Investigating Digital Infrastructures

GIJN Cyber Investigation Training - Week 4

Etienne Maynier - May 2023

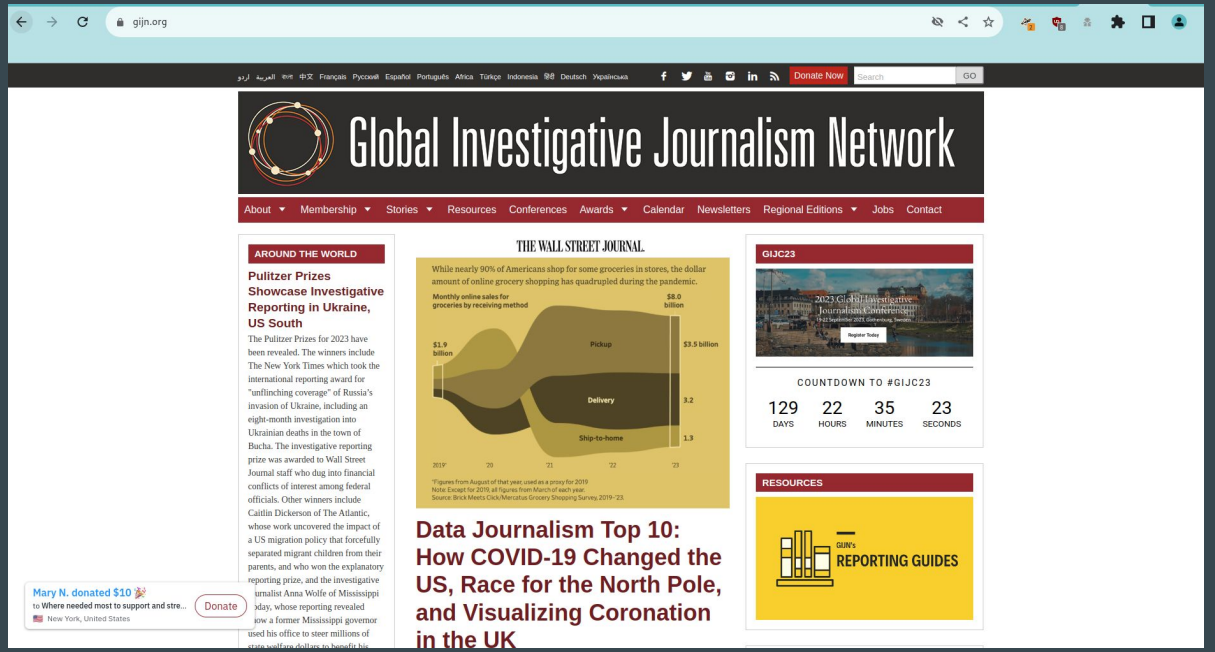
Today

- Objective : learn how to investigate digital infrastructures
- 1 - How do they work?
- 2 - What data sources are available?
- 3 - Examples

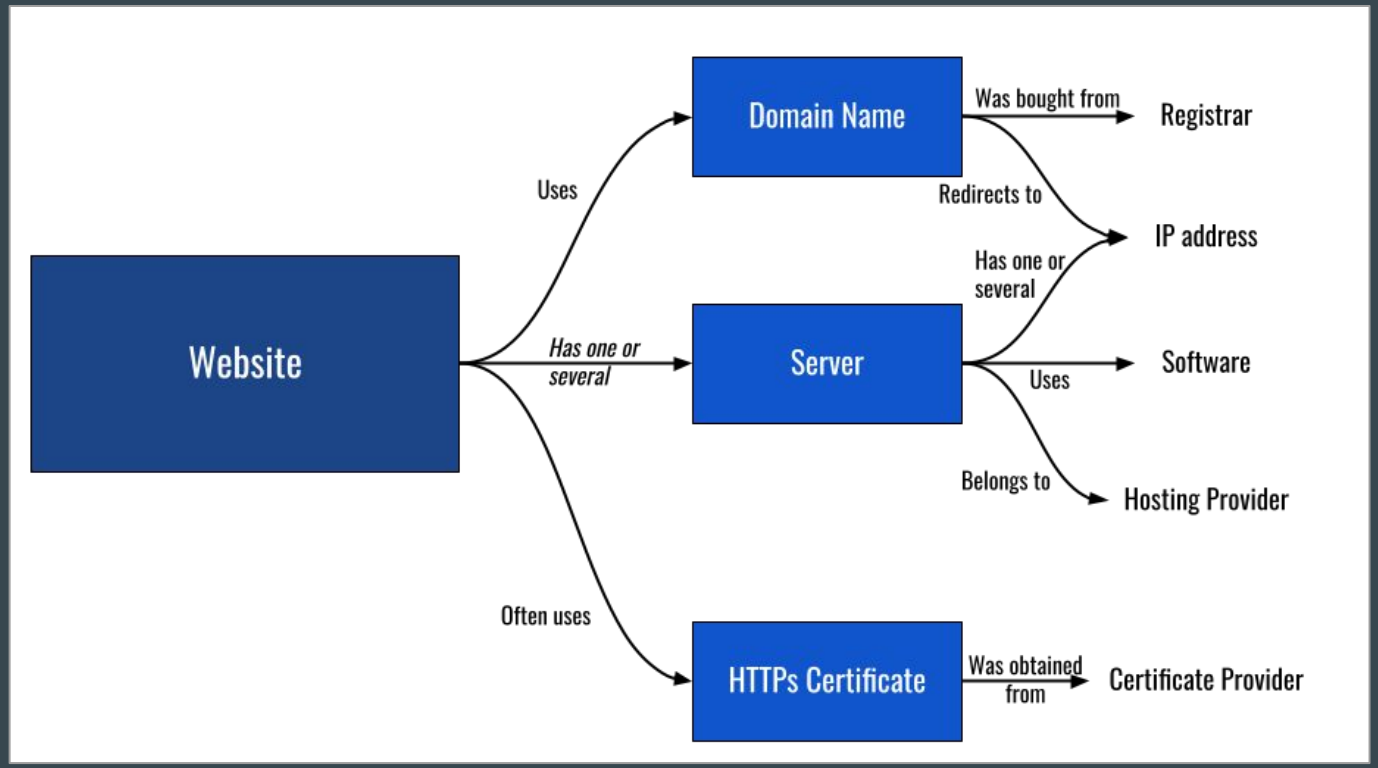
How Digital Infrastructure Work?

Technology is easy

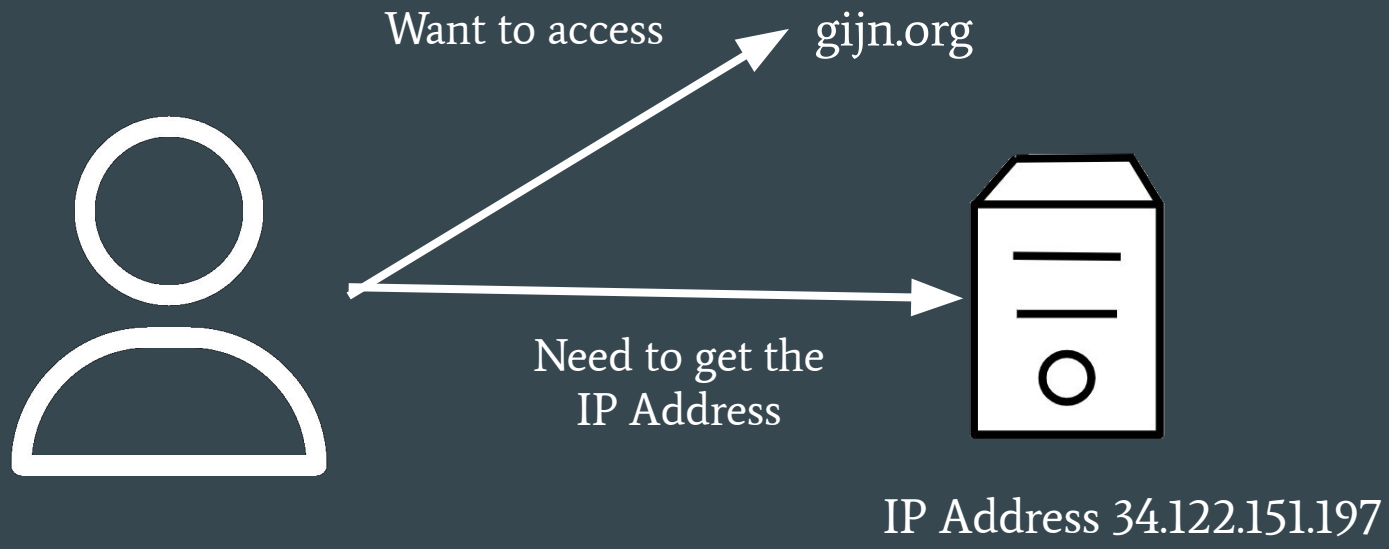
Type GIJN.org in your browser



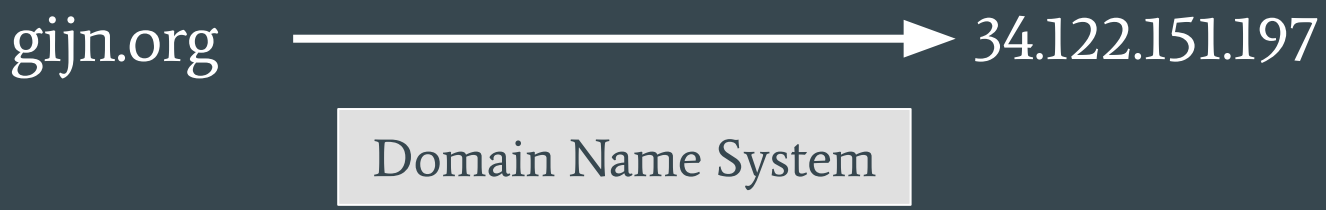
Under the hood



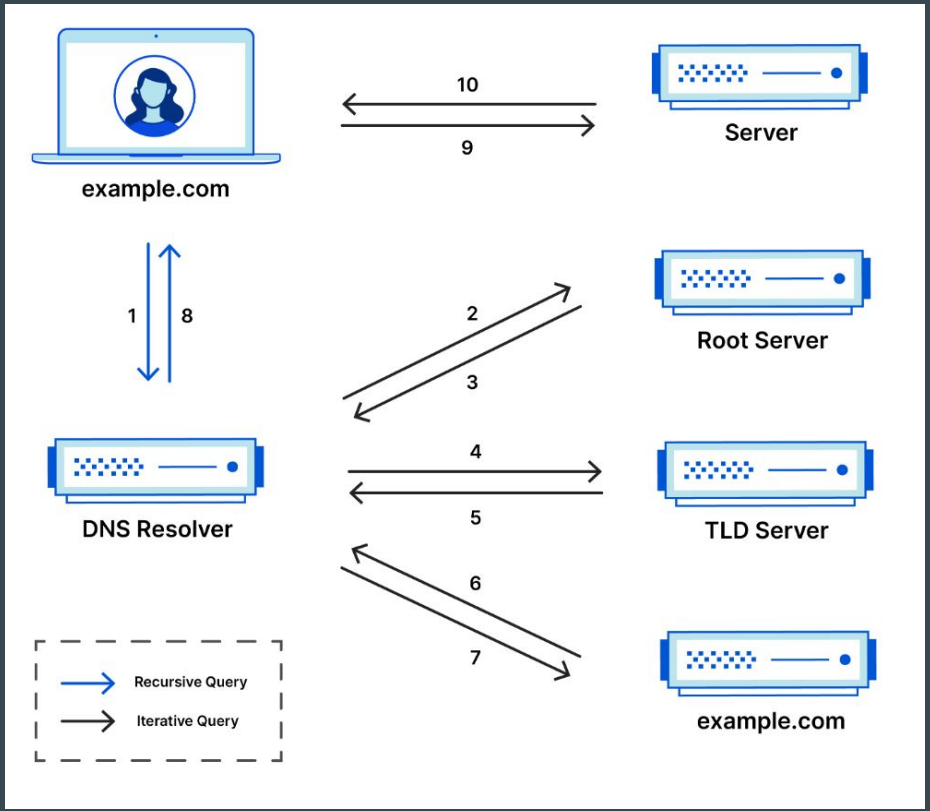
Domain Name: How does it work?



Domain Name: How does it work?



Domain Name: How does it work?



Domain Name: Different DNS Types

```
# A
34.122.151.197: ASN396982 GOOGLE-CLOUD-PLATFORM - Council Bluffs United States

# AAAA
No AAAA entry configured

# NS
ns2.bluehost.com. - 162.159.25.175 - ASN13335 CLOUDFLARENET - None None
ns1.bluehost.com. - 162.159.24.80 - ASN13335 CLOUDFLARENET - None None

# MX:
5 alt2.aspmx.l.google.com. - 142.251.9.26 - ASN15169 GOOGLE - None United States
5 alt1.aspmx.l.google.com. - 142.250.153.26 - ASN15169 GOOGLE - None United States
10 aspmx3.googlemail.com. - 142.251.9.26 - ASN15169 GOOGLE - None United States
1 aspmx.l.google.com. - 108.177.15.27 - ASN15169 GOOGLE - None United States
10 aspmx2.googlemail.com. - 142.250.153.26 - ASN15169 GOOGLE - None United States

# SOA
NS: ns1.bluehost.com.
Owner: root.box5551@bluehost.com

# TXT:
"v=spf1 include:servers.mcsv.net include:_spf.google.com ?all"
"google-site-verification=4hFNkNXFz9jO96jBlsXmi7cYawU4isC_q6-nHvWol4A"
```

Domain Name: Registration

GoDaddy
Registrar used to buy gijn.org

Public Internet Registry
Registry managing .org

Domain Name: Whois

- Registries maintain databases of domain owner information called WHOIS
- Registrars have to collect information for this database
- Now most data is hidden for privacy reasons
- Still useful to know when a domain was registered

Let’s check GIJN Whois

Connect to https://centralops.net/co/ and check gijn.org

Whois

```
Domain Name: gijn.org
Registry Domain ID: c7cc6ed06499446d8d2b22adaad4fe9a-LROR
Registrar WHOIS Server: http://whois.godaddy.com
Registrar URL: http://www.whois.godaddy.com
Updated Date: 2022-10-04T10:57:00Z
Creation Date: 2009-06-24T18:23:19Z
Registry Expiry Date: 2024-06-24T18:23:19Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Domains By Proxy, LLC
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Arizona
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: US
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information
```

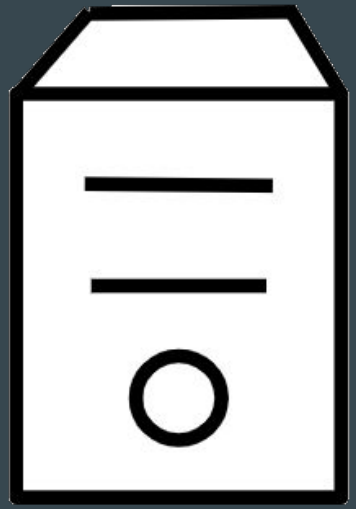
Domain Structure

Top Level Domain (TLD)

Domain Name
-> Whois information

Subdomain
-> Each subdomain can have different DNS entries (wildcard DNS configuration exist)

Now the Server



Just a computer running in someone's network

Need an IP address to be able to communicate

IPv4 like 34.122.151.197

IPv6 like 2a00:1450:4007:80e::200e

IP Address

- Regional Internet Registries distribute IP ranges to organisations

- To be accessible on Internet, they need to be part of an Autonomous System (AS), an organisation identified by a number and that can advertise IPs on Internet

- Anyone can register an Autonomous System, some companies have several AS

Autonomous Systems

```
AS0     -Reserved AS-
AS1     LVLT-1 - Level 3 Communications, Inc.
AS2     UDEL-DCN - University of Delaware
AS3     MIT-GATEWAYS - Massachusetts Institute of Technology
AS4     ISI-AS - University of Southern California
AS5     SYMBOLICS - Symbolics, Inc.
AS6     BULL-NETWORK for further information please visit http://www.bull.com
AS7     UK Defence Research Agency
AS8     RICE-AS - Rice University
AS9     CMU-ROUTER - Carnegie Mellon University
AS10    CSNET-EXT-AS - CSNET Coordination and Information Center (CSNET-CIC)
AS11    HARVARD - Harvard University
AS12    NYU-DOMAIN - New York University
AS13    DNIC-AS-00013 - Headquarters, USAISC
AS14    COLUMBIA-GW - Columbia University
AS15    NET-DYNAMICS-EXP - DYNAMICS
AS16    LBL - Lawrence Berkeley National Laboratory
AS17    PURDUE - Purdue University
AS18    UTEXAS - University of Texas at Austin
AS19    CSS-DOMAIN - SMDC c/o Science Applications International Corporation
AS20    UR - University of Rochester
AS21    RAND - The RAND Corporation
AS22    DNIC-AS-00022 - Navy Network Information Center (NNIC)
AS23    NISN-SIP-AS - National Aeronautics and Space Administration
AS24    AMES-NAS-GW - National Aeronautics and Space Administration
AS25    UCB - University of California at Berkeley
AS26    CORNELL - Cornell University
AS27    UMDNET - University of Maryland
AS28    DFVLR-SYS Deutsches Zentrum fuer Luft- und Raumfahrt
AS29    YALE-AS - Yale University
AS30    SRI-AICNET - SRI International
AS31    CIT - California Institute of Technology
AS32    STANFORD - Stanford University
AS33    HP-DIGITAL-33 - Hewlett-Packard Company
AS34    UDELNET - University of Delaware
```

GIJN

Let’s check GIJN IP : 34.122.151.197 on ipinfo.io

IP Addresses

162.55.191.113 belongs to AS396982 Google LLC

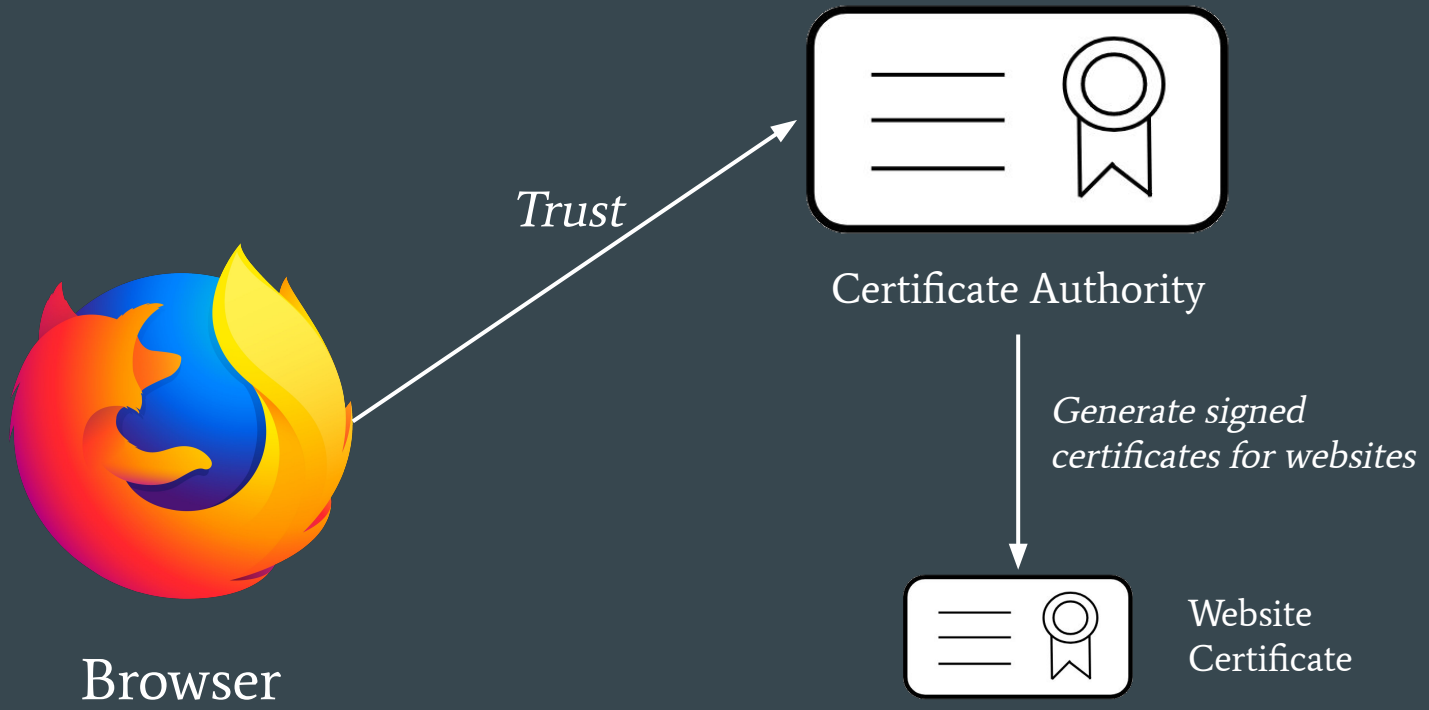
Bonus : you can use Whois for IP addresses

```
Domain Name: GOOGLEUSERCONTENT.COM
Registry Domain ID: 1528918319_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2022-10-16T09:27:01Z
Creation Date: 2008-11-17T15:58:29Z
Registry Expiry Date: 2023-11-17T15:58:29Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: NS1.GOOGLE.COM
Name Server: NS2.GOOGLE.COM
Name Server: NS3.GOOGLE.COM
Name Server: NS4.GOOGLE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
```

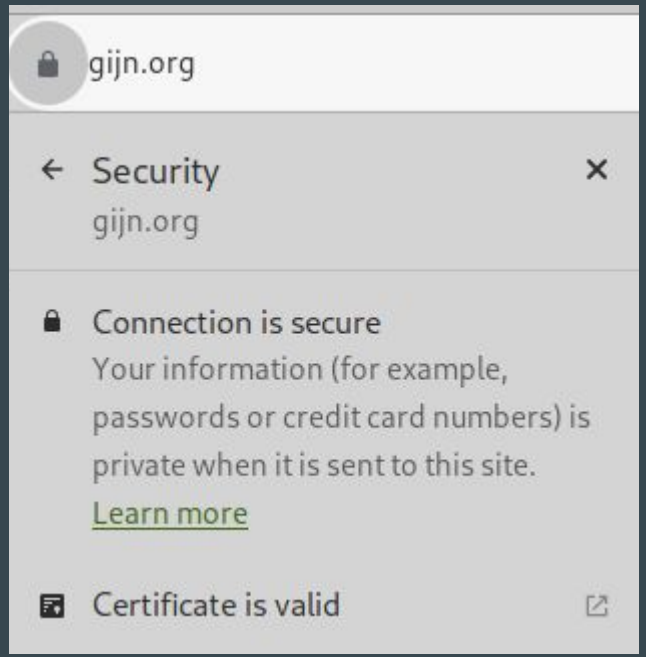
HTTPs Certificates

- Internet was developed in a very insecure way, security was added after
- HTTP is the default protocol for the web, HTTPs its secure version
- “Check that there is a green lock”

HTTPs: how does it work?



gijn.org



Issued To

Common Name (CN)	gijn.org
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By

Common Name (CN)	R3
Organization (O)	Let's Encrypt
Organizational Unit (OU)	<Not Part Of Certificate>

Validity Period

Issued On	Saturday, April 29, 2023 at 5:24:08 AM
Expires On	Friday, July 28, 2023 at 5:24:07 AM

Fingerprints

SHA-256 Fingerprint	A3 C2 D4 7C 03 E5 F9 21 FE BE FC AD 9E 7F 39 02 A0 F3 B5 DD 7C 9B C2 E5 2A C7 C4 EB 5A 43 CD F8
SHA-1 Fingerprint	0F CF AE A1 C8 CB 59 5B C6 E0 FC 2D F5 E3 68 32 89 33 02 84

Exercice

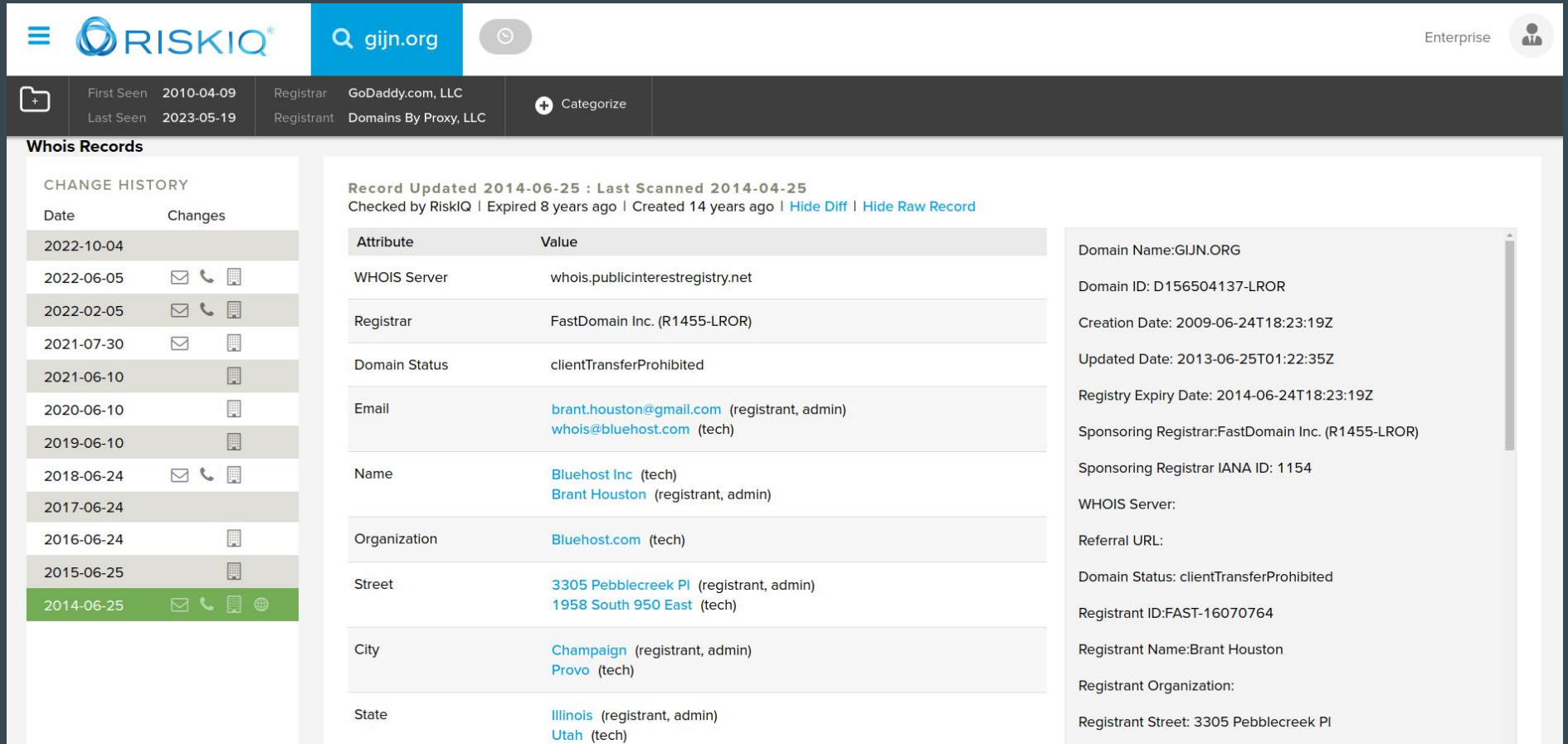
What can you find on https://www.afp.com/ ?

Break time

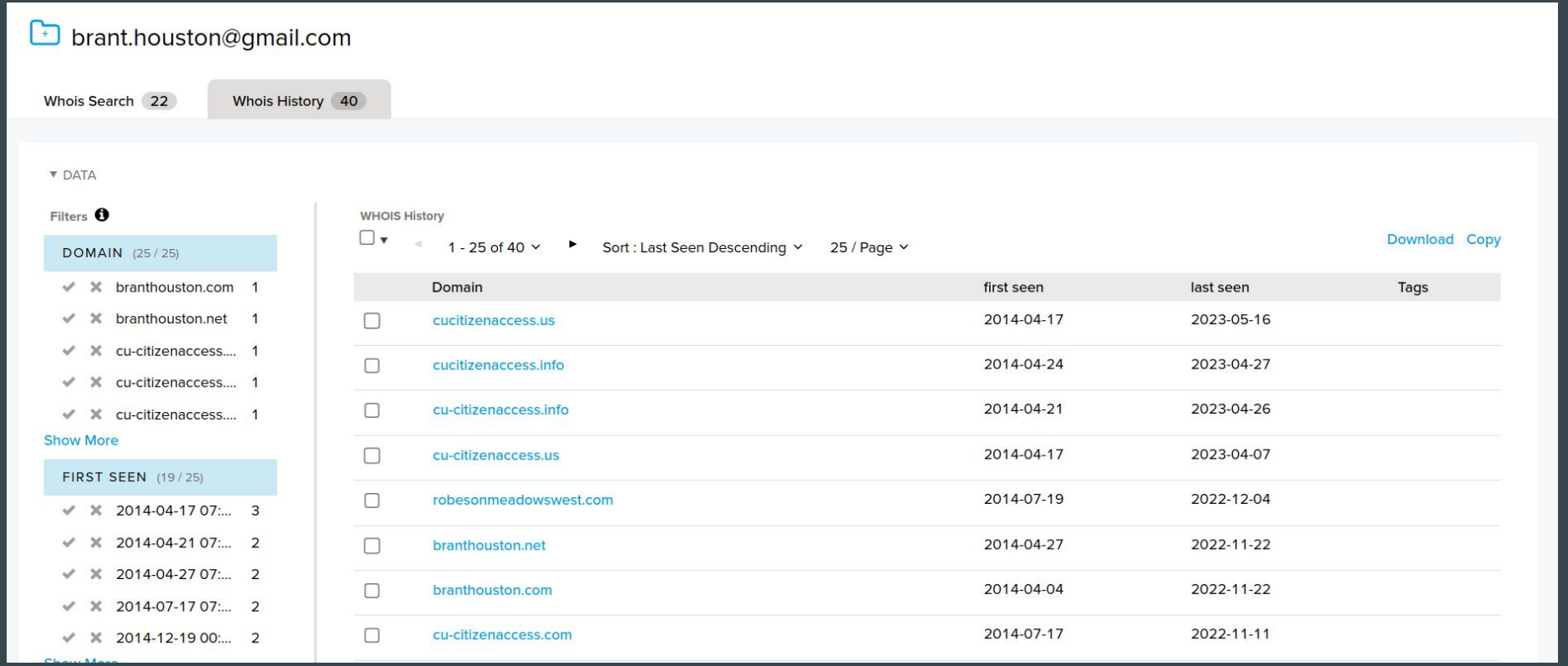
Getting more interesting information

1 - Historical Whois

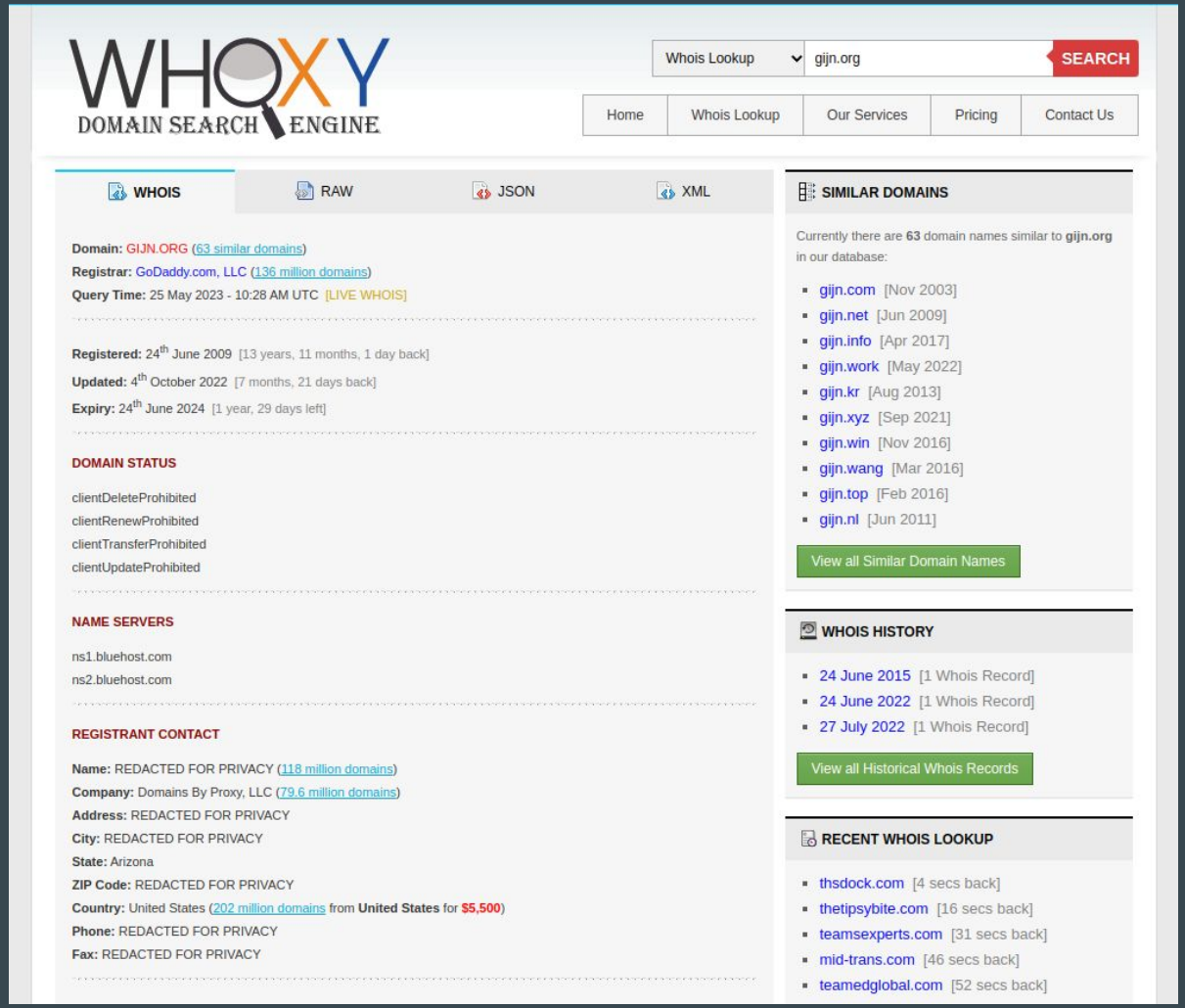
Historical Whois



Historical Whois

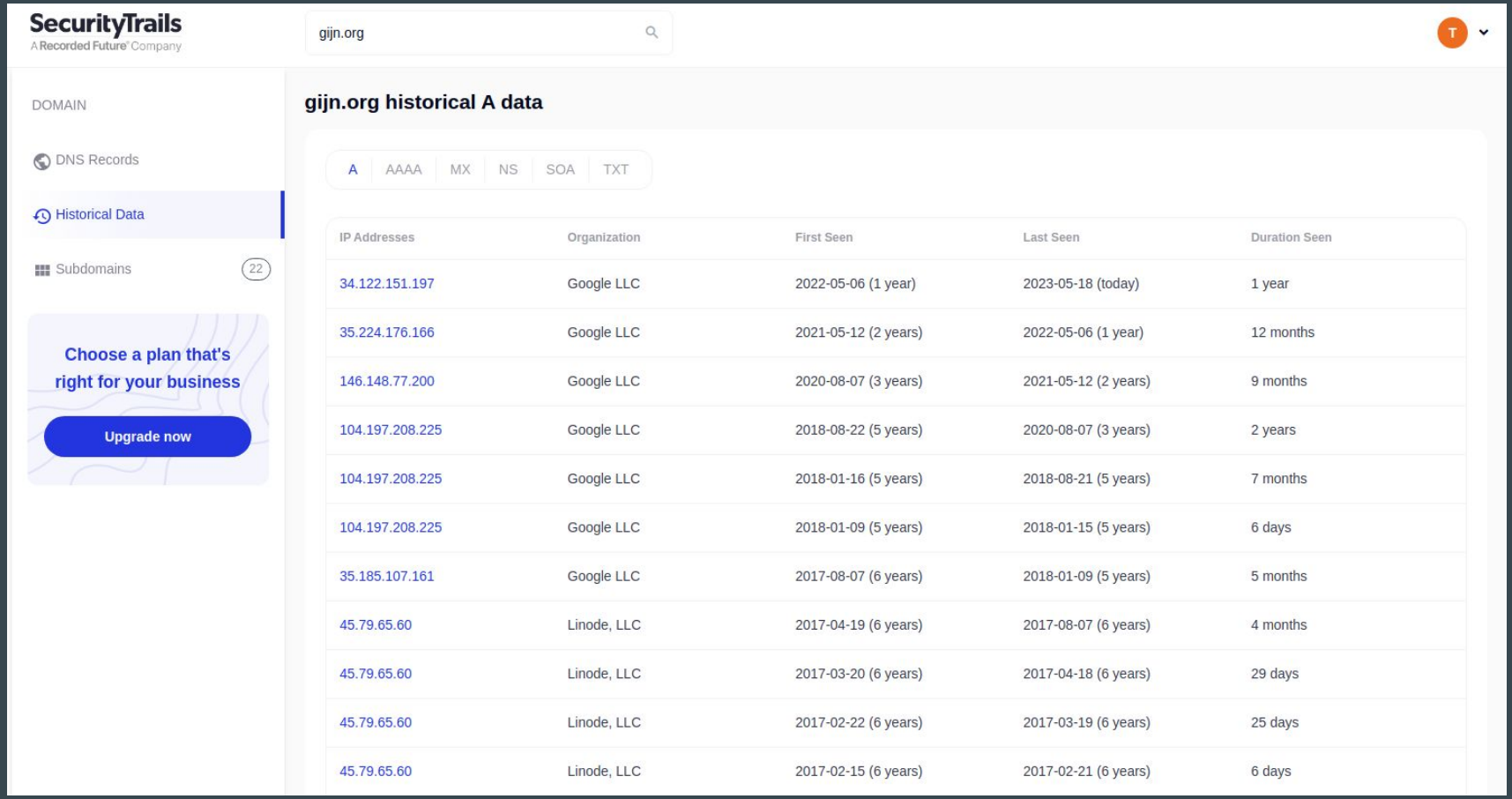


Whoxy


WHOXY
DOMAIN SEARCH ENGINE
Whois Lookup
gijn.org
SEARCH
Home
Whois Lookup
Our Services
Pricing
Contact Us
WHOIS
RAW
JSON
XML
Domain: GIJN.ORG (63 similar domains)
Registrar: GoDaddy.com, LLC (136 million domains)
Query Time: 25 May 2023 - 10:28 AM UTC [LIVE WHOIS]
Registered: 24th June 2009 [13 years, 11 months, 1 day back]
Updated: 4th October 2022 [7 months, 21 days back]
Expiry: 24th June 2024 [1 year, 29 days left]
DOMAIN STATUS
clientDeleteProhibited
clientRenewProhibited
clientTransferProhibited
clientUpdateProhibited
NAME SERVERS
ns1.bluehost.com
ns2.bluehost.com
REGISTRANT CONTACT
Name: REDACTED FOR PRIVACY (118 million domains)
Company: Domains By Proxy, LLC (79.6 million domains)
Address: REDACTED FOR PRIVACY
City: REDACTED FOR PRIVACY
State: Arizona
ZIP Code: REDACTED FOR PRIVACY
Country: United States (202 million domains from United States for $5,500)
Phone: REDACTED FOR PRIVACY
Fax: REDACTED FOR PRIVACY
SIMILAR DOMAINS
Currently there are 63 domain names similar to gijn.org in our database:
gijn.com [Nov 2003]
gijn.net [Jun 2009]
gijn.info [Apr 2017]
gijn.work [May 2022]
gijn.kr [Aug 2013]
gijn.xyz [Sep 2021]
gijn.win [Nov 2016]
gijn.wang [Mar 2016]
gijn.top [Feb 2016]
gijn.nl [Jun 2011]
View all Similar Domain Names
WHOIS HISTORY
24 June 2015 [1 Whois Record]
24 June 2022 [1 Whois Record]
27 July 2022 [1 Whois Record]
View all Historical Whois Records
RECENT WHOIS LOOKUP
thsdock.com [4 secs back]
thetipsybite.com [16 secs back]
teamsexperts.com [31 secs back]
mid-trans.com [46 secs back]
teamedglobal.com [52 secs back]

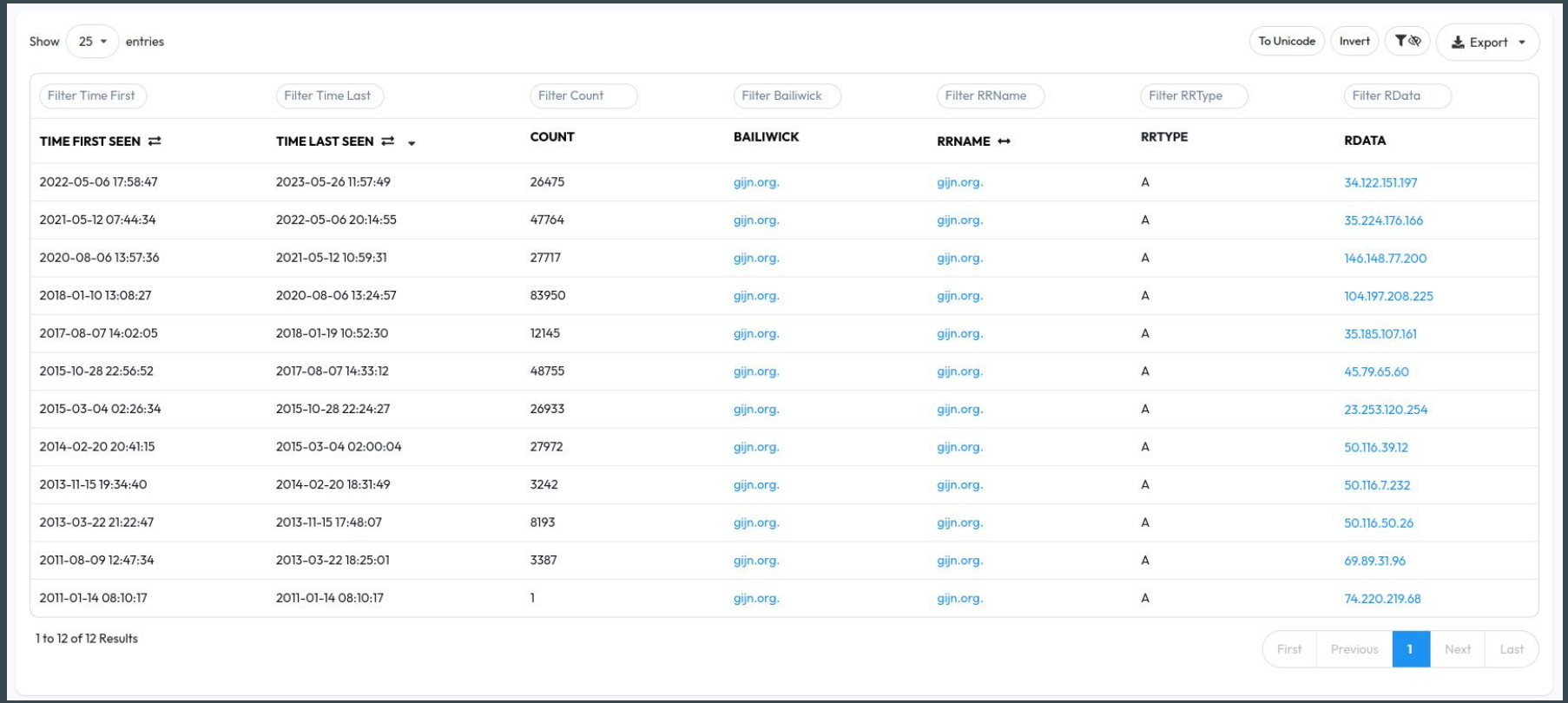
2 - Passive DNS

Passive DNS



IP Addresses	Organization	First Seen	Last Seen	Duration Seen
34.122.151.197	Google LLC	2022-05-06 (1 year)	2023-05-18 (today)	1 year
35.224.176.166	Google LLC	2021-05-12 (2 years)	2022-05-06 (1 year)	12 months
146.148.77.200	Google LLC	2020-08-07 (3 years)	2021-05-12 (2 years)	9 months
104.197.208.225	Google LLC	2018-08-22 (5 years)	2020-08-07 (3 years)	2 years
104.197.208.225	Google LLC	2018-01-16 (5 years)	2018-08-21 (5 years)	7 months
104.197.208.225	Google LLC	2018-01-09 (5 years)	2018-01-15 (5 years)	6 days
35.185.107.161	Google LLC	2017-08-07 (6 years)	2018-01-09 (5 years)	5 months
45.79.65.60	Linode, LLC	2017-04-19 (6 years)	2017-08-07 (6 years)	4 months
45.79.65.60	Linode, LLC	2017-03-20 (6 years)	2017-04-18 (6 years)	29 days
45.79.65.60	Linode, LLC	2017-02-22 (6 years)	2017-03-19 (6 years)	25 days
45.79.65.60	Linode, LLC	2017-02-15 (6 years)	2017-02-21 (6 years)	6 days

DNSDB



Show 25 entries

To Unicode | Invert | Export

Filter Time First	Filter Time Last	Filter Count	Filter Bailiwick	Filter RRName	Filter RRType	Filter RData
TIME FIRST SEEN	**TIME LAST SEEN**	**COUNT**	**BAILIWICK**	**RRNAME**	**RRTYPE**	**RDATA**
2022-05-06 17:58:47	2023-05-26 11:57:49	26475	gijn.org.	gijn.org.	A	34.122.151.197
2021-05-12 07:44:34	2022-05-06 20:14:55	47764	gijn.org.	gijn.org.	A	35.224.176.166
2020-08-06 13:57:36	2021-05-12 10:59:31	27717	gijn.org.	gijn.org.	A	146.148.77.200
2018-01-10 13:08:27	2020-08-06 13:24:57	83950	gijn.org.	gijn.org.	A	104.197.208.225
2017-08-07 14:02:05	2018-01-19 10:52:30	12145	gijn.org.	gijn.org.	A	35.185.107.161
2015-10-28 22:56:52	2017-08-07 14:33:12	48755	gijn.org.	gijn.org.	A	45.79.65.60
2015-03-04 02:26:34	2015-10-28 22:24:27	26933	gijn.org.	gijn.org.	A	23.253.120.254
2014-02-20 20:41:15	2015-03-04 02:00:04	27972	gijn.org.	gijn.org.	A	50.116.39.12
2013-11-15 19:34:40	2014-02-20 18:31:49	3242	gijn.org.	gijn.org.	A	50.116.7.232
2013-03-22 21:22:47	2013-11-15 17:48:07	8193	gijn.org.	gijn.org.	A	50.116.50.26
2011-08-09 12:47:34	2013-03-22 18:25:01	3387	gijn.org.	gijn.org.	A	69.89.31.96
2011-01-14 08:10:17	2011-01-14 08:10:17	1	gijn.org.	gijn.org.	A	74.220.219.68

1 to 12 of 12 Results

First | Previous | 1 | Next | Last

What kind of server is it?

Successful Query for: RData 34.122.151.197 (ip) (Limit 5000)
Found 223 Results

Show 25 entries

To Unicode | Invert | Export

Filter Time First	Filter Time Last	Filter Count	Filter RRName	Filter RRType	Filter RData
TIME FIRST SEEN	**TIME LAST SEEN**	**COUNT**	**RRNAME**	**RRTYPE**	**RDATA**
2022-05-17 16:48:58	2023-05-26 16:31:14	3659	qsrautomation1.wpengine.com.	A	34.122.151.197
2022-03-16 02:44:08	2023-05-26 16:20:56	1121	nowourworld.com.	A	34.122.151.197
2022-03-24 12:57:53	2023-05-26 15:05:51	5278	friesianconnection.com.	A	34.122.151.197
2022-06-03 14:58:33	2023-05-26 14:56:34	1207	constellation.aero.	A	34.122.151.197
2022-02-26 07:01:05	2023-05-26 14:48:14	1328	strainsanity.com.	A	34.122.151.197
2022-11-11 23:49:10	2023-05-26 14:23:04	181	elliottsstedev.wpengine.com.	A	34.122.151.197
2022-02-28 22:01:49	2023-05-26 13:53:33	1046	hamptonsgroup.com.	A	34.122.151.197
2022-10-29 15:38:34	2023-05-26 13:11:51	219	cowboyoffice.wpengine.com.	A	34.122.151.197
2022-11-14 18:59:41	2023-05-26 13:01:30	6154	letswinpc.org.	A	34.122.151.197
2022-03-26 09:35:25	2023-05-26 13:01:11	3307	pierreskincare.com.	A	34.122.151.197
2022-02-26 00:34:38	2023-05-26 12:25:55	510	geminiprd.wpengine.com.	A	34.122.151.197
2022-02-26 00:34:38	2023-05-26 12:25:54	1033	geminimotor.com.	A	34.122.151.197
2022-05-06 17:58:47	2023-05-26 11:57:49	26475	gijn.org.	A	34.122.151.197
2022-05-09 15:34:56	2023-05-26 11:42:56	18980	gijnstaging.wpengine.com.	A	34.122.151.197
2022-03-25 20:26:04	2023-05-26 11:27:59	15747	340breport.com.	A	34.122.151.197

Other example : what kind of server is it?

Successful Query for: RData 162.55.191.113 (ip) (Limit 5000)
Found 6 Results

Show 25 entries

To Unicode | Invert | Export

Filter Time First	Filter Time Last	Filter Count	Filter RRName	Filter RRType	Filter RData
TIME FIRST SEEN	**TIME LAST SEEN**	**COUNT**	**RRNAME**	**RRTYPE**	**RDATA**
2022-01-10 10:56:27	2023-05-28 23:44:28	3611	randhome.io.	A	162.55.191.113
2022-01-10 10:00:59	2023-05-28 23:44:26	515	www.randhome.io.	A	162.55.191.113
2022-01-13 21:43:49	2023-05-26 00:31:42	300	ipvtechbib.randhome.io.	A	162.55.191.113
2022-08-09 11:44:38	2023-05-09 18:49:53	51	stalkerwa.re.	A	162.55.191.113
2021-05-15 11:36:26	2023-03-09 20:33:05	23	static.113.191.55.162.clients.your-server.de.	A	162.55.191.113
2022-10-26 11:36:05	2022-10-28 14:02:30	120	badbadbad.eu.	A	162.55.191.113

1 to 6 of 6 Results

First | Previous | 1 | Next | Last

Passive DNS

Lots of specific cases when analyzing passive DNS, some examples:

- CDN / Reverse Proxy : Cloudflare, Fastly, Sucuri Web Protection
  - Hide the real IP of the server
- Sinkhole
- Parking pages

3 - Certificate Transparency

Certificate Transparency Databases

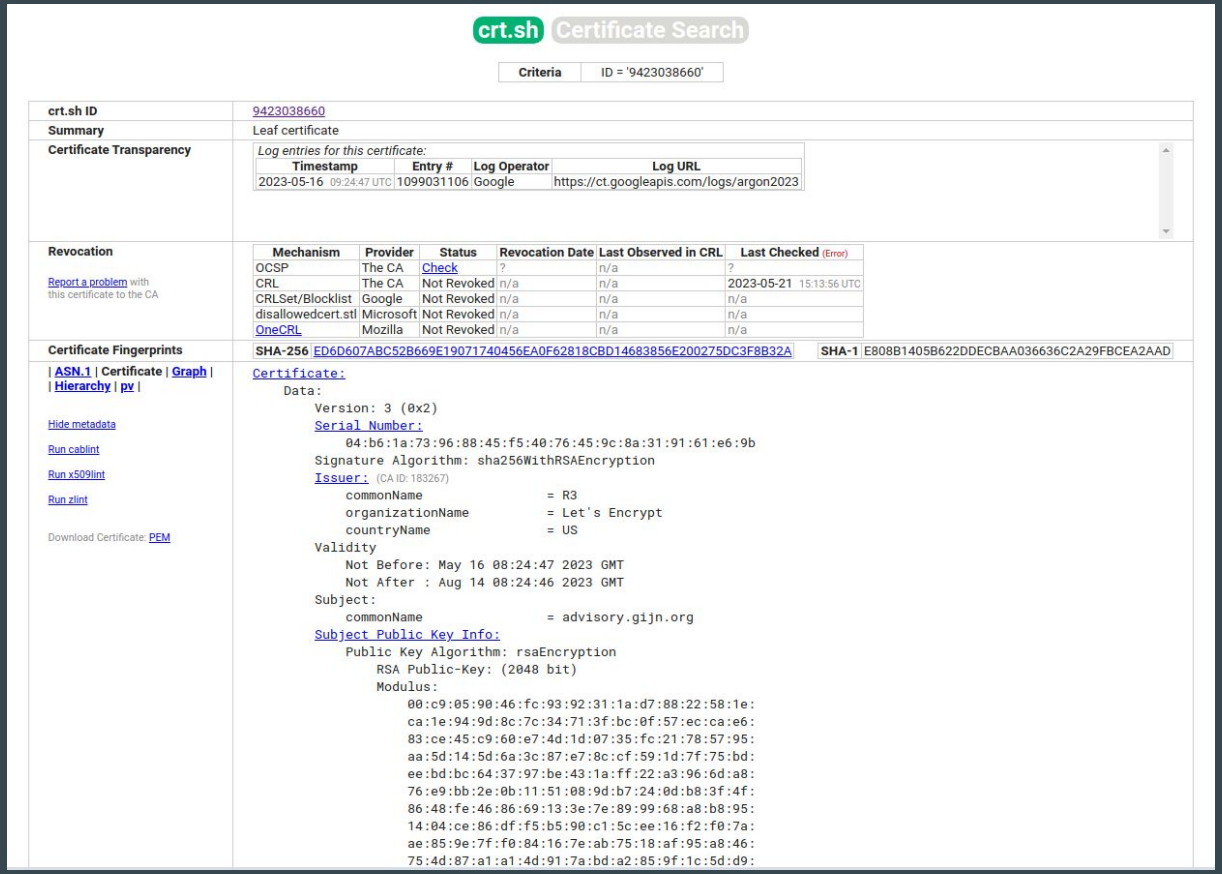
crt.sh Identity Search  Group by Issuer

Criteria	Type: Identity Match: ILIKE Search: 'gijn.org'

Certificates

crt.sh ID	Logged At ⇑	Not Before	Not After	Common Name	Matching Identities	Issuer Name
9435770579	2023-05-20	2023-05-20	2023-08-18	helpdesk.gijn.org	helpdesk.gijn.org	C=US, O=Let's Encrypt, CN=R3
9423038660	2023-05-16	2023-05-16	2023-08-14	advisory.gijn.org	advisory.gijn.org	C=US, O=Let's Encrypt, CN=R3
9402525413	2023-05-16	2023-05-16	2023-08-14	advisory.gijn.org	advisory.gijn.org	C=US, O=Let's Encrypt, CN=R3
9411973108	2023-05-15	2023-05-15	2023-08-13	gijc21.gijn.org	gijc21.gijn.org	C=US, O=Let's Encrypt, CN=R3
9394880260	2023-05-15	2023-05-15	2023-08-13	gijc21.gijn.org	gijc21.gijn.org	C=US, O=Let's Encrypt, CN=R3
9373010075	2023-05-13	2023-05-13	2024-05-12	gijn.org	gijn.org	C=US, O="Cloudflare, Inc.", CN=Cloudflare Inc ECC CA-3
9373010063	2023-05-13	2023-05-13	2024-05-12	gijn.org	gijn.org	C=US, O="Cloudflare, Inc.", CN=Cloudflare Inc RSA CA-2
9271263187	2023-04-29	2023-04-29	2023-07-28	gijn.org	gijn.org	C=US, O=Let's Encrypt, CN=R3
9259301928	2023-04-29	2023-04-29	2023-07-28	gijn.org	gijn.org	C=US, O=Let's Encrypt, CN=R3
9270983301	2023-04-29	2023-04-29	2023-07-28	cn.gijn.org	cn.gijn.org	C=US, O=Let's Encrypt, CN=R3
9258944957	2023-04-29	2023-04-29	2023-07-28	cn.gijn.org	cn.gijn.org	C=US, O=Let's Encrypt, CN=R3
9270983032	2023-04-29	2023-04-29	2023-07-28	impact.gijn.org	impact.gijn.org	C=US, O=Let's Encrypt, CN=R3
9258944885	2023-04-29	2023-04-29	2023-07-28	impact.gijn.org	impact.gijn.org	C=US, O=Let's Encrypt, CN=R3
9270738449	2023-04-29	2023-04-29	2023-07-28	www.gijn.org	www.gijn.org	C=US, O=Let's Encrypt, CN=R3
9258607729	2023-04-29	2023-04-29	2023-07-28	www.gijn.org	www.gijn.org	C=US, O=Let's Encrypt, CN=R3
9200203864	2023-04-20	2023-04-20	2023-07-19	autodiscover.gijn.org	autodiscover.gijn.org cpanel.gijn.org cpcalendars.gijn.org cpcontacts.gijn.org webdisk.gijn.org webmail.gijn.org	C=US, O=Let's Encrypt, CN=R3
9192876741	2023-04-20	2023-04-20	2023-07-19	autodiscover.gijn.org	autodiscover.gijn.org cpanel.gijn.org cpcalendars.gijn.org cpcontacts.gijn.org webdisk.gijn.org webmail.gijn.org	C=US, O=Let's Encrypt, CN=R3
9166231270	2023-04-16	2023-04-16	2023-07-15	resources.gijn.org	resources.gijn.org	C=US, O=Let's Encrypt, CN=R3
9166227787	2023-04-16	2023-04-16	2023-07-15	resources.gijn.org	resources.gijn.org	C=US, O=Let's Encrypt, CN=R3
8961071059	2023-03-21	2023-03-21	2023-06-19	helpdesk.gijn.org	helpdesk.gijn.org	C=US, O=Let's Encrypt, CN=R3
8946668782	2023-03-21	2023-03-21	2023-06-19	helpdesk.gijn.org	helpdesk.gijn.org	C=US, O=Let's Encrypt, CN=R3
8880036226	2023-03-09	2023-03-09	2023-06-07	advisory.gijn.org	advisory.gijn.org	C=US, O=Let's Encrypt, CN=R3
8845077525	2023-03-09	2023-03-09	2023-06-07	advisory.gijn.org	advisory.gijn.org	C=US, O=Let's Encrypt, CN=R3
8869534714	2023-03-08	2023-03-08	2023-06-06	gijc21.gijn.org	gijc21.gijn.org	C=US, O=Let's Encrypt, CN=R3
8836510210	2023-03-08	2023-03-08	2023-06-06	gijc21.gijn.org	gijc21.gijn.org	C=US, O=Let's Encrypt, CN=R3
8800967519	2023-03-04	2023-01-29	2024-01-28	impact.gijn.org	impact.gijn.org	C=US, O="Cloudflare, Inc.", CN=Cloudflare Inc RSA CA-2
8783292174	2023-03-02	2023-01-29	2024-01-28	cn.gijn.org	cn.gijn.org	C=US, O="Cloudflare, Inc.", CN=Cloudflare Inc RSA CA-2
8767079130	2023-02-20	2023-02-20	2023-05-21	gijn.org	gijn.org	C=US, O=Let's Encrypt, CN=R3
8695322554	2023-02-20	2023-02-20	2023-05-21	gijn.org	gijn.org	C=US, O=Let's Encrypt, CN=R3
8766820944	2023-02-20	2023-02-20	2023-05-21	cn.gijn.org	cn.gijn.org	C=US, O=Let's Encrypt, CN=R3
8694636863	2023-02-20	2023-02-20	2023-05-21	cn.gijn.org	cn.gijn.org	C=US, O=Let's Encrypt, CN=R3
8766821108	2023-02-20	2023-02-20	2023-05-21	impact.gijn.org	impact.gijn.org	C=US, O=Let's Encrypt, CN=R3
8695028240	2023-02-20	2023-02-20	2023-05-21	impact.gijn.org	impact.gijn.org	C=US, O=Let's Encrypt, CN=R3
8766544661	2023-02-20	2023-02-20	2023-05-21	www.gijn.org	www.gijn.org	C=US, O=Let's Encrypt, CN=R3
8694789196	2023-02-20	2023-02-20	2023-05-21	www.gijn.org	www.gijn.org	C=US, O=Let's Encrypt, CN=R3
8689588156	2023-02-19	2023-01-29	2024-01-28	gijc21.gijn.org	gijc21.gijn.org	C=US, O="Cloudflare, Inc.", CN=Cloudflare Inc RSA CA-2

Certificate Transparency Databases



crt.sh Certificate Search

Criteria: ID = '9423038660'

crt.sh ID	9423038660
Summary	Leaf certificate

Certificate Transparency

Log entries for this certificate:

Timestamp	Entry #	Log Operator	Log URL
2023-05-16 09:24:47 UTC	1099031106	Google	https://ct.googleapis.com/logs/argon2023

Revocation

Report a problem with this certificate to the CA

Mechanism	Provider	Status	Revocation Date	Last Observed in CRL	Last Checked (Error)
OCSP	The CA	Check	?	n/a	?
CRL	The CA	Not Revoked	n/a	n/a	2023-05-21 15:13:56 UTC
CRLSet/Blocklist	Google	Not Revoked	n/a	n/a	n/a
disallowedcert.stl	Microsoft	Not Revoked	n/a	n/a	n/a
OneCRL	Mozilla	Not Revoked	n/a	n/a	n/a

Certificate Fingerprints

SHA-256 ED6D607ABC52B669E19071740456EA0F62818CBD14683856E200275DC3F8B32A

SHA-1 E808B1405B622DDECBAA036636C2A29FBCEA2AAD

| ASN.1 | Certificate | Graph | Hierarchy | pv |

Hide metadata

Run cablint

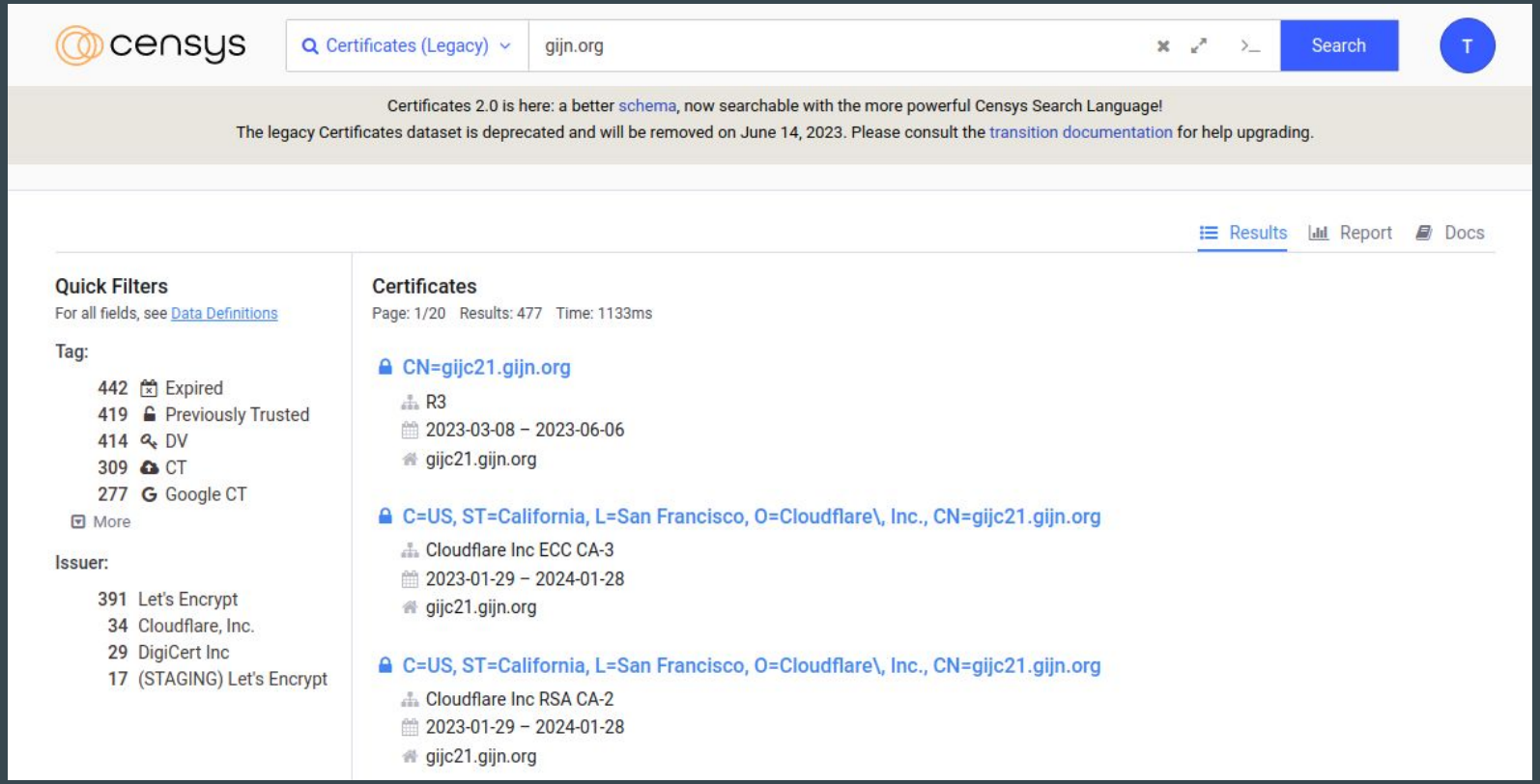
Run x509lint

Run zlint

Download Certificate: PEM

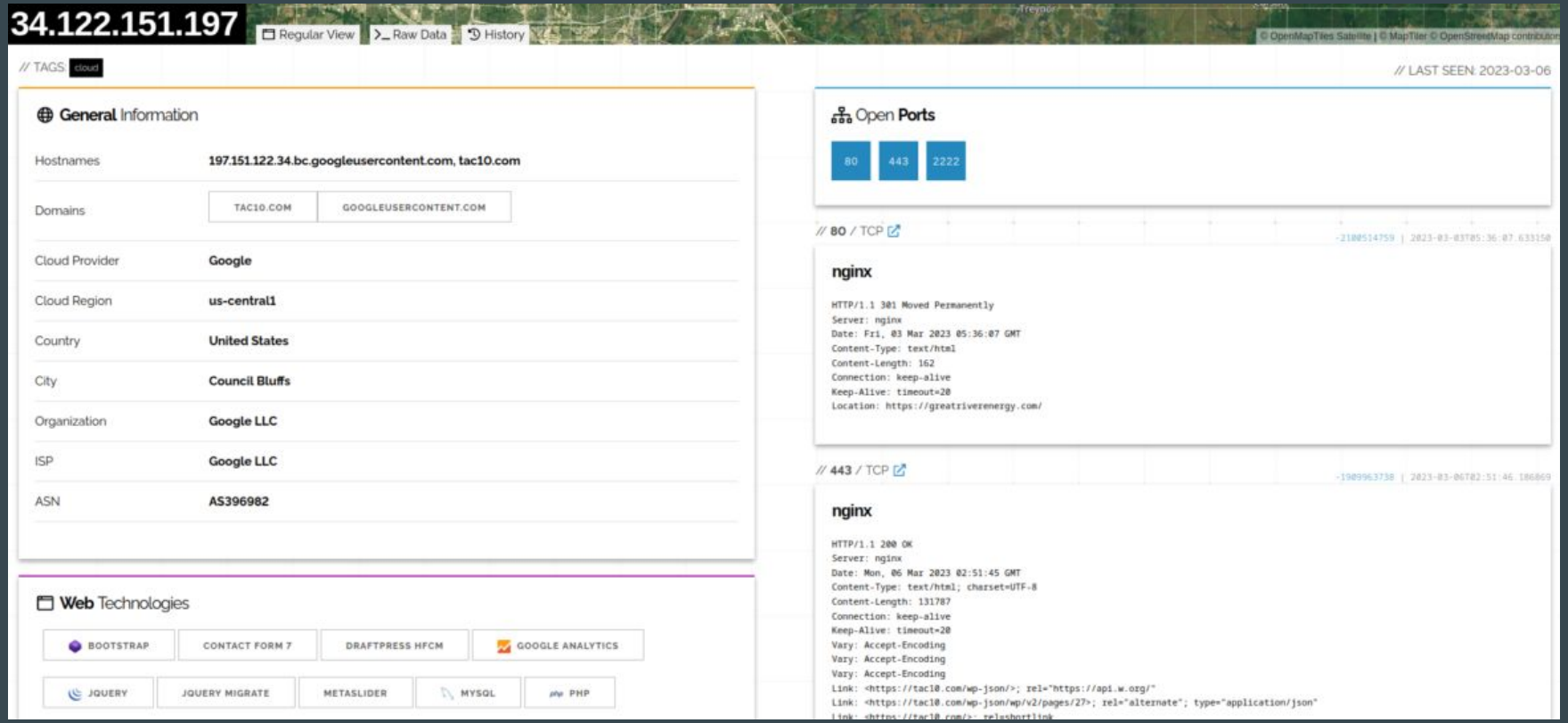
```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            04:b6:1a:73:96:88:45:f5:40:76:45:9c:8a:31:91:61:e6:9b
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: (CA ID: 183267)
            commonName               = R3
            organizationName         = Let's Encrypt
            countryName              = US
        Validity
            Not Before: May 16 08:24:47 2023 GMT
            Not After : Aug 14 08:24:46 2023 GMT
        Subject:
            commonName               = advisory.gijn.org
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:c9:05:90:46:fc:93:92:31:1a:d7:88:22:58:1e:
                    ca:1e:94:9d:8c:7c:34:71:3f:bc:0f:57:ec:ca:e6:
                    83:ce:45:c9:60:e7:4d:1d:07:35:fc:21:78:57:95:
                    aa:5d:14:5d:6a:3c:87:e7:8c:cf:59:1d:7f:75:bd:
                    ee:bd:bc:64:37:97:be:43:1a:ff:22:a3:96:6d:a8:
                    76:e9:bb:2e:0b:11:51:08:9d:b7:24:0d:b8:3f:4f:
                    86:48:fe:46:86:69:13:3e:7e:89:99:68:a8:b8:95:
                    14:04:ce:86:df:f5:b5:90:c1:5c:ee:16:f2:f0:7a:
                    ae:85:9e:7f:f0:84:16:7e:ab:75:18:af:95:a8:46:
                    75:4d:87:a1:a1:4d:91:7a:bd:a2:85:9f:1c:5d:d9:
```

Certificate Transparency Databases

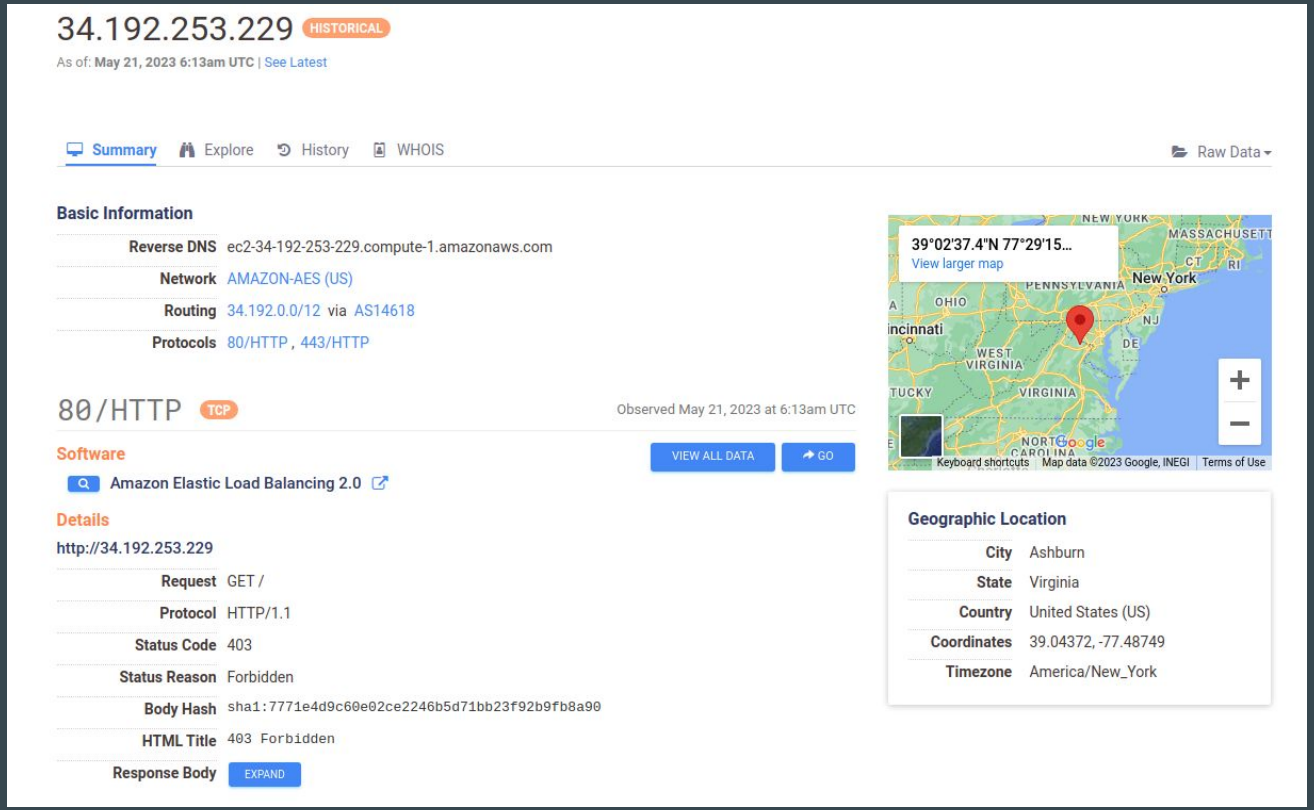


4 - Internet Wide Scans

Internet Wide Scans



Internet Wide Scans



5 - Bonus Analytics ID

Bonus: Analytics ID

```
        </style>
        <meta name="generator" content="Site Kit by Google 1.99.0" /><link rel="apple-touch-icon" href="/wp-content/uploads/2012/12/gijn-sq.png"/>            <script>
                    var _gaq = _gaq || [];
                    _gaq.push(['_setAccount', 'UA-25037912-1']);
                    _gaq.push(['_trackPageview']);
                    (function() {
                        var ga = document.createElement('script'); ga.type = 'text/javascript'; ga.async = true;
                        ga.src = ('https:' == document.location.protocol ? 'https://ssl' : 'http://www') + '.google-analytics.com/ga.js';
                        var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(ga, s);
                    })();
                </script>
                <link rel="icon" href="https://gijn.org/wp-content/uploads/2013/05/cropped-LogoGIJNGr-32x32.png" sizes="32x32" />
<link rel="icon" href="https://gijn.org/wp-content/uploads/2013/05/cropped-LogoGIJNGr-192x192.png" sizes="192x192" />
<link rel="apple-touch-icon" href="https://gijn.org/wp-content/uploads/2013/05/cropped-LogoGIJNGr-180x180.png" />
<meta name="msapplication-TileImage" content="https://gijn.org/wp-content/uploads/2013/05/cropped-LogoGIJNGr-270x270.png" />
        <style type="text/css" id="wp-custom-css">
            .entry-content p a {
color: #B83D48;
```

See https://www.bellingcat.com/resources/how-tos/2015/07/23/unveiling-hidden-connections-with-google-analytics-ids/

TRACKERS

1 - 25 of 1,781 | Sort : Last Seen Descending | 25 / Page | Download | Copy

Hostname	First	Last	Type	Value	Tags
gijn.org	2022-06-24	2023-05-24	TwitterShortlinkId	6jk7axdmsp	
gijn.org	2022-06-24	2023-05-24	TwitterId	mswojo04qz	
gijn.org	2022-06-24	2023-05-24	TwitterId	olafverhaeghe	
gijn.org	2022-06-24	2023-05-24	TwitterId	yan0	
gijn.org	2022-06-24	2023-05-24	TwitterShortlinkId	oralcztk7i	
gijn.org	2013-05-07	2023-05-24	GoogleAnalyticsAccountNumber	ua-25037912	
gijn.org	2013-05-07	2023-05-24	TwitterId	gijn	
gijn.org	2022-06-24	2023-05-24	TwitterId	lucguillemot	
gijn.org	2022-06-24	2023-05-24	TwitterShortlinkId	zvhvxaosw5	
gijn.org	2022-06-24	2023-05-24	TwitterId	mshalliemiller	
gijn.org	2022-06-24	2023-05-24	TwitterId	thomasroelens	
gijn.org	2021-07-01	2023-05-24	TwitterId	washingtonpost	
gijn.org	2022-06-24	2023-05-24	TwitterShortlinkId	mjqod7f9rz	
gijn.org	2021-03-31	2023-05-24	InstagramId	gijnorg	
gijn.org	2022-06-24	2023-05-24	TwitterShortlinkId	xem0gqu5la	
gijn.org	2022-06-24	2023-05-24	TwitterId	6jk7axdmsp	

RISKIQ ua-25037912

ua-25037912 (GoogleAnalyticsAccountNumber)

Tracker Search: Hosts 8 | Tracker Search: IP Addresses 47

DATA

Filters

HOSTNAME (8 / 8)

- advisory.gijn.org 1
- gijc21.gijn.org 1
- gijn.freshdesk.com 1
- gijn.org 1
- gijn.us5.list-man... 1

Show More

TAG

SYSTEM TAG

Tracker Search

1 - 8 of 8 | Sort : Last Seen Descending | 25 / Page

Hostname	First Seen	Last Seen
gijn.org	2013-05-07	2023-05-24
helpdesk.gijn.org	2018-01-29	2023-04-25
gijnstaging.wpengine.com	2023-04-20	2023-04-20
advisory.gijn.org	2022-06-03	2023-04-01
gijc21.gijn.org	2022-12-15	2023-03-17
gijn.us5.list-manage.com	2018-07-28	2023-01-31
mailchi.mp	2020-04-21	2020-07-28
gijn.freshdesk.com	2018-02-04	2018-02-04

1 - 8 of 8

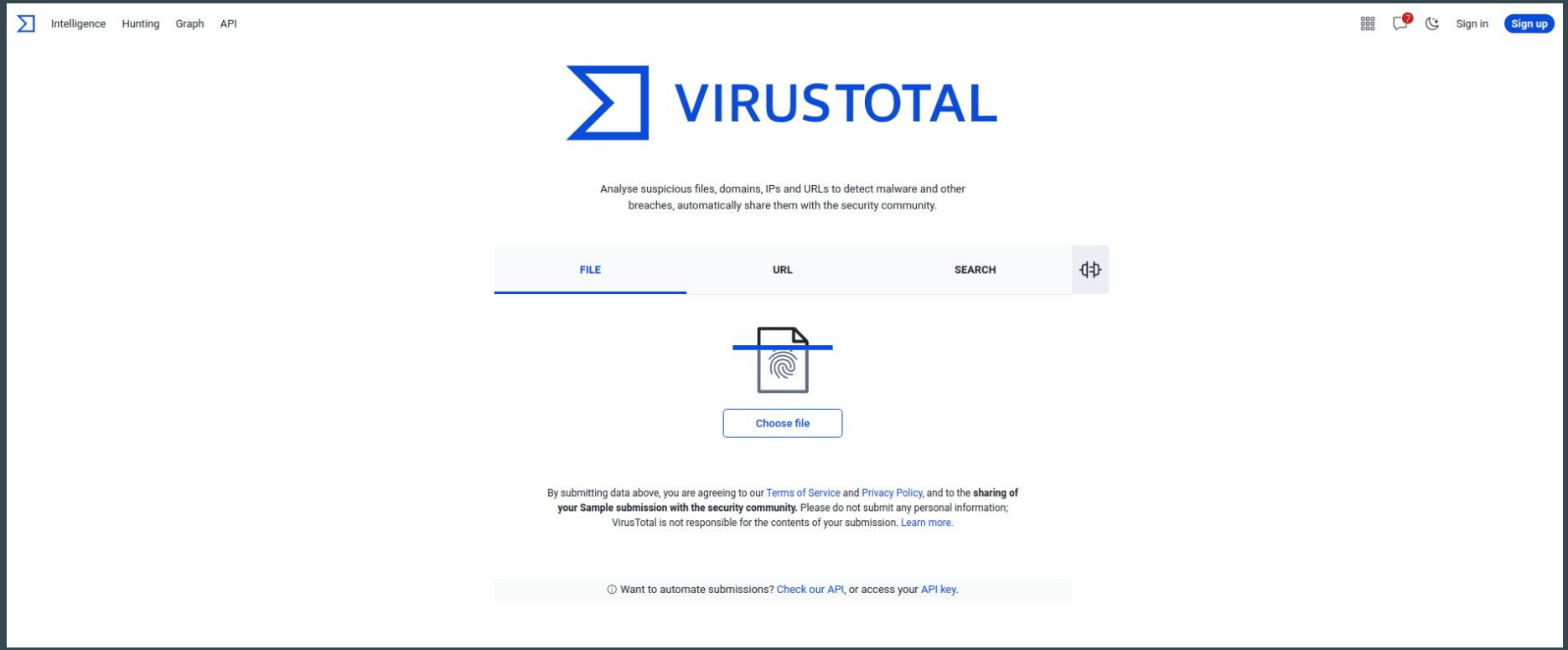
Exercise

What can you find on https://www.afp.com/ ?

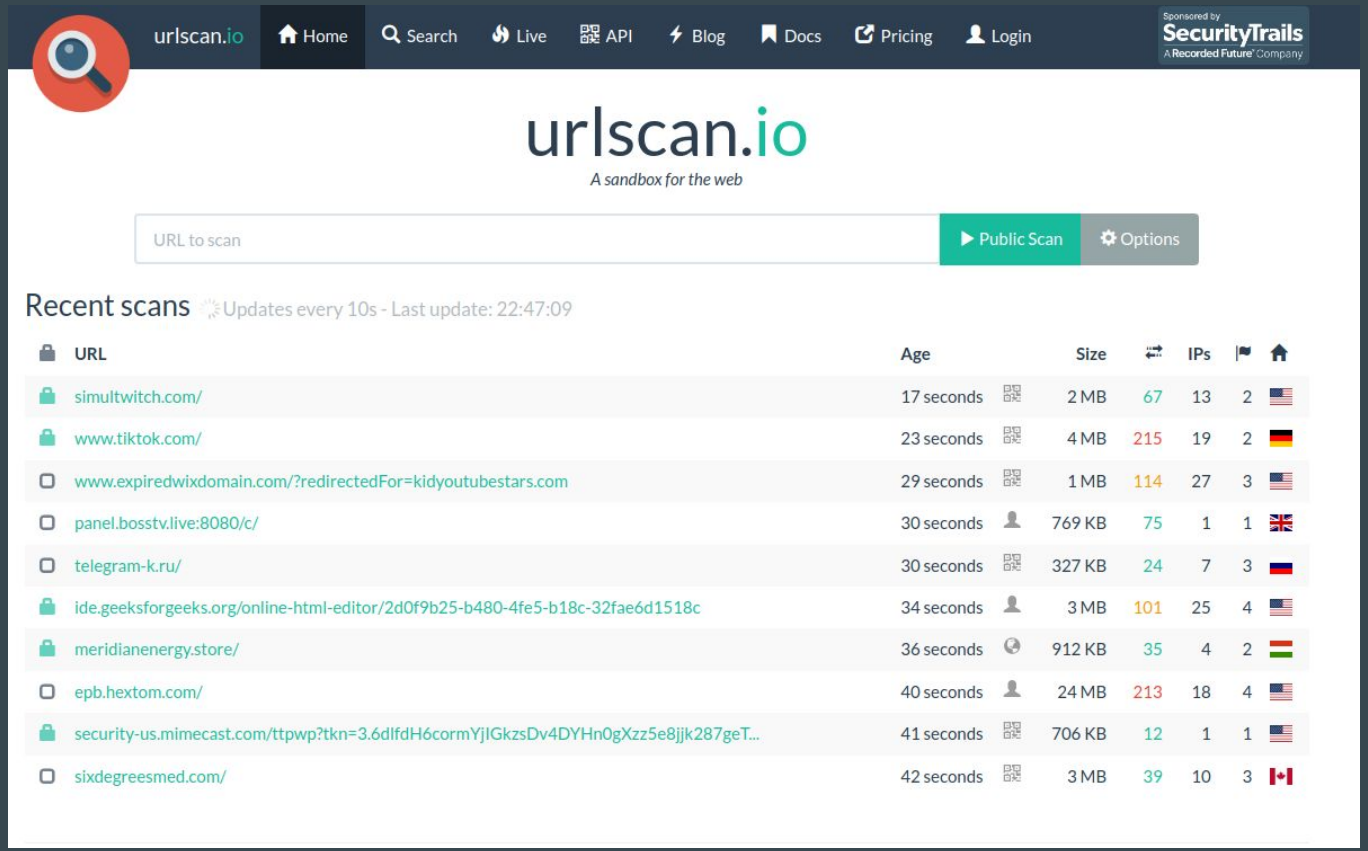
Break time

Additional Interesting Platforms

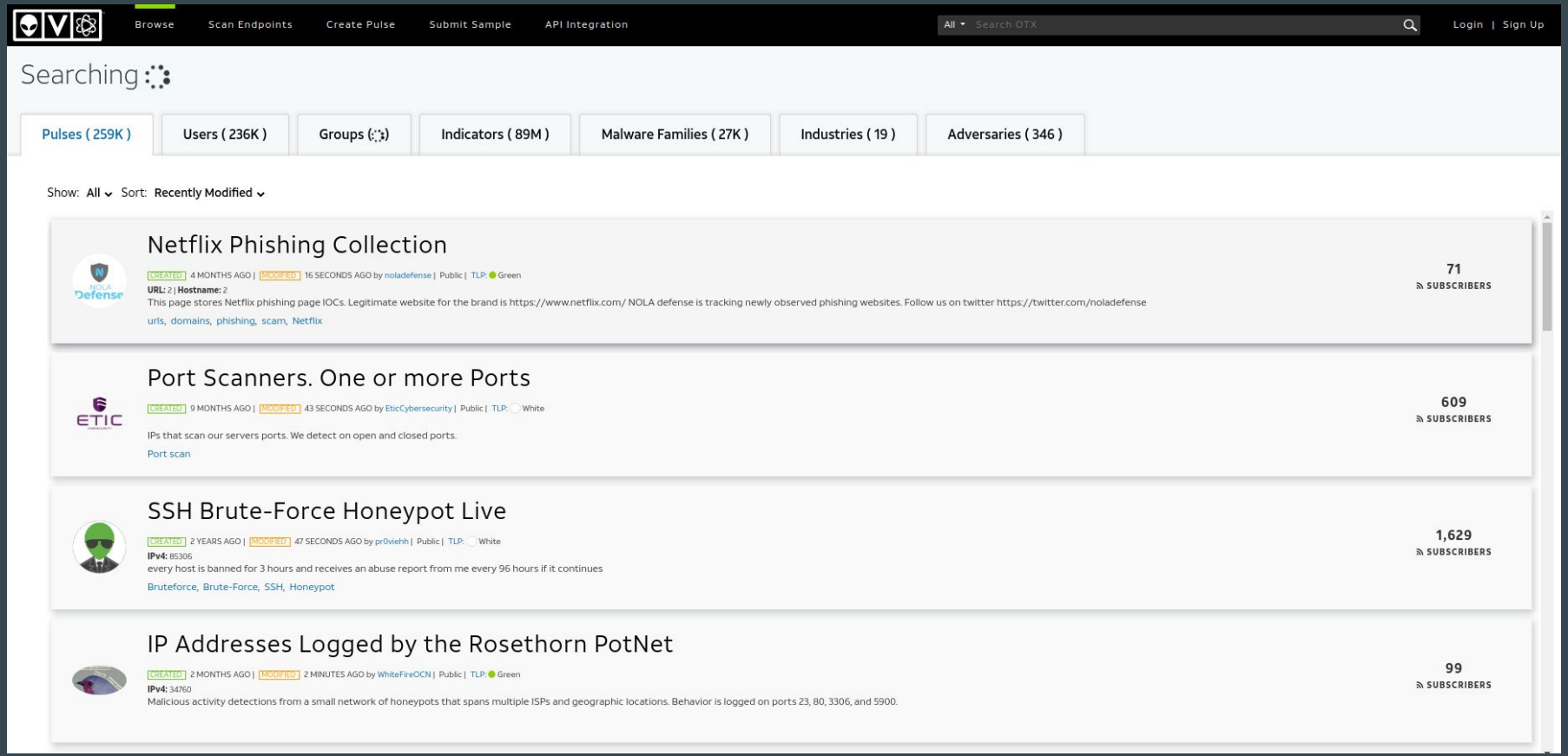
Virus Total

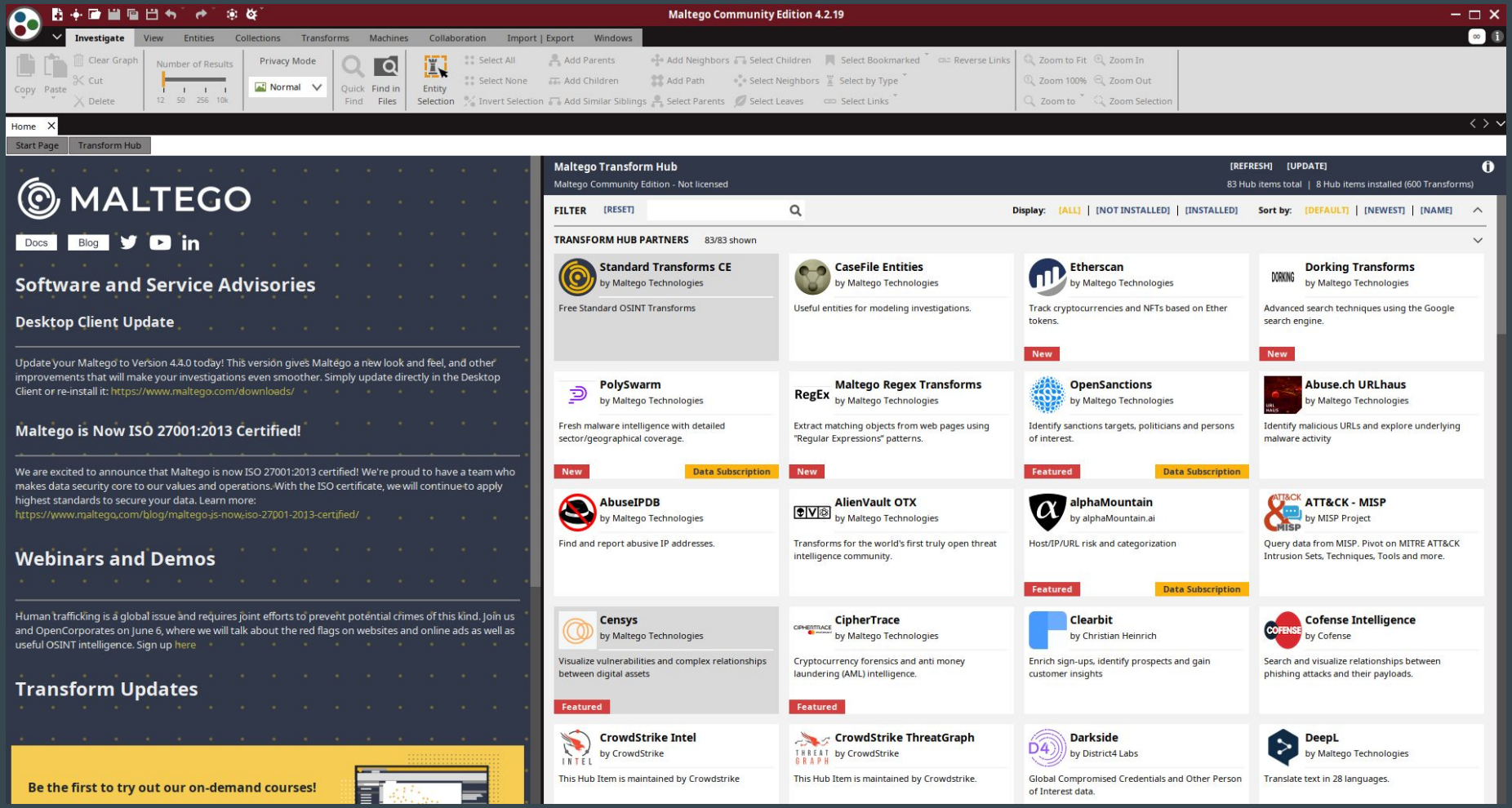

Intelligence
Hunting
Graph
API
Sign in
Sign up
VIRUSTOTAL
Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.
FILE
URL
SEARCH
Choose file
By submitting data above, you are agreeing to our Terms of Service and Privacy Policy, and to the sharing of your Sample submission with the security community. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.
Want to automate submissions? Check our API, or access your API key.

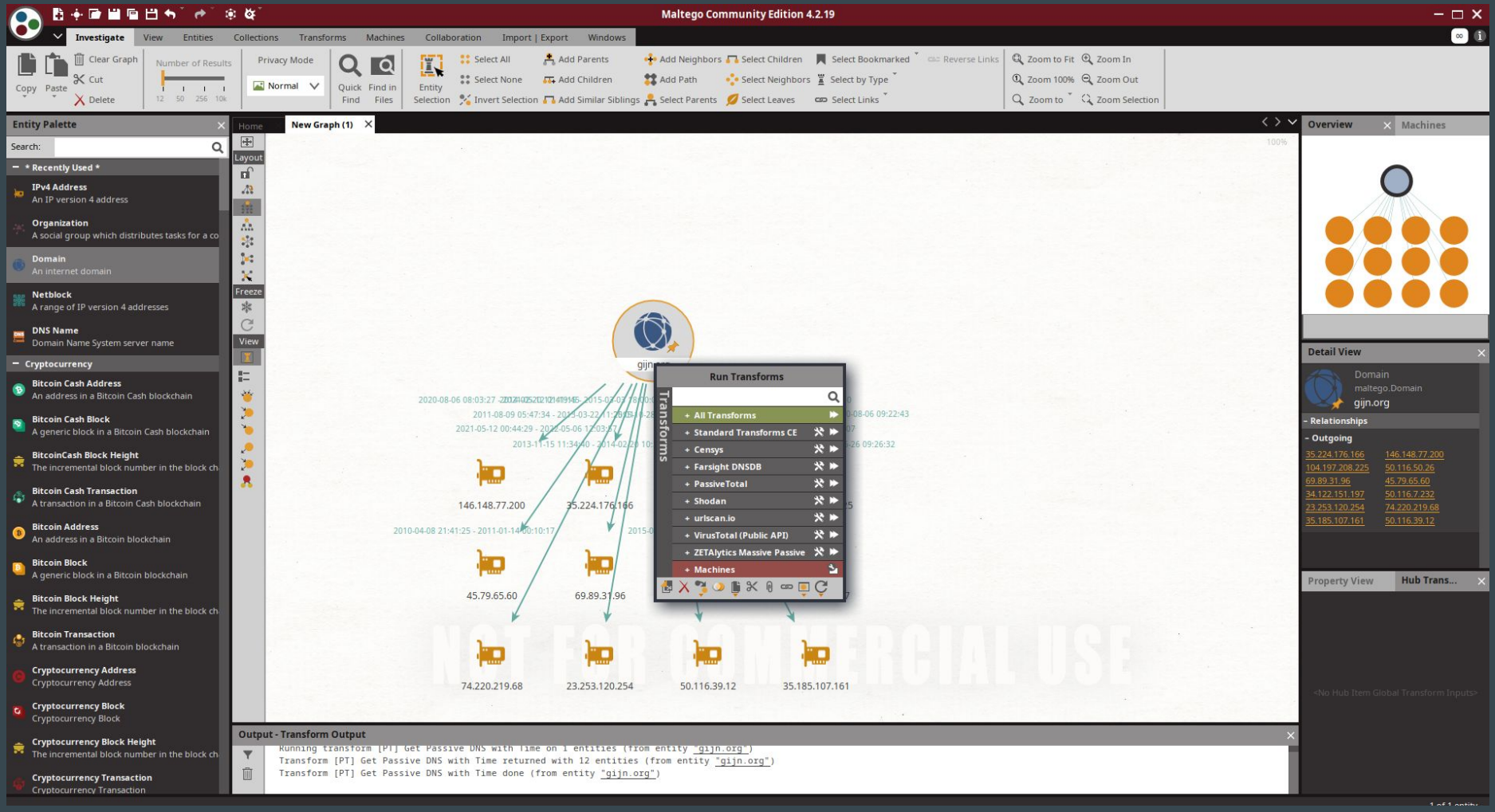
URL Scan


urlscan.io
Home
Search
Live
API
Blog
Docs
Pricing
Login
Sponsored by SecurityTrails A Recorded Future Company
urlscan.io
A sandbox for the web
URL to scan
Public Scan
Options
Recent scans
Updates every 10s - Last update: 22:47:09
URL
Age
Size
IPs
simultwitch.com/ 17 seconds 2 MB 67 13 2
www.tiktok.com/ 23 seconds 4 MB 215 19 2
www.expiredwixdomain.com/?redirectedFor=kidyoutubestars.com 29 seconds 1 MB 114 27 3
panel.bosstv.live:8080/c/ 30 seconds 769 KB 75 1 1
telegram-k.ru/ 30 seconds 327 KB 24 7 3
ide.geeksforgeeks.org/online-html-editor/2d0f9b25-b480-4fe5-b18c-32fae6d1518c 34 seconds 3 MB 101 25 4
meridianenergy.store/ 36 seconds 912 KB 35 4 2
epb.hextom.com/ 40 seconds 24 MB 213 18 4
security-us.mimecast.com/ttpwp?tkn=3.6dIfdH6cormYjIGkzsDv4DYHn0gXzz5e8jjk287geT... 41 seconds 706 KB 12 1 1
sixdegreesmed.com/ 42 seconds 3 MB 39 10 3

AlienVault OTX




Maltego Community Edition 4.2.19
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
Clear Graph
Cut
Delete
Copy
Paste
Number of Results
12
50
256
10k
Privacy Mode
Normal
Quick Find
Find in Files
Entity Selection
Select All
Select None
Invert Selection
Add Parents
Add Children
Add Similar Siblings
Add Neighbors
Add Path
Select Parents
Select Children
Select Neighbors
Select Leaves
Select Bookmarked
Select by Type
Select Links
Reverse Links
Zoom to Fit
Zoom In
Zoom 100%
Zoom Out
Zoom to
Zoom Selection
Home
Start Page
Transform Hub
MALTEGO
Docs
Blog
Software and Service Advisories
Desktop Client Update
Update your Maltego to Version 4.4.0 today! This version gives Maltego a new look and feel, and other improvements that will make your investigations even smoother. Simply update directly in the Desktop Client or re-install it: https://www.maltego.com/downloads/
Maltego is Now ISO 27001:2013 Certified!
We are excited to announce that Maltego is now ISO 27001:2013 certified! We're proud to have a team who makes data security core to our values and operations. With the ISO certificate, we will continue to apply highest standards to secure your data. Learn more:
https://www.maltego.com/blog/maltego-is-now-iso-27001-2013-certified/
Webinars and Demos
Human trafficking is a global issue and requires joint efforts to prevent potential crimes of this kind. Join us and OpenCorporates on June 6, where we will talk about the red flags on websites and online ads as well as useful OSINT intelligence. Sign up here
Transform Updates
Be the first to try out our on-demand courses!
Maltego Transform Hub
Maltego Community Edition - Not licensed
[REFRESH]
[UPDATE]
83 Hub items total | 8 Hub items installed (600 Transforms)
FILTER
[RESET]
Display: [ALL] | [NOT INSTALLED] | [INSTALLED]
Sort by: [DEFAULT] | [NEWEST] | [NAME]
TRANSFORM HUB PARTNERS
83/83 shown
Standard Transforms CE
by Maltego Technologies
Free Standard OSINT Transforms
CaseFile Entities
by Maltego Technologies
Useful entities for modeling investigations.
Etherscan
by Maltego Technologies
Track cryptocurrencies and NFTs based on Ether tokens.
New
Dorking Transforms
by Maltego Technologies
Advanced search techniques using the Google search engine.
New
PolySwarm
by Maltego Technologies
Fresh malware intelligence with detailed sector/geographical coverage.
New
Data Subscription
Maltego Regex Transforms
by Maltego Technologies
Extract matching objects from web pages using "Regular Expressions" patterns.
New
OpenSanctions
by Maltego Technologies
Identify sanctions targets, politicians and persons of interest.
Featured
Data Subscription
Abuse.ch URLhaus
by Maltego Technologies
Identify malicious URLs and explore underlying malware activity
AbuseIPDB
by Maltego Technologies
Find and report abusive IP addresses.
AlienVault OTX
by Maltego Technologies
Transforms for the world's first truly open threat intelligence community.
alphaMountain
by alphaMountain.ai
Host/IP/URL risk and categorization
Featured
Data Subscription
ATT&CK - MISP
by MISP Project
Query data from MISP. Pivot on MITRE ATT&CK Intrusion Sets, Techniques, Tools and more.
Censys
by Maltego Technologies
Visualize vulnerabilities and complex relationships between digital assets
Featured
CipherTrace
by Maltego Technologies
Cryptocurrency forensics and anti money laundering (AML) intelligence.
Featured
Clearbit
by Christian Heinrich
Enrich sign-ups, identify prospects and gain customer insights
Cofense Intelligence
by Cofense
Search and visualize relationships between phishing attacks and their payloads.
CrowdStrike Intel
by CrowdStrike
This Hub Item is maintained by Crowdstrike
CrowdStrike ThreatGraph
by CrowdStrike
This Hub Item is maintained by Crowdstrike.
Darkside
by District4 Labs
Global Compromised Credentials and Other Person of Interest data.
DeepL
by Maltego Technologies
Translate text in 28 languages.


Maltego Community Edition 4.2.19
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
Entity Palette
Search:
* Recently Used *
IPv4 Address
An IP version 4 address
Organization
A social group which distributes tasks for a co
Domain
An internet domain
Netblock
A range of IP version 4 addresses
DNS Name
Domain Name System server name
Cryptocurrency
Bitcoin Cash Address
An address in a Bitcoin Cash blockchain
Bitcoin Cash Block
A generic block in a Bitcoin Cash blockchain
BitcoinCash Block Height
The incremental block number in the block ch
Bitcoin Cash Transaction
A transaction in a Bitcoin Cash blockchain
Bitcoin Address
An address in a Bitcoin blockchain
Bitcