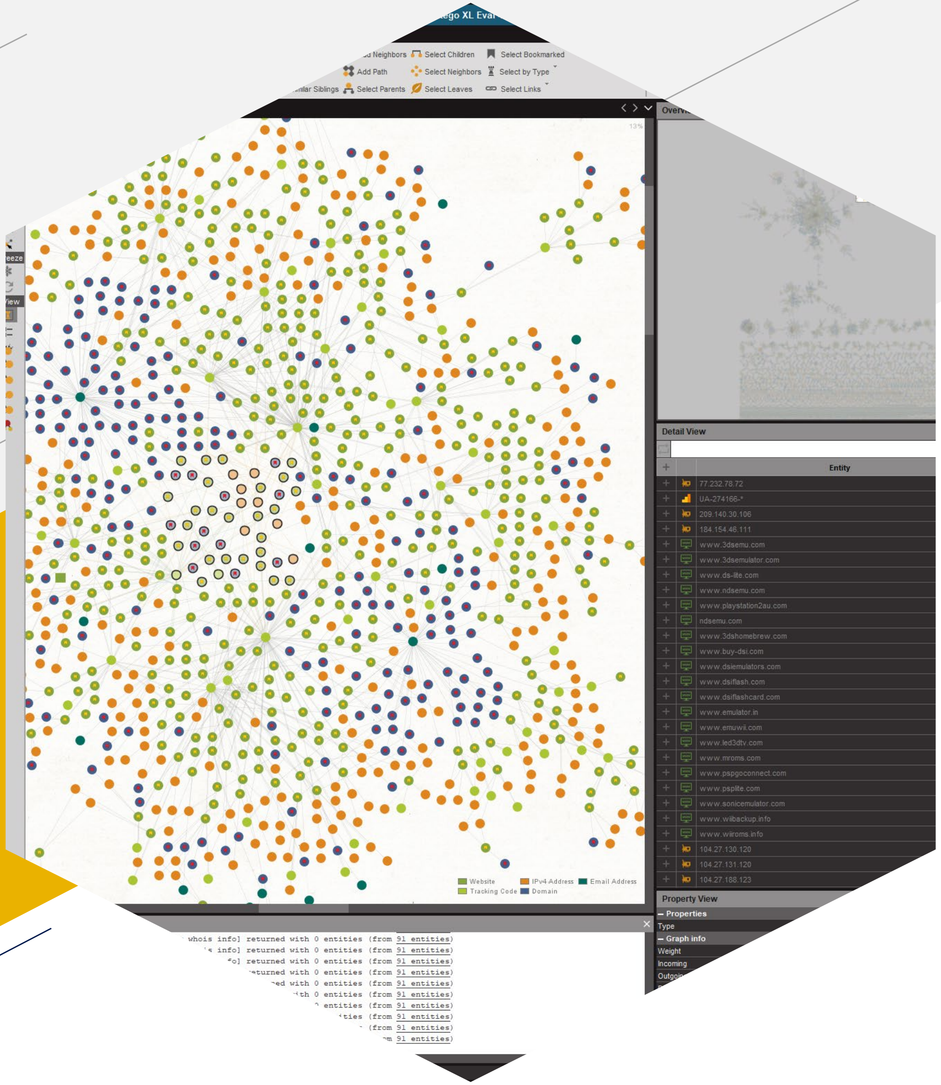
Status

– Properties

Description	<Different Values>
Status	Ready
Location	socialLinks
Default set	<none>
Input	<Different Values>
Output	Phrase [maltego.Phrase]

– Transform Inputs

WhoisXML API key	[redacted]



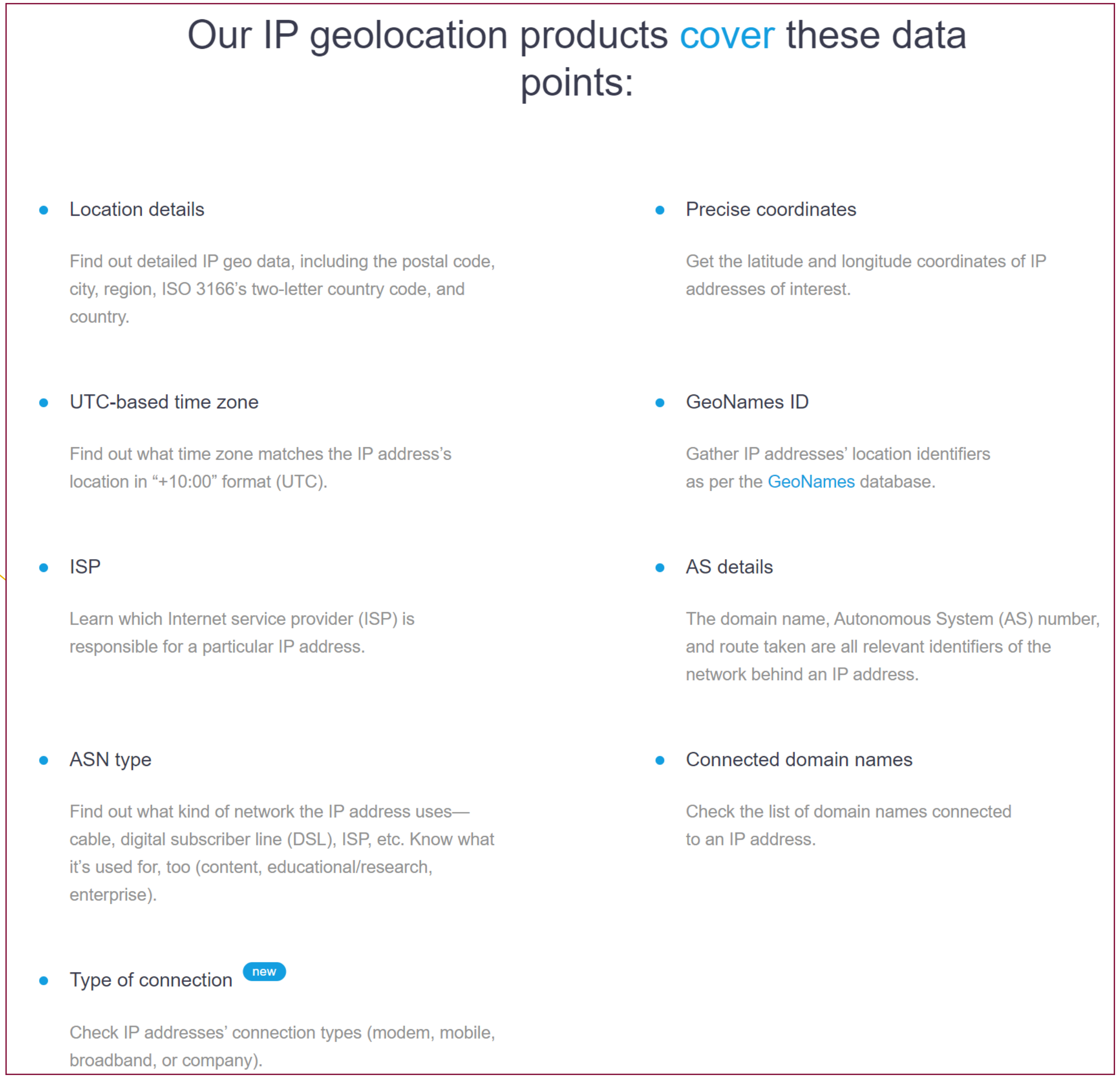
		Entity
+		77.232.78.72
+		UA-274166-*
+		209.140.30.106
+		184.154.46.111
+		www.3dsemu.com
+		www.3dsemulator.com
+		www.ds-lite.com
+		www.ndsemu.com
+		www.playstation2au.com
+		ndsemu.com
+		www.3dshomebrew.com
+		www.buy-dsi.com
+		www.dsiemulators.com
+		www.dsiflash.com
+		www.dsiflashcard.com
+		www.emulator.in
+		www.emuwii.com
+		www.led3dtv.com
+		www.mroms.com
+		www.pspgoconnect.com
+		www.psplite.com
+		www.sonicemulator.com
+		www.wiibackup.info
+		www.wiiroms.info
+		104.27.130.120
+		104.27.131.120
+		104.27.188.123

```
 whois info] returned with 0 entities (from 91 entities)
  is info] returned with 0 entities (from 91 entities)
     fo] returned with 0 entities (from 91 entities)
        eturned with 0 entities (from 91 entities)
           ed with 0 entities (from 91 entities)
              ith 0 entities (from 91 entities)
                  entities (from 91 entities)
                     ities (from 91 entities)
                           (from 91 entities)
                             om 91 entities)
```

14 New Transforms

Details

IP Geolocation



Our IP geolocation products cover these data points:

- Location details

  Find out detailed IP geo data, including the postal code, city, region, ISO 3166's two-letter country code, and country.

- UTC-based time zone

  Find out what time zone matches the IP address's location in "+10:00" format (UTC).

- ISP

  Learn which Internet service provider (ISP) is responsible for a particular IP address.

- ASN type

  Find out what kind of network the IP address uses—cable, digital subscriber line (DSL), ISP, etc. Know what it's used for, too (content, educational/research, enterprise).

- Type of connection new

  Check IP addresses' connection types (modem, mobile, broadband, or company).

- Precise coordinates

  Get the latitude and longitude coordinates of IP addresses of interest.

- GeoNames ID

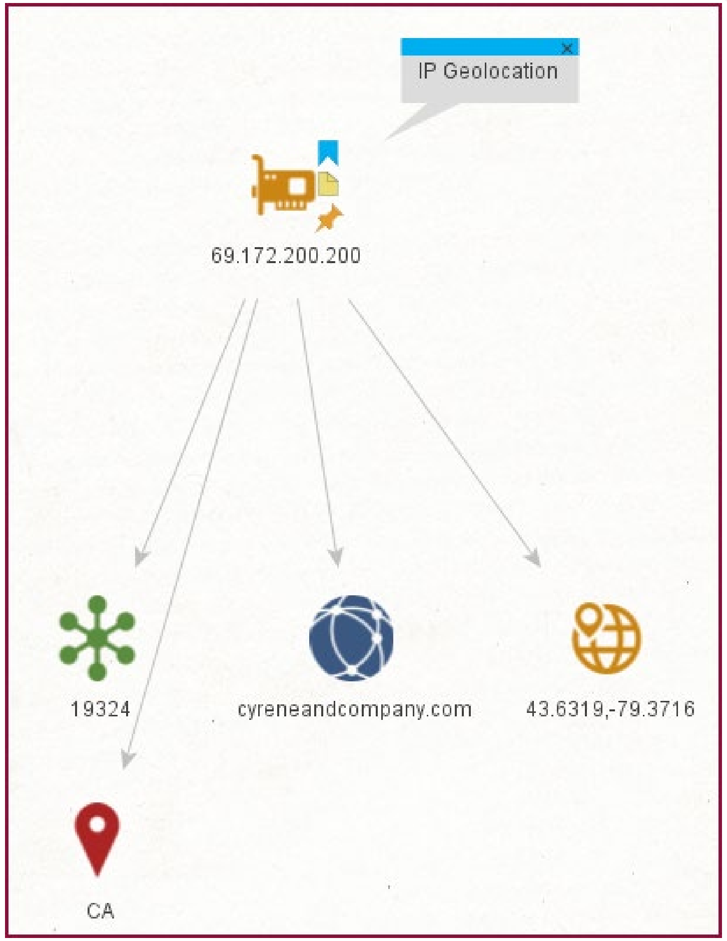
  Gather IP addresses' location identifiers as per the GeoNames database.

- AS details

  The domain name, Autonomous System (AS) number, and route taken are all relevant identifiers of the network behind an IP address.

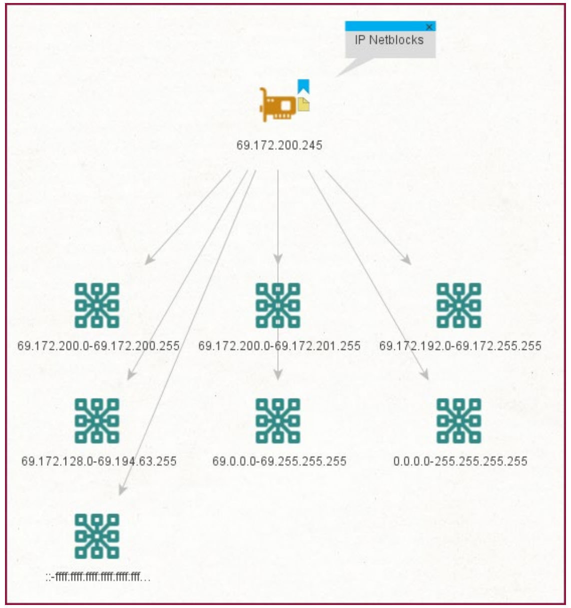
- Connected domain names

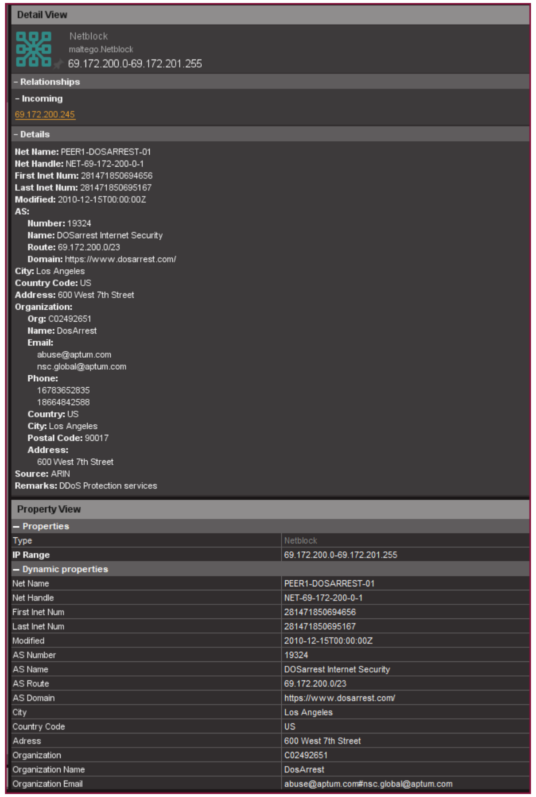
  Check the list of domain names connected to an IP address.



IP Netblocks

- Get detailed information about the IP range a particular IP belongs to
- With one API call get exhaustive information on the IP range that a given IP address belongs to, with detailed ownership information regarding each range.
- **Input**
  - AS [maltego.AS]
  - Company [maltego.company]
  - IPv4 Address [maltego.IPv4Address]
  - IPv6 Address [maltego.IPv6Address]
  - Phrase [maltego.Phrase]





Detail View

Netblock
maltego.Netblock
69.172.200.0-69.172.201.255

– Relationships

– Incoming

69.172.200.245

– Details

Net Name: PEER1-DOSARREST-01
Net Handle: NET-69-172-200-0-1
First Inet Num: 281471850694656
Last Inet Num: 281471850695167
Modified: 2010-12-15T00:00:00Z
AS:
  Number: 19324
  Name: DOSarrest Internet Security
  Route: 69.172.200.0/23
  Domain: https://www.dosarrest.com/
City: Los Angeles
Country Code: US
Address: 600 West 7th Street
Organization:
  Org: C02492651
  Name: DosArrest
  Email:
    abuse@aptum.com
    nsc.global@aptum.com
  Phone:
    16783652835
    18664842588
  Country: US
  City: Los Angeles
  Postal Code: 90017
  Address:
    600 West 7th Street
Source: ARIN
Remarks: DDoS Protection services

Property View

– Properties

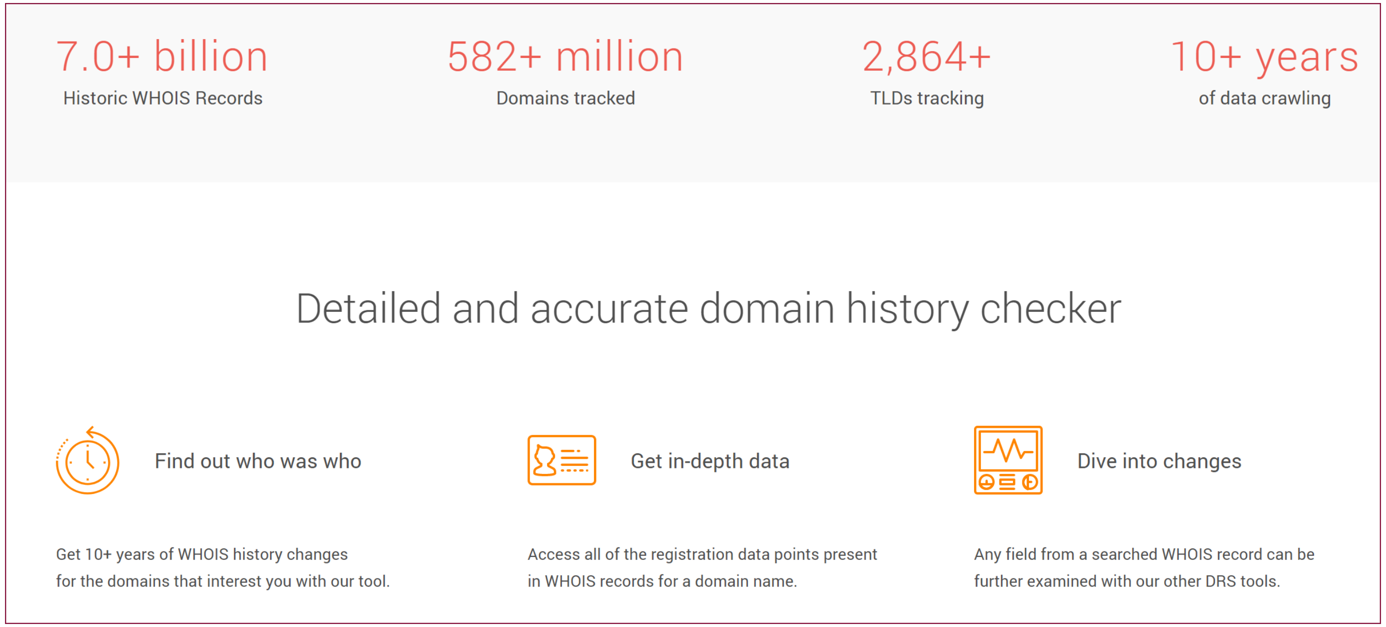
Type	Netblock
IP Range	69.172.200.0-69.172.201.255

– Dynamic properties

Net Name	PEER1-DOSARREST-01
Net Handle	NET-69-172-200-0-1
First Inet Num	281471850694656
Last Inet Num	281471850695167
Modified	2010-12-15T00:00:00Z
AS Number	19324
AS Name	DOSarrest Internet Security
AS Route	69.172.200.0/23
AS Domain	https://www.dosarrest.com/
City	Los Angeles
Country Code	US
Adress	600 West 7th Street
Organization	C02492651
Organization Name	DosArrest
Organization Email	abuse@aptum.com#nsc.global@aptum.com

Whois / Whois History

- WHOIS History Search is a tool that gives users access to complete historical WHOIS records, including **domain ownership and registrar information over time**. We have tracked the history of millions of domain names for **more than 10 years**. All relevant historical WHOIS changes are recorded in our database and accessible via our domain history checker and other WHOIS History products.



7.0+ billion
Historic WHOIS Records

582+ million
Domains tracked

2,864+
TLDs tracking

10+ years
of data crawling

Detailed and accurate domain history checker

Find out who was who

Get 10+ years of WHOIS history changes for the domains that interest you with our tool.

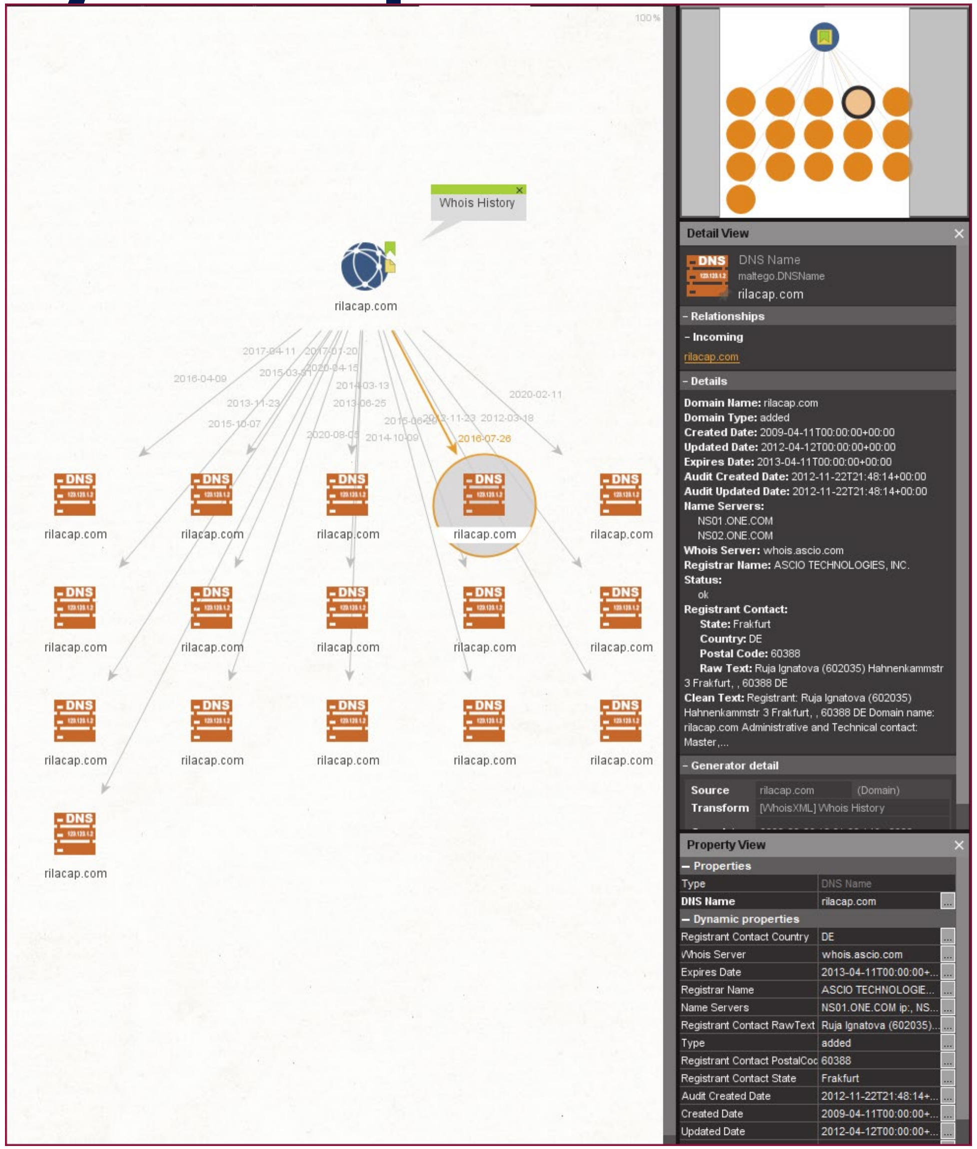
Get in-depth data

Access all of the registration data points present in WHOIS records for a domain name.

Dive into changes

Any field from a searched WHOIS record can be further examined with our other DRS tools.

Whois History -Sample-



Detail View

DNS Name
maltego.DNSName
rilacap.com

- Relationships

- Incoming

rilacap.com

- Details

Domain Name: rilacap.com
Domain Type: added
Created Date: 2009-04-11T00:00:00+00:00
Updated Date: 2012-04-12T00:00:00+00:00
Expires Date: 2013-04-11T00:00:00+00:00
Audit Created Date: 2012-11-22T21:48:14+00:00
Audit Updated Date: 2012-11-22T21:48:14+00:00
Name Servers:
NS01.ONE.COM
NS02.ONE.COM
Whois Server: whois.ascio.com
Registrar Name: ASCIO TECHNOLOGIES, INC.
Status:
ok
Registrant Contact:
State: Frakfurt
Country: DE
Postal Code: 60388
Raw Text: Ruja Ignatova (602035) Hahnenkammstr 3 Frakfurt, , 60388 DE
Clean Text: Registrant: Ruja Ignatova (602035) Hahnenkammstr 3 Frakfurt, , 60388 DE Domain name: rilacap.com Administrative and Technical contact: Master,...

- Generator detail

Source	rilacap.com	(Domain)
Transform	[WhoisXML] Whois History	

Property View

– Properties

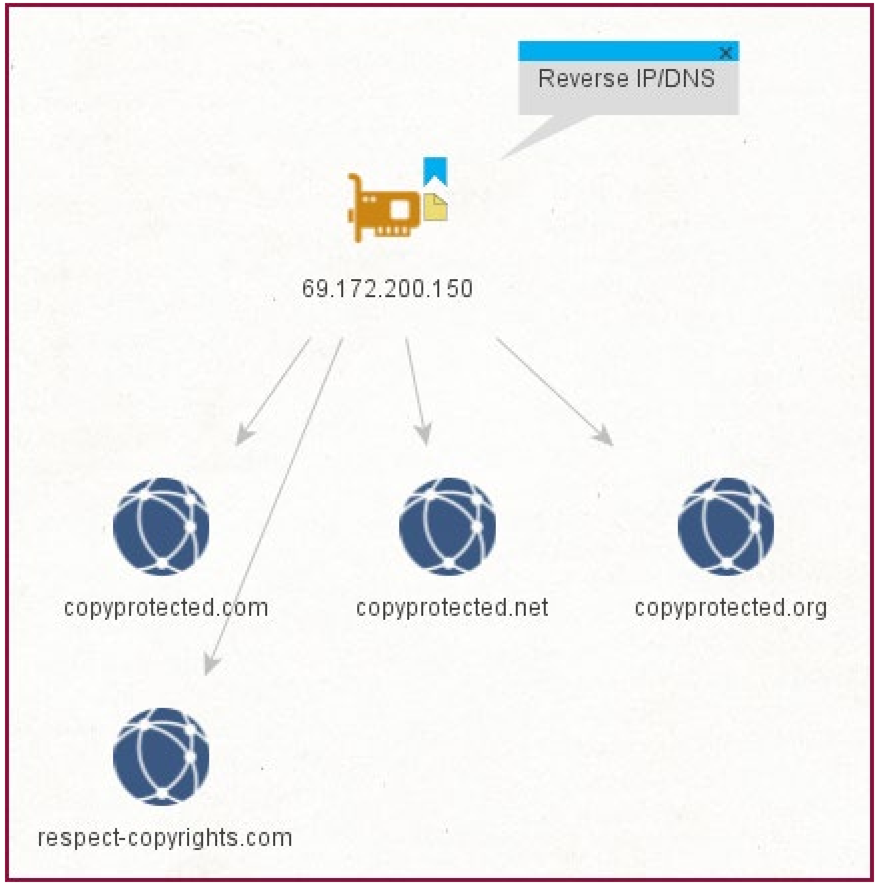
Type	DNS Name
DNS Name	rilacap.com

– Dynamic properties

Registrant Contact Country	DE
Whois Server	whois.ascio.com
Expires Date	2013-04-11T00:00:00+...
Registrar Name	ASCIO TECHNOLOGIE...
Name Servers	NS01.ONE.COM ip:, NS...
Registrant Contact RawText	Ruja Ignatova (602035)...
Type	added
Registrant Contact PostalCoc	60388
Registrant Contact State	Frakfurt
Audit Created Date	2012-11-22T21:48:14+...
Created Date	2009-04-11T00:00:00+...
Updated Date	2012-04-12T00:00:00+...

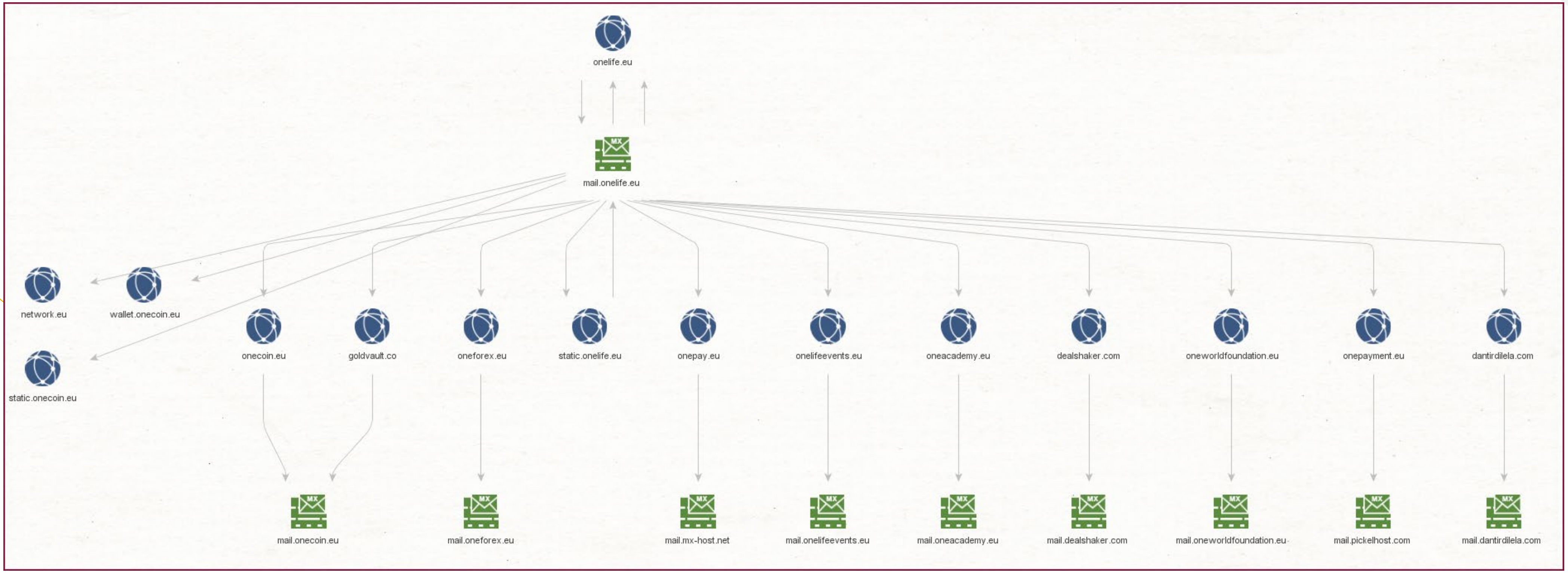
Reverse IP/DNS

- Reverse IP & DNS API reveals all domains that share an IP address in a single API call



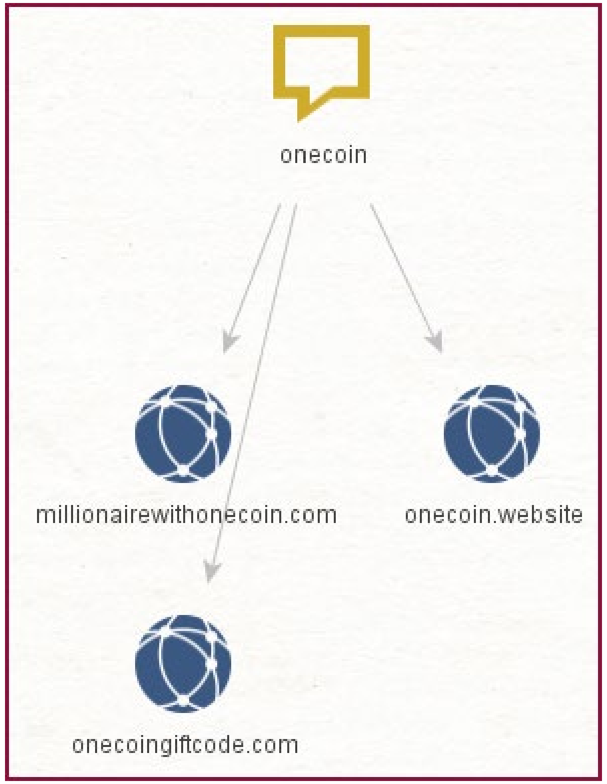
Reverse MX / NS

- We provide results pulled from the world's largest and constantly updated DNS database with information on 1,771,916,995 domains and subdomains, 142,703,533 MX records updated daily.



Brand Alert

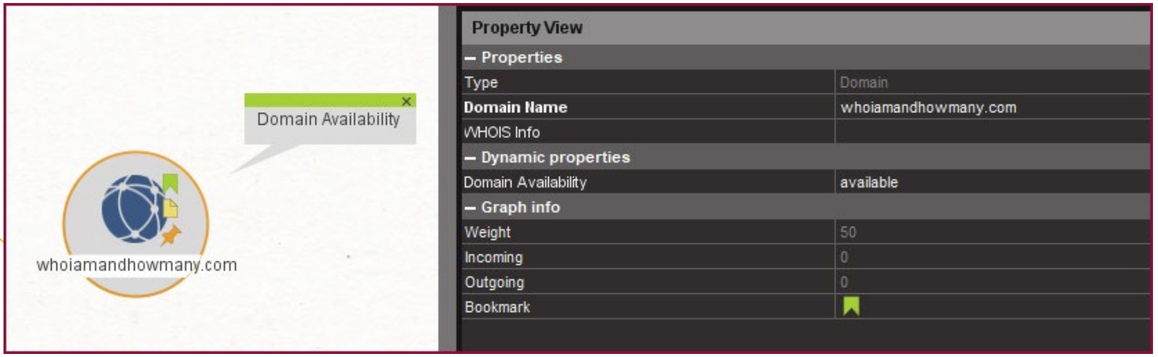
- Brand Alert API searches across all recently registered & deleted domain names and returns result sets consisting of domain names that contain term(s) that are specified by you.
- Input:
  - Phrase [maltego.Phrase]



Domain Availability

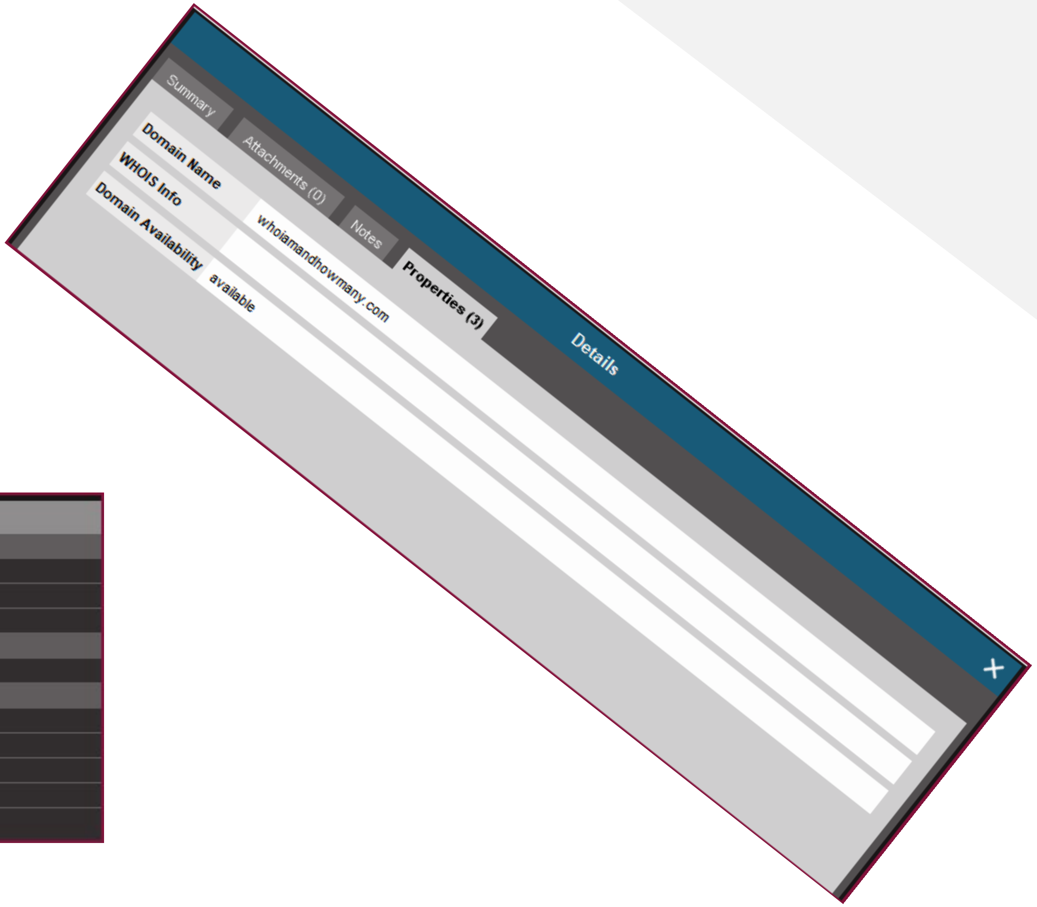
- Checks domain availability for registration.

- This API works for nearly all top-level domains (TLDs).



Property View

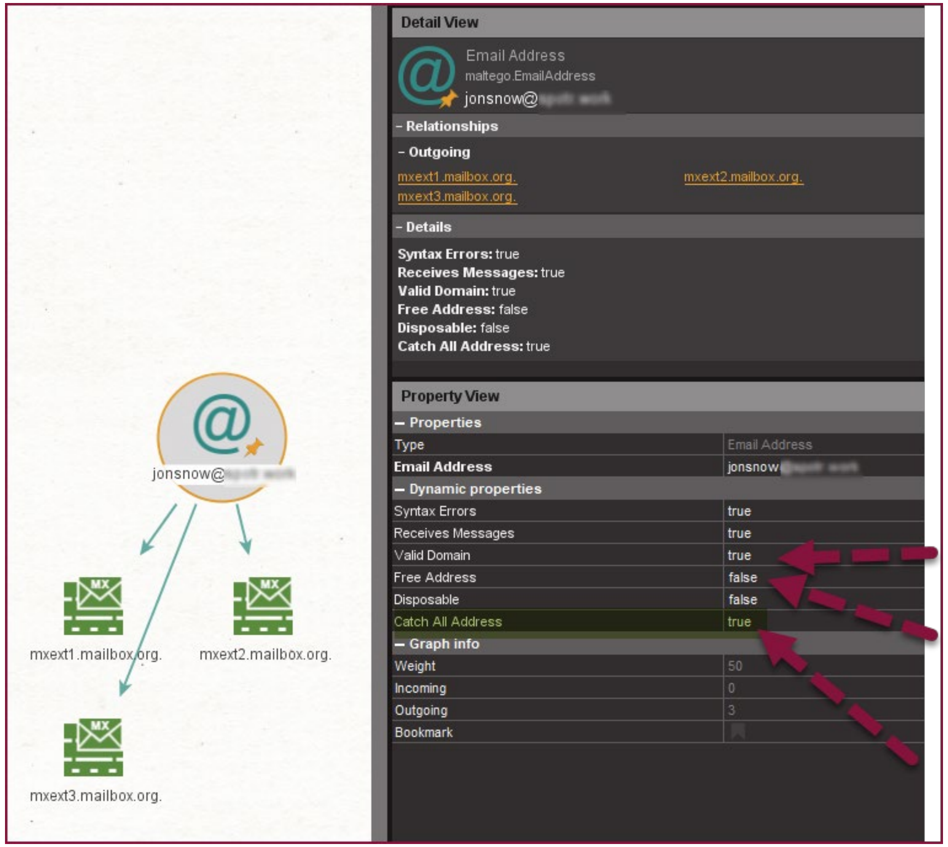
– Properties	
Type	Domain
Domain Name	whoiamandhowmany.com
WHOIS Info	
– Dynamic properties	
Domain Availability	available
– Graph info	
Weight	50
Incoming	0
Outgoing	0
Bookmark	🔖



Domain Name	whoiamandhowmany.com
WHOIS Info	
Domain Availability	available

Email Verification

- Use Email Verification API to verify the existence, validity & quality of any email address
- Email Verification API performs a comprehensive validation of email addresses in real-time and conveniently. Verify the email addresses coming from new user registrations, reduce email bouncing, block spam, and more.



Detail View

Email Address
maltego.EmailAddress
jonsnow@[redacted]

- Relationships
- Outgoing

mxext1.mailbox.org. mxext2.mailbox.org.
mxext3.mailbox.org.

- Details

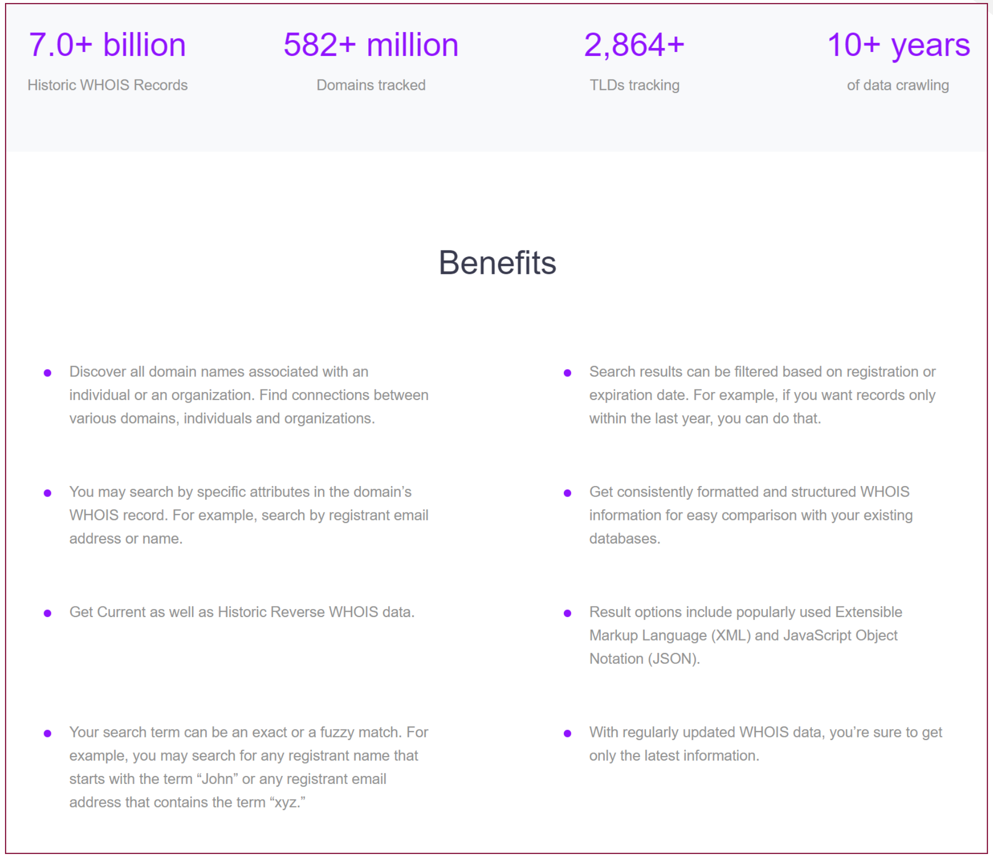
Syntax Errors: true
Receives Messages: true
Valid Domain: true
Free Address: false
Disposable: false
Catch All Address: true

Property View

– Properties	
Type	Email Address
Email Address	jonsnow[redacted]
– Dynamic properties	
Syntax Errors	true
Receives Messages	true
Valid Domain	true
Free Address	false
Disposable	false
Catch All Address	true
– Graph info	
Weight	50
Incoming	0
Outgoing	3
Bookmark	

Reverse Whois

- Find all domain names which contain a specified search terms in their WHOIS records
- With one API call for search terms such as a domain owner’s name, email address, phone number, postal address, etc., you will get a list of all the linked domains that contain the identifier.

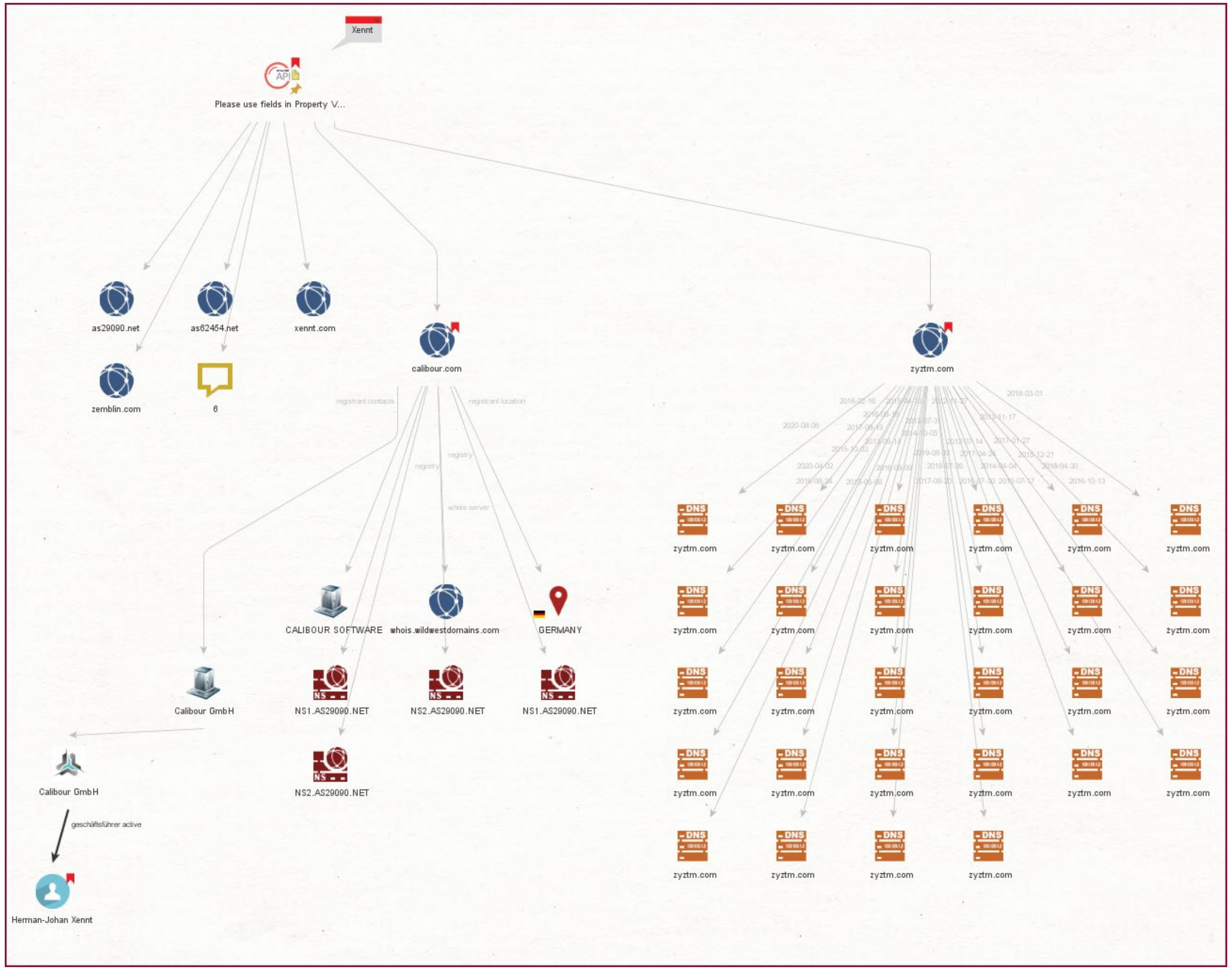


7.0+ billion	582+ million	2,864+	10+ years
Historic WHOIS Records	Domains tracked	TLDs tracking	of data crawling

Benefits

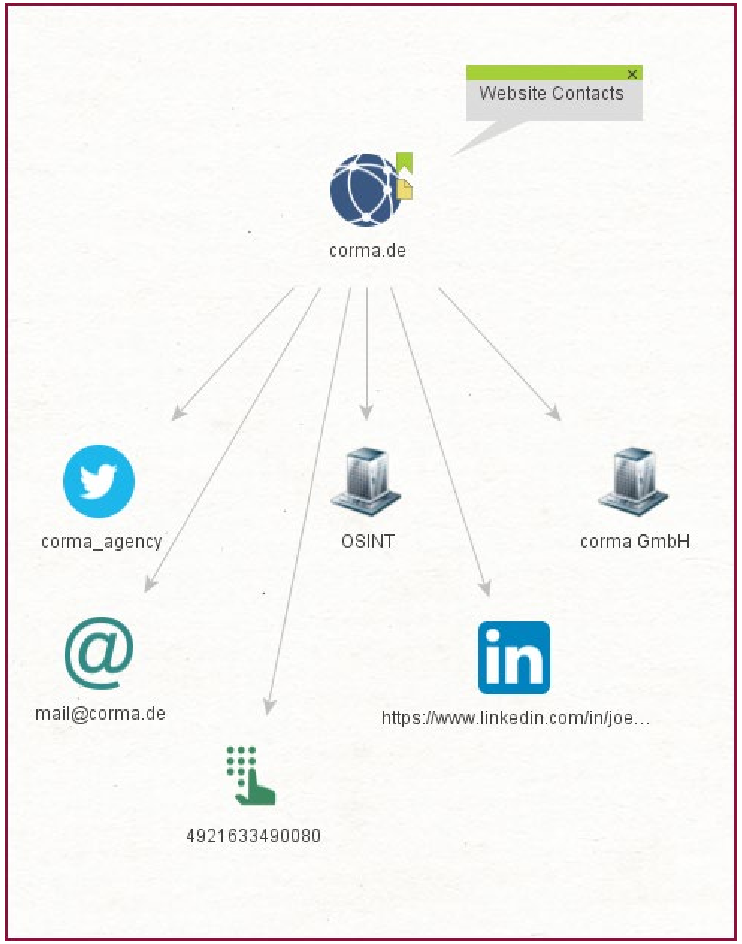
- Discover all domain names associated with an individual or an organization. Find connections between various domains, individuals and organizations.
- You may search by specific attributes in the domain’s WHOIS record. For example, search by registrant email address or name.
- Get Current as well as Historic Reverse WHOIS data.
- Your search term can be an exact or a fuzzy match. For example, you may search for any registrant name that starts with the term “John” or any registrant email address that contains the term “xyz.”
- Search results can be filtered based on registration or expiration date. For example, if you want records only within the last year, you can do that.
- Get consistently formatted and structured WHOIS information for easy comparison with your existing databases.
- Result options include popularly used Extensible Markup Language (XML) and JavaScript Object Notation (JSON).
- With regularly updated WHOIS data, you’re sure to get only the latest information.

Reverse Whois Sample „cyberbunker“



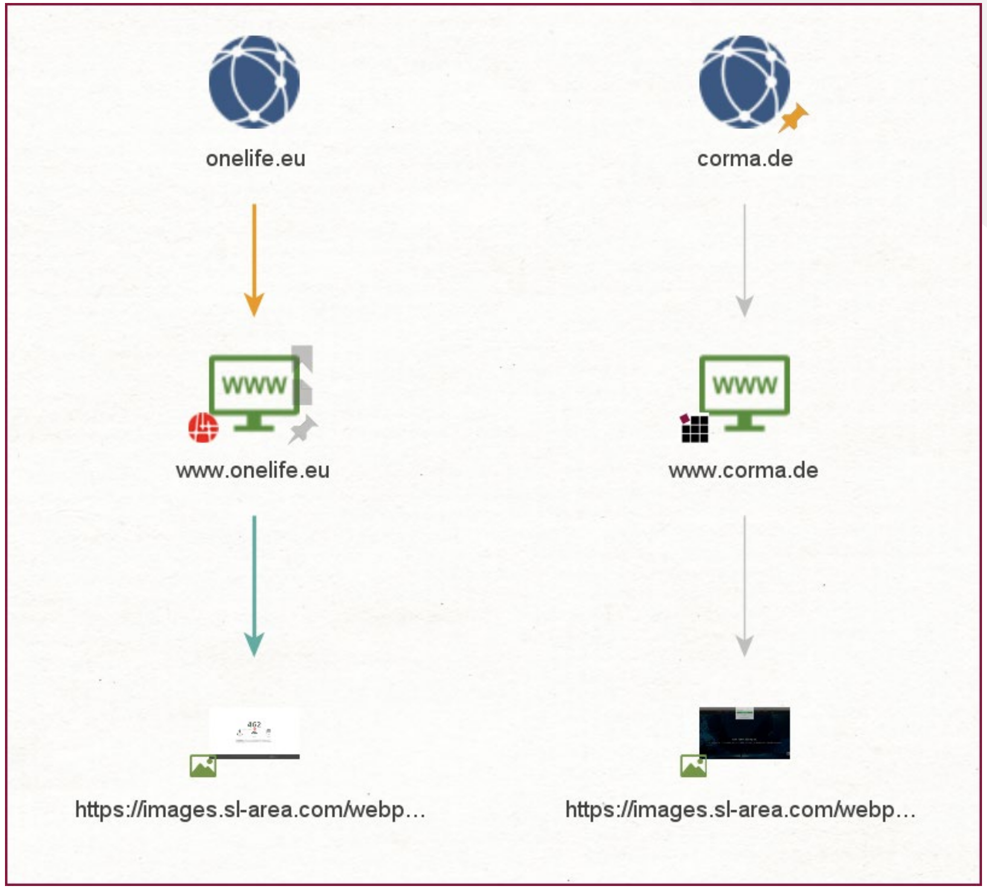
Website Contacts

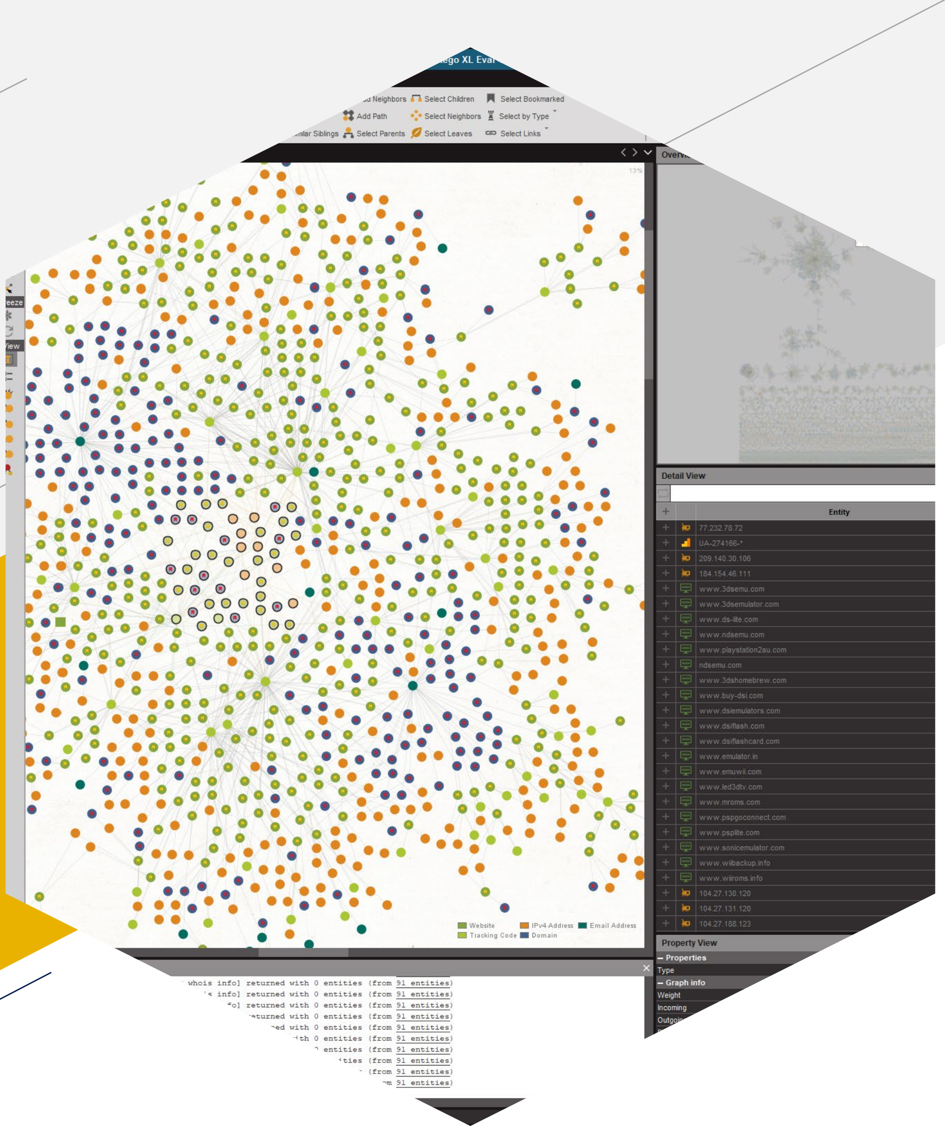
- Get full contact information from 235+ million active domain names
- Get well-structured domain owners' contact information including the company name its key contacts together with direct-dialphone numbers, email addresses, social links based on the data parsed from website content, social networks, SSL certificates and other sources.



Website Screenshots

- **Get a screenshot of any web page with one** API call
- Google Chrome engine-based Screenshot API allows you to instantly get a screenshot of any web page as a jpg, png or PDF file with embedded links which you can easily integrate into your product or use for any other business purposes.


onelife.eu
corma.de
www.onelife.eu
www.corma.de
https://images.sl-area.com/webp...
https://images.sl-area.com/webp...



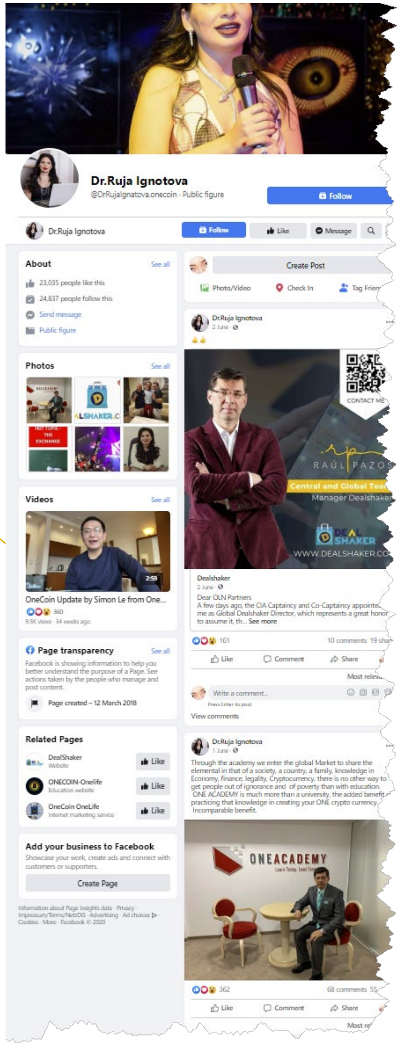
Entity
77.232.78.72
UA-274166-*
209.140.30.106
184.154.46.111
www.3dsemu.com
www.3dsemulator.com
www.ds-lite.com
www.ndsemu.com
www.playstation2au.com
ndsemu.com
www.3dshomebrew.com
www.buy-dsi.com
www.dsiemulators.com
www.dsiflash.com
www.dsiflashcard.com
www.emulator.in
www.emuwii.com
www.led3dtv.com
www.mroms.com
www.pspgoconnect.com
www.psplite.com
www.sonicemulator.com
www.wiibackup.info
www.wiiroms.info
104.27.130.120
104.27.131.120
104.27.188.123

```
 whois info] returned with 0 entities (from 91 entities)
        s info] returned with 0 entities (from 91 entities)
           fo] returned with 0 entities (from 91 entities)
               eturned with 0 entities (from 91 entities)
                     ed with 0 entities (from 91 entities)
                          ith 0 entities (from 91 entities)
                                entities (from 91 entities)
                                    ities (from 91 entities)
                                          (from 91 entities)
                                             m 91 entities)
```

Case Study Cryptoqueen – Where is Dr. Ruja?

some first investigative steps

Introducing: Dr. Ruja Ignatova



Dr.Ruja Ignotova
@DrRujaIgnatova.onecoin · Public figure

About See all
- 23,035 people like this
- 24,837 people follow this
- Send message
- Public figure

Photos See all

Videos See all

OneCoin Update by Simon Le from One...
360
9.5K views · 34 weeks ago

Page transparency See all

Facebook is showing information to help you better understand the purpose of a Page. See actions taken by the people who manage and post content.

Page created – 12 March 2018

Related Pages
- DealShaker Website — Like
- ONECOIN-Onelife Education website — Like
- OneCoin OneLife Internet marketing service — Like

Add your business to Facebook
Showcase your work, create ads and connect with customers or supporters.
Create Page

Information about Page Insights data · Privacy · Impressum/Terms/NetzDG · Advertising · Ad choices · Cookies · More · Facebook © 2020

Dr.Ruja Ignotova
2 June

Dealshaker
2 June
Dear OLN Partners
A few days ago, the CIA Captaincy and Co-Captaincy appointe me as Global Dealshaker Director, which represents a great honor to assume it, th... See more

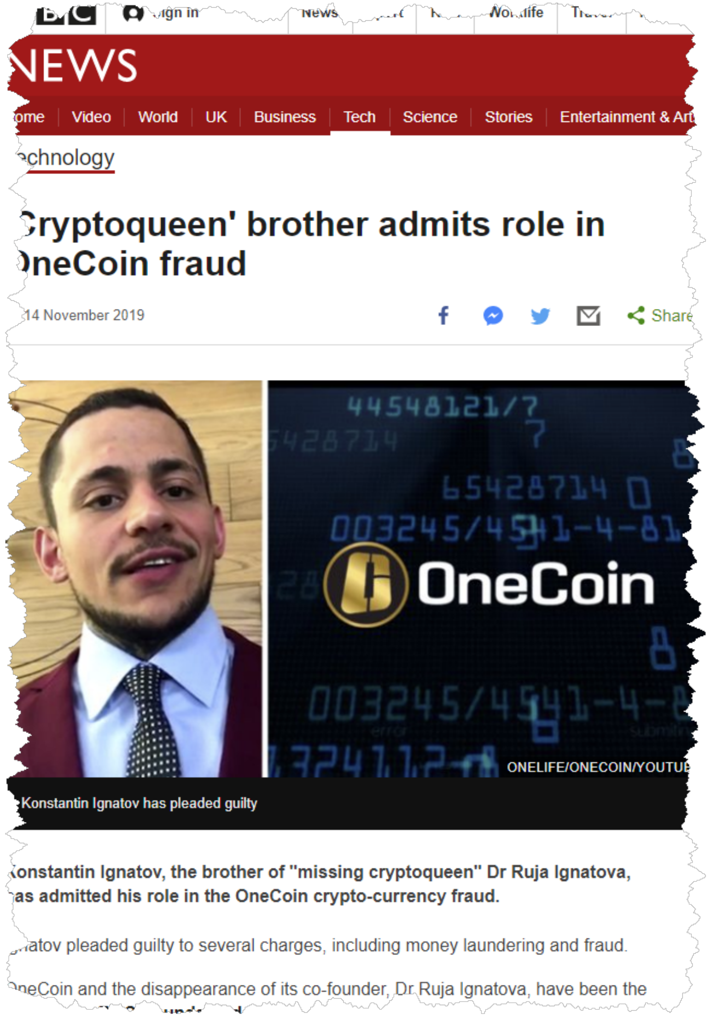
161 · 10 comments 19 sha

Like · Comment · Share
Most relev
Write a comment...
Press Enter to post
View comments

Dr.Ruja Ignotova
1 June
Through the academy we enter the global Market to share the elemental in that of a society, a country, a family, knowledge in Economy, finance, legality, Cryptocurrency, there is no other way to get people out of ignorance and of poverty than with education. ONE ACADEMY is much more than a university, the added benefit o practicing that knowledge in creating your ONE crypto currency. Incomparable benefit.

362 · 68 comments 55

Like · Comment · Share
Most re



echnology

'Cryptoqueen' brother admits role in OneCoin fraud

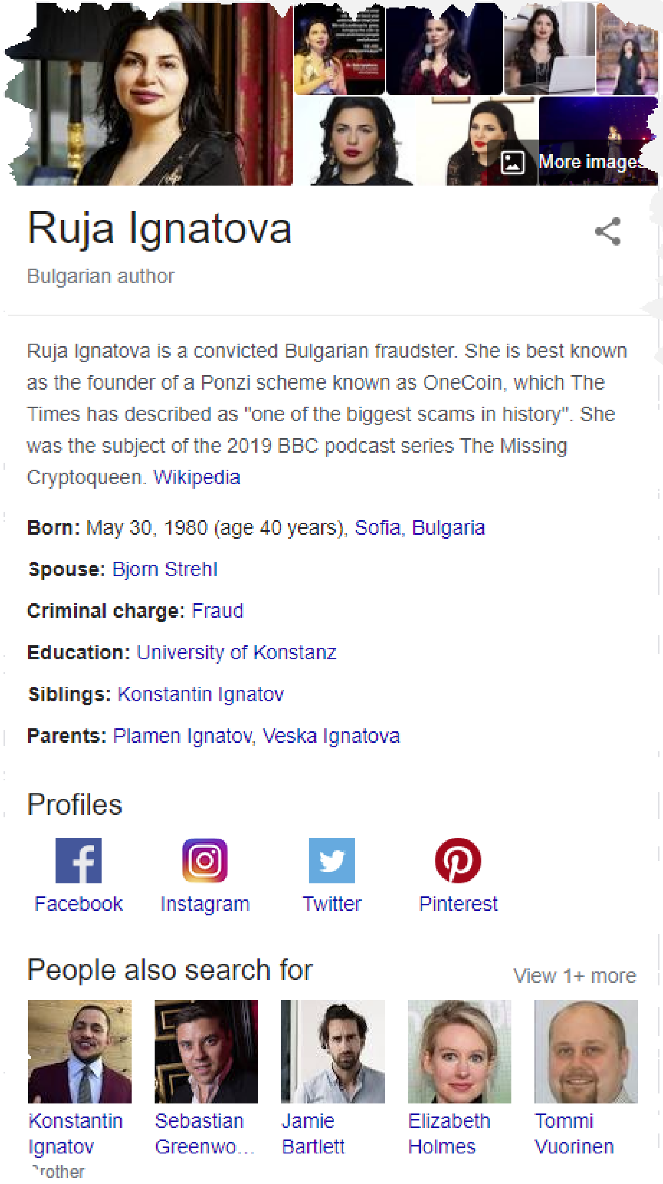
14 November 2019

Konstantin Ignatov has pleaded guilty

Konstantin Ignatov, the brother of "missing cryptoqueen" Dr Ruja Ignatova, has admitted his role in the OneCoin crypto-currency fraud.

Ignatov pleaded guilty to several charges, including money laundering and fraud.

OneCoin and the disappearance of its co-founder, Dr Ruja Ignatova, have been the



Ruja Ignatova

Bulgarian author

Ruja Ignatova is a convicted Bulgarian fraudster. She is best known as the founder of a Ponzi scheme known as OneCoin, which The Times has described as "one of the biggest scams in history". She was the subject of the 2019 BBC podcast series The Missing Cryptoqueen. Wikipedia

Born: May 30, 1980 (age 40 years), Sofia, Bulgaria

Spouse: Bjorn Strehl

Criminal charge: Fraud

Education: University of Konstanz

Siblings: Konstantin Ignatov

Parents: Plamen Ignatov, Veska Ignatova

Profiles

Facebook · Instagram · Twitter · Pinterest

People also search for

View 1+ more

Konstantin Ignatov
Brother

Sebastian Greenwo...

Jamie Bartlett

Elizabeth Holmes

Tommi Vuorinen

The beginning of the hunt

25 October 2017 is a grey day in Sofia. Dr. Ruja Ignatova has packed her things.

Outside light drizzle, it is fresh. When she arrives at the airport, the temperature continues to drop.

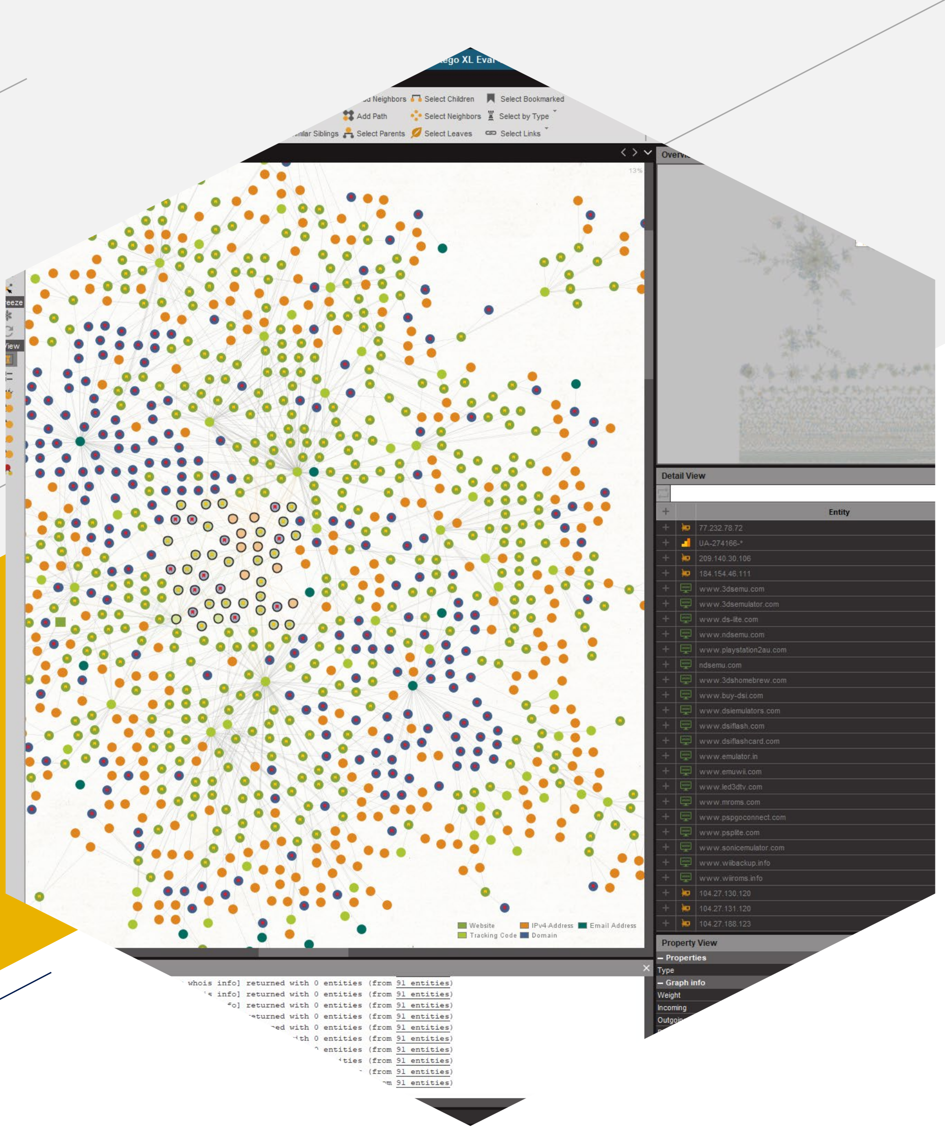
Ruja goes to the counter of Ryan Air and checks in to Athens.

The ticket was bought by Konstantin Ignatov, her younger brother and later successor.

Dr. Ruja, who used to travel in private jets, squeezes herself into one of the narrow budget seats.

On this autumn day, a Wednesday, she lands in Athens a good hour later and is met by two Russian-speaking men.

Since then, there has been no trace of what is probably the world's greatest female con artist.



Entity
77.232.78.72
UA-274166-*
209.140.30.106
184.154.46.111
www.3dsemu.com
www.3dsemulator.com
www.ds-lite.com
www.ndsemu.com
www.playstation2au.com
ndsemu.com
www.3dshomebrew.com
www.buy-dsi.com
www.dsiemulators.com
www.dsiflash.com
www.dsiflashcard.com
www.emulator.in
www.emuwii.com
www.led3dtv.com
www.mroms.com
www.pspgoconnect.com
www.psplite.com
www.sonicemulator.com
www.wiibackup.info
www.wiiroms.info
104.27.130.120
104.27.131.120
104.27.188.123

```
whois info] returned with 0 entities (from 91 entities)
 's info] returned with 0 entities (from 91 entities)
      fo] returned with 0 entities (from 91 entities)
          eturned with 0 entities (from 91 entities)
              ed with 0 entities (from 91 entities)
                  ith 0 entities (from 91 entities)
                        entities (from 91 entities)
                             ities (from 91 entities)
                                    (from 91 entities)
                                       m 91 entities)
```

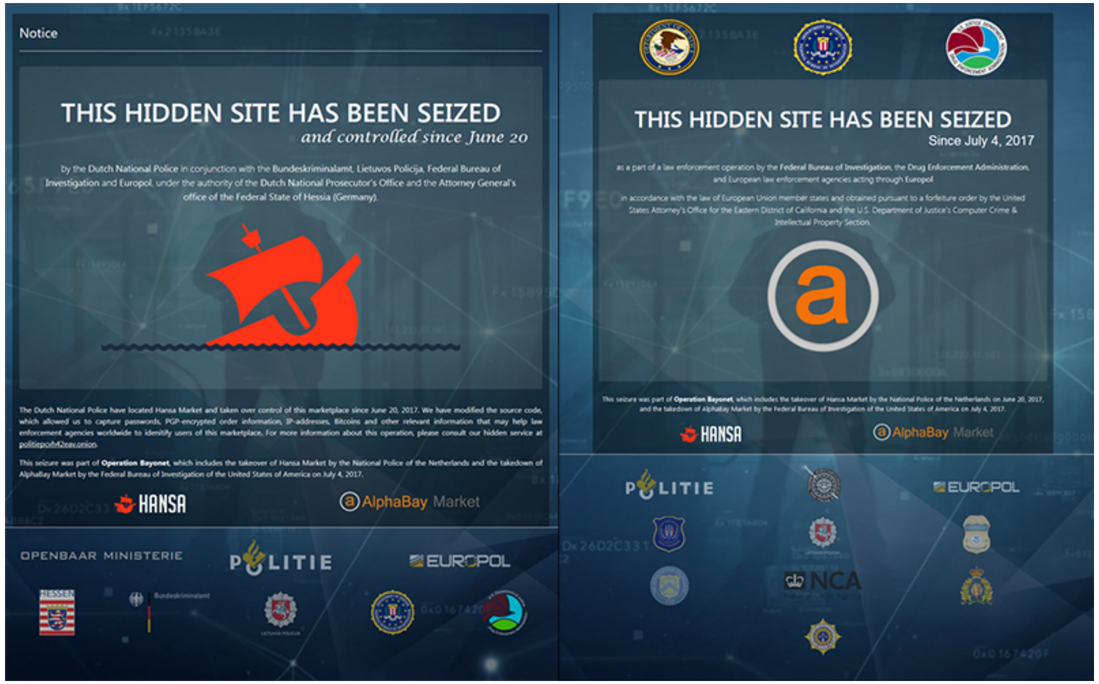
Case Study Operation Bayonet – What can we find in Whois History?

Back into the dark corners of the Internet

Operation Bayonet

- Operation Bayonet was a multinational law enforcement operation culminating in 2017 targeting the AlphaBay and Hansa darknet markets. Many other darknet markets were also shut down.

source: Wikipedia / europol



Notice

THIS HIDDEN SITE HAS BEEN SEIZED
and controlled since June 20

by the Dutch National Police in conjunction with the Bundeskriminalamt, Lietuvos Policija, Federal Bureau of Investigation and Europol, under the authority of the Dutch National Prosecutor's Office and the Attorney General's office of the Federal State of Hessia (Germany).

The Dutch National Police have located Hansa Market and taken over control of this marketplace since June 20, 2017. We have modified the source code, which allowed us to capture passwords, PGP-encrypted order information, IP-addresses, Bitcoins and other relevant information that may help law enforcement agencies worldwide to identify users of this marketplace. For more information about this operation, please consult our hidden service at politiepcvh42eav.onion.

This seizure was part of **Operation Bayonet**, which includes the takeover of Hansa Market by the National Police of the Netherlands and the takedown of AlphaBay Market by the Federal Bureau of Investigation of the United States of America on July 4, 2017.

THIS HIDDEN SITE HAS BEEN SEIZED
Since July 4, 2017

as a part of a law enforcement operation by the Federal Bureau of Investigation, the Drug Enforcement Administration, and European law enforcement agencies acting through Europol

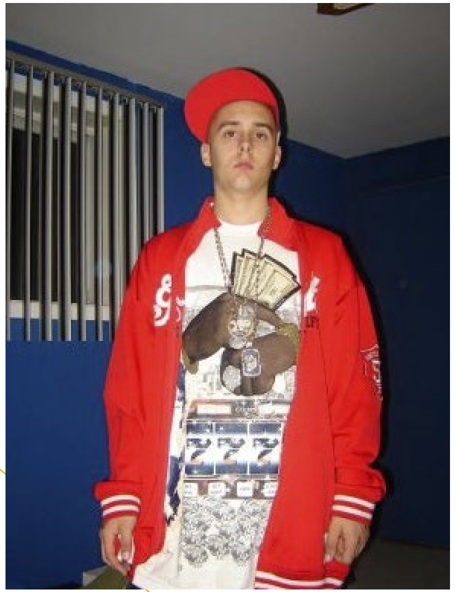
in accordance with the law of European Union member states and obtained pursuant to a forfeiture order by the United States Attorney's Office for the Eastern District of California and the U.S. Department of Justice's Computer Crime & Intellectual Property Section.

This seizure was part of **Operation Bayonet**, which includes the takeover of Hansa Market by the National Police of the Netherlands on June 20, 2017, and the takedown of AlphaBay Market by the Federal Bureau of Investigation of the United States of America on July 4, 2017.

> “THE QUALITY REALLY WENT UP. EVERYONE WAS VERY SATISFIED WITH THE LEVEL OF SERVICE THEY GOT.”
>
> GERT RAS,
> HEAD OF THE NETHERLANDS
> NATIONAL HIGH TECH CRIME UNIT

„Mastermind“ Alexandre Cazes

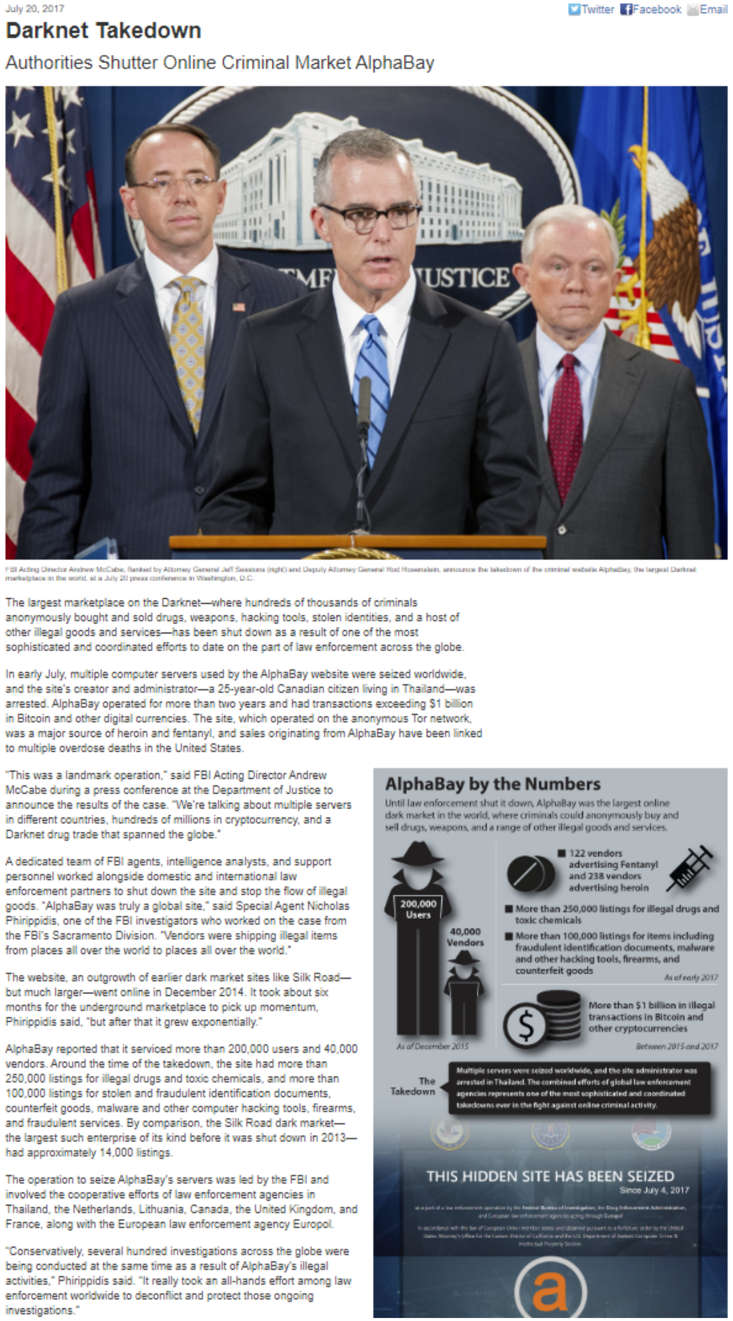
- Age of 17:



- Age of 25:

- last image

Takedown



July 20, 2017

Twitter Facebook Email

Darknet Takedown

Authorities Shutter Online Criminal Market AlphaBay

FBI Acting Director Andrew McCabe, flanked by Attorney General Jeff Sessions (right) and Deputy Attorney General Rod Rosenstein, announce the takedown of the criminal website AlphaBay, the largest Darknet marketplace in the world, at a July 20 press conference in Washington, D.C.

The largest marketplace on the Darknet—where hundreds of thousands of criminals anonymously bought and sold drugs, weapons, hacking tools, stolen identities, and a host of other illegal goods and services—has been shut down as a result of one of the most sophisticated and coordinated efforts to date on the part of law enforcement across the globe.

In early July, multiple computer servers used by the AlphaBay website were seized worldwide, and the site's creator and administrator—a 25-year-old Canadian citizen living in Thailand—was arrested. AlphaBay operated for more than two years and had transactions exceeding $1 billion in Bitcoin and other digital currencies. The site, which operated on the anonymous Tor network, was a major source of heroin and fentanyl, and sales originating from AlphaBay have been linked to multiple overdose deaths in the United States.

"This was a landmark operation," said FBI Acting Director Andrew McCabe during a press conference at the Department of Justice to announce the results of the case. "We're talking about multiple servers in different countries, hundreds of millions in cryptocurrency, and a Darknet drug trade that spanned the globe."

A dedicated team of FBI agents, intelligence analysts, and support personnel worked alongside domestic and international law enforcement partners to shut down the site and stop the flow of illegal goods. "AlphaBay was truly a global site," said Special Agent Nicholas Phirippidis, one of the FBI investigators who worked on the case from the FBI's Sacramento Division. "Vendors were shipping illegal items from places all over the world to places all over the world."

The website, an outgrowth of earlier dark market sites like Silk Road—but much larger—went online in December 2014. It took about six months for the underground marketplace to pick up momentum, Phirippidis said, "but after that it grew exponentially."

AlphaBay reported that it serviced more than 200,000 users and 40,000 vendors. Around the time of the takedown, the site had more than 250,000 listings for illegal drugs and toxic chemicals, and more than 100,000 listings for stolen and fraudulent identification documents, counterfeit goods, malware and other computer hacking tools, firearms, and fraudulent services. By comparison, the Silk Road dark market—the largest such enterprise of its kind before it was shut down in 2013—had approximately 14,000 listings.

The operation to seize AlphaBay's servers was led by the FBI and involved the cooperative efforts of law enforcement agencies in Thailand, the Netherlands, Lithuania, Canada, the United Kingdom, and France, along with the European law enforcement agency Europol.

"Conservatively, several hundred investigations across the globe were being conducted at the same time as a result of AlphaBay's illegal activities," Phirippidis said. "It really took an all-hands effort among law enforcement worldwide to deconflict and protect those ongoing investigations."

AlphaBay by the Numbers

Until law enforcement shut it down, AlphaBay was the largest online dark market in the world, where criminals could anonymously buy and sell drugs, weapons, and a range of other illegal goods and services.

200,000 Users

40,000 Vendors

As of December 2015

- 122 vendors advertising Fentanyl and 238 vendors advertising heroin
- More than 250,000 listings for illegal drugs and toxic chemicals
- More than 100,000 listings for items including fraudulent identification documents, malware and other hacking tools, firearms, and counterfeit goods

As of early 2017

More than $1 billion in illegal transactions in Bitcoin and other cryptocurrencies

Between 2015 and 2017

The Takedown

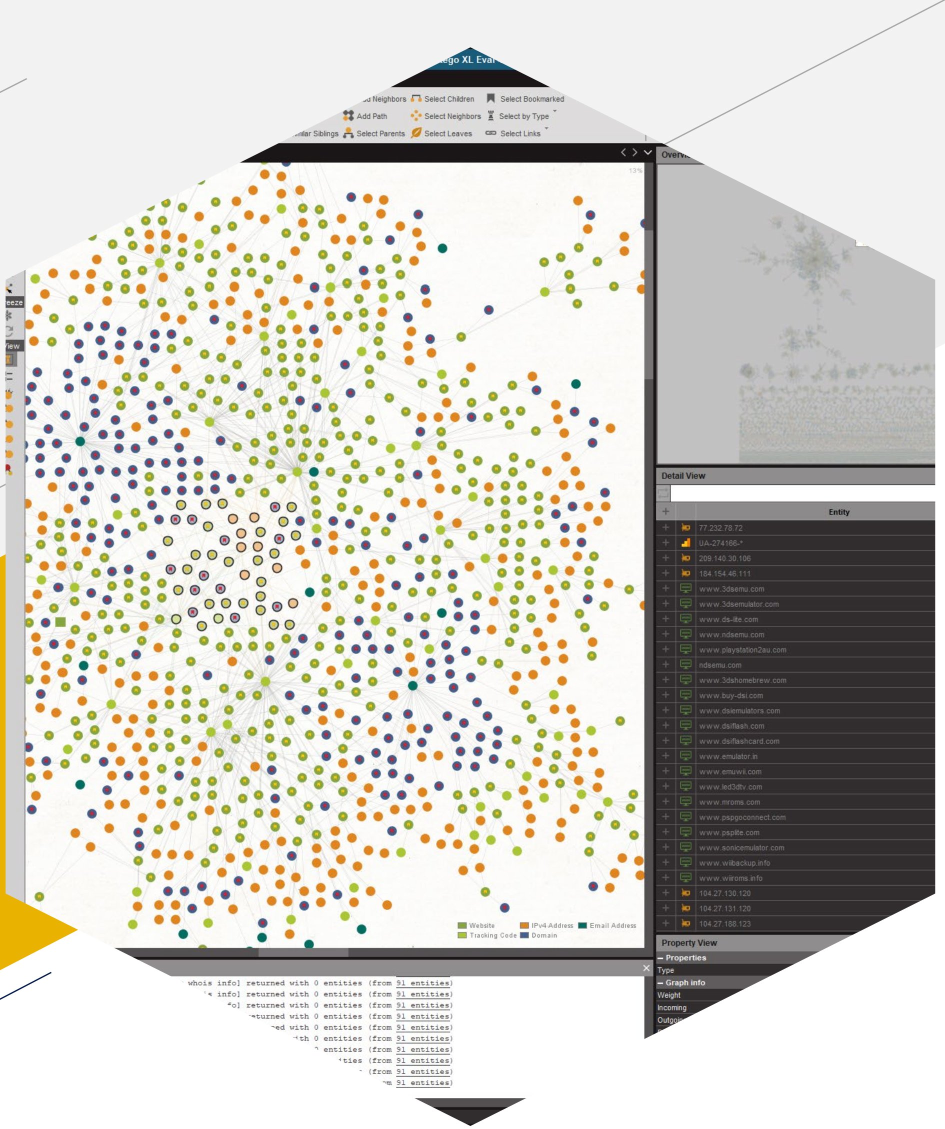
Multiple servers were seized worldwide, and the site administrator was arrested in Thailand. The combined efforts of global law enforcement agencies represents one of the most sophisticated and coordinated takedowns ever in the fight against online criminal activity.

THIS HIDDEN SITE HAS BEEN SEIZED

Since July 4, 2017

as a part of a law enforcement operation by the Federal Bureau of Investigation, the Drug Enforcement Administration, and European law enforcement agencies acting through Europol

in accordance with the law of European Union member states and obtained pursuant to a forfeiture order by the United States Attorney's Office for the Eastern District of California and the U.S. Department of Justice's Computer Crime & Intellectual Property Section.



Detail View

		Entity
+		77.232.78.72
+		UA-274166-*
+		209.140.30.106
+		184.154.46.111
+		www.3dsemu.com
+		www.3dsemulator.com
+		www.ds-lite.com
+		www.ndsemu.com
+		www.playstation2au.com
+		ndsemu.com
+		www.3dshomebrew.com
+		www.buy-dsi.com
+		www.dsiemulators.com
+		www.dsiflash.com
+		www.dsiflashcard.com
+		www.emulator.in
+		www.emuwii.com
+		www.led3dtv.com
+		www.mroms.com
+		www.pspgoconnect.com
+		www.psplite.com
+		www.sonicemulator.com
+		www.wiibackup.info
+		www.wiiroms.info
+		104.27.130.120
+		104.27.131.120
+		104.27.188.123

Property View

– Properties

Type

– Graph info

Weight

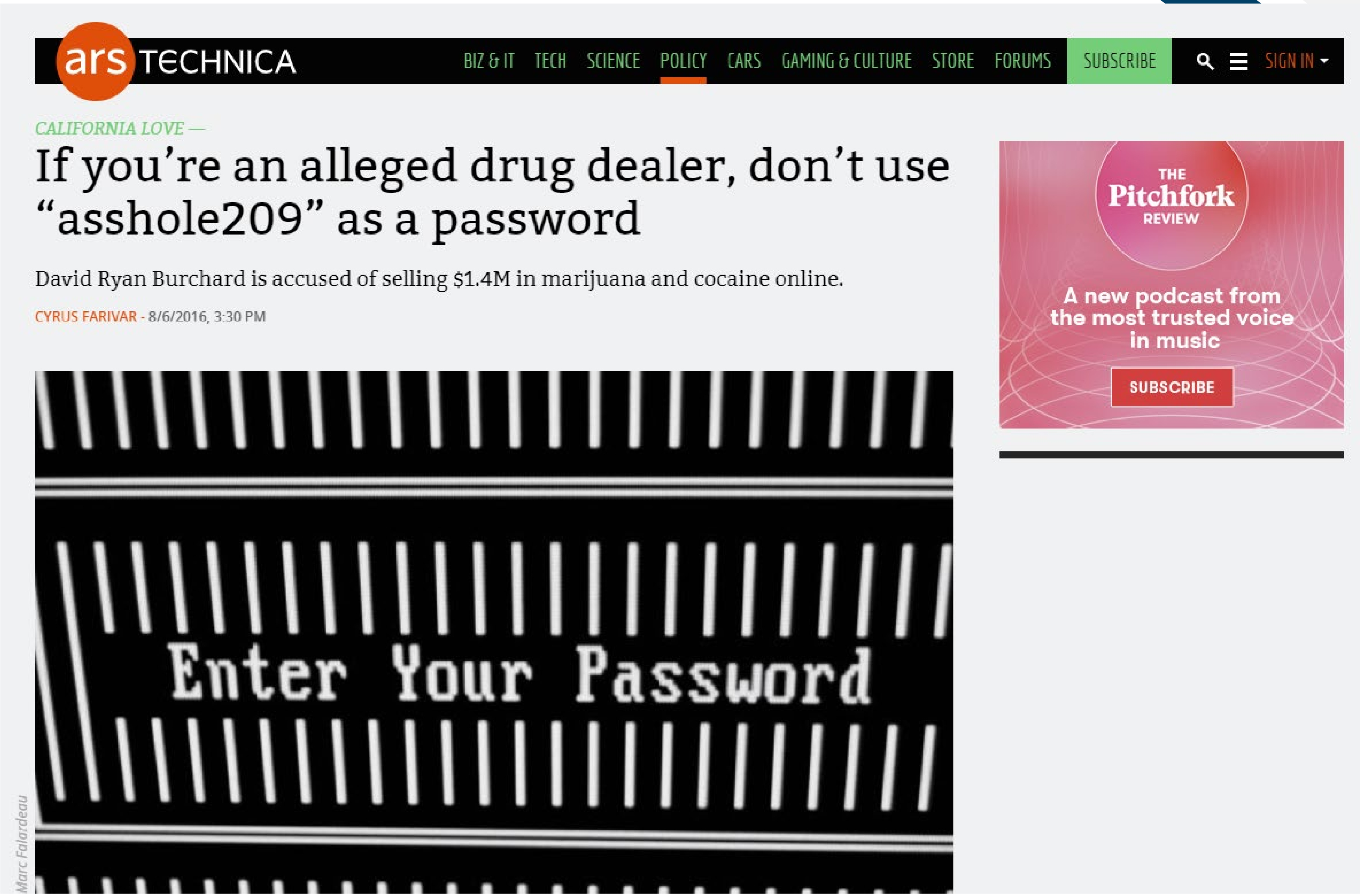
Incoming

Outgoi…

```
 whois info] returned with 0 entities (from 91 entities)
    's info] returned with 0 entities (from 91 entities)
        fo] returned with 0 entities (from 91 entities)
           eturned with 0 entities (from 91 entities)
              ed with 0 entities (from 91 entities)
                 ith 0 entities (from 91 entities)
                      entities (from 91 entities)
                         ities (from 91 entities)
                               (from 91 entities)
                                 om 91 entities)
```

Case Study Register your Username as Trademark

Again into the dark corners of the Internet



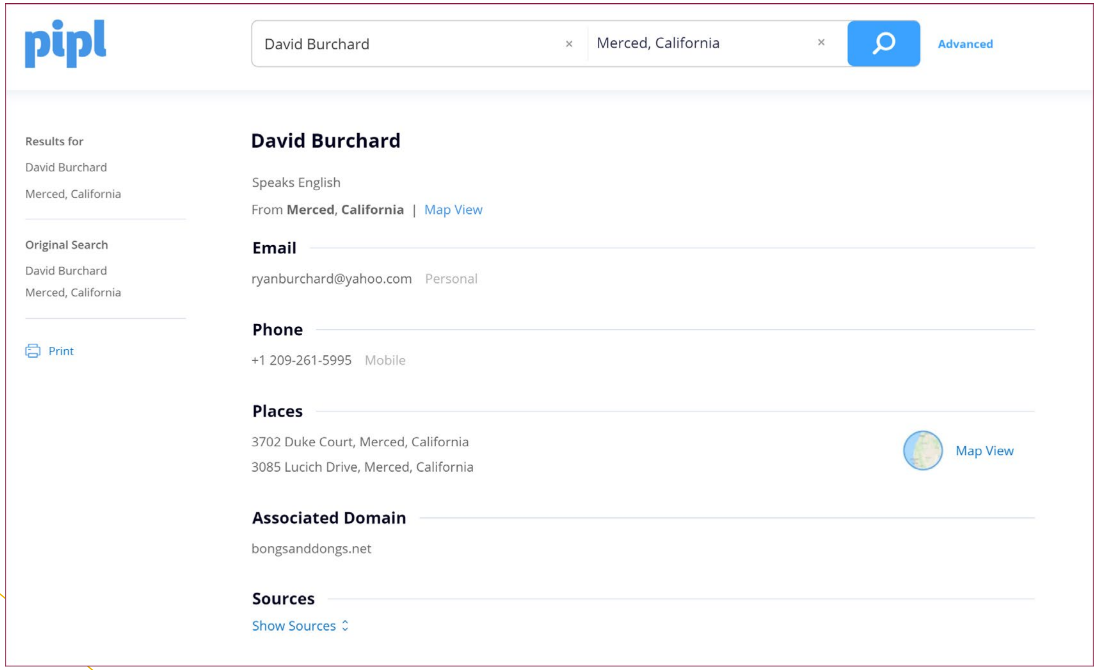
CALIFORNIA LOVE —

If you’re an alleged drug dealer, don’t use “asshole209” as a password

David Ryan Burchard is accused of selling $1.4M in marijuana and cocaine online.

CYRUS FARIVAR - 8/6/2016, 3:30 PM

David Burchard



Results for

David Burchard

Merced, California

Original Search

David Burchard

Merced, California

Print

David Burchard

Speaks English

From **Merced, California** | Map View

Email

ryanburchard@yahoo.com Personal

Phone

+1 209-261-5995 Mobile

Places

3702 Duke Court, Merced, California

3085 Lucich Drive, Merced, California

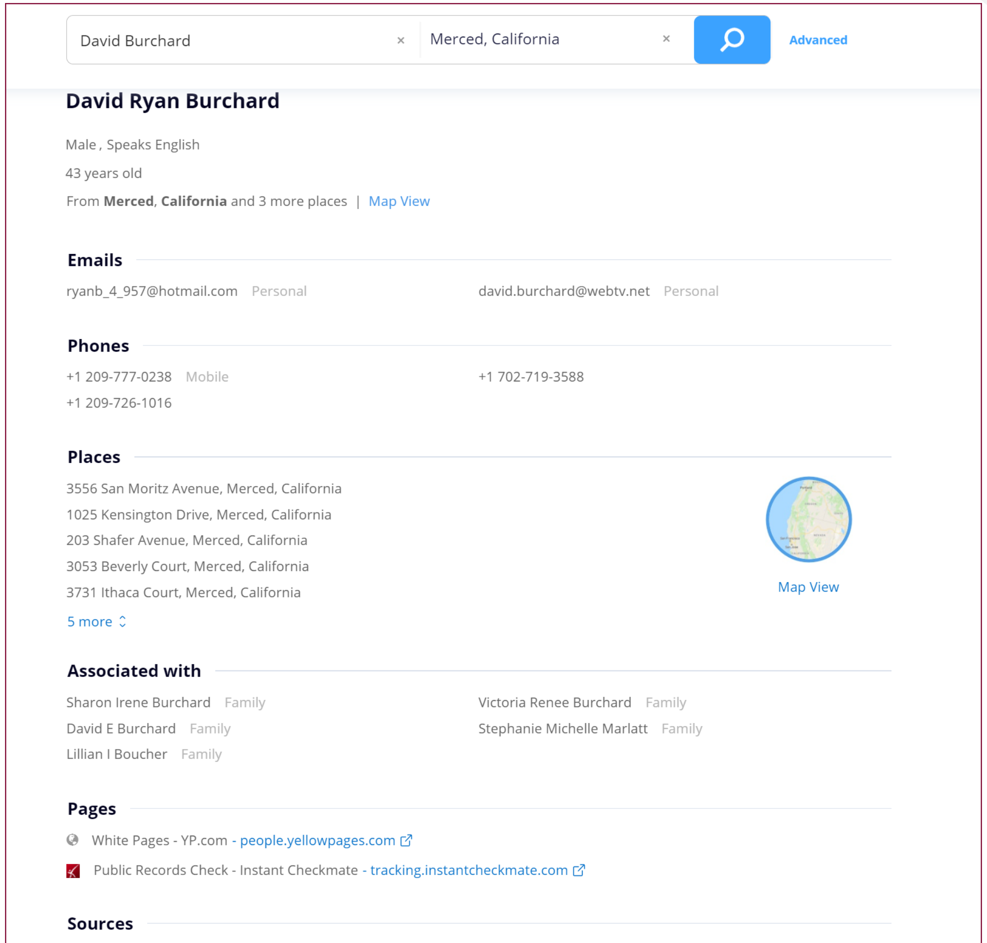
Map View

Associated Domain

bongsanddongs.net

Sources

Show Sources



David Ryan Burchard

Male , Speaks English

43 years old

From **Merced, California** and 3 more places | Map View

Emails

ryanb_4_957@hotmail.com Personal	david.burchard@webtv.net Personal

Phones

+1 209-777-0238 Mobile	+1 702-719-3588
+1 209-726-1016	

Places

3556 San Moritz Avenue, Merced, California

1025 Kensington Drive, Merced, California

203 Shafer Avenue, Merced, California

3053 Beverly Court, Merced, California

3731 Ithaca Court, Merced, California

5 more

Map View

Associated with

Sharon Irene Burchard Family	Victoria Renee Burchard Family
David E Burchard Family	Stephanie Michelle Marlatt Family
Lillian I Boucher Family	

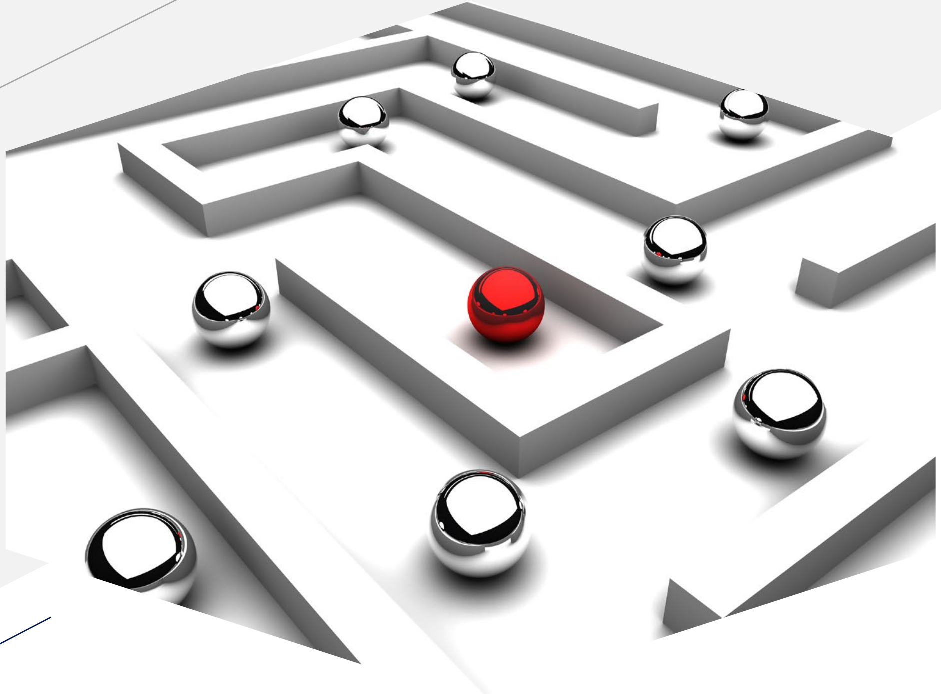
Pages

White Pages - YP.com - people.yellowpages.com

Public Records Check - Instant Checkmate - tracking.instantcheckmate.com

Sources

corma
We look deeper



Many thanks!

Jörn Weber

+49 2163 349 0081

jw@corma.de

www.corma.de / corma.training

Twitter: @corma_agency

corma GmbH
Hochstr. 2
41379 Brüggen

Social Links: Contact Details

Solve your case with our tool

We have integrated Whois XML API functionality visualisation into Social Links.

To start using domains and IP addresses in your investigation along with Social Media and the DarkNet Search, please contact our Sales Team.

Social Links
Sales Team

sales@mtg-bi.com

To get Whois XML API key, go to
https://main.whoisxmlapi.com/

Social Links: Contact Details

Solve your case with our tool

We are always there to help you.

In case of any questions about running our programme, please contact our Support Team.

Social Links
Support Team

support@mtg-bi.com

Questions and Answers

You Must Know the TRUTH

Sonya Oronova
Project Manager
at Social Links

sonya@mtg-bi.com

Jörn Weber
OSINT Expert
at Corma

jw@corma.de

Alex Ronquillo
Sr. Director of Business Development
at Whois API

alex.ronquillo@whoisxmlapi.com

Social Links: Where We Post Our Updates

www.mtg-bi.com/blog

sales@mtg-bi.com

@_SocialLinks_

Social Links

Social Links Maltego Transforms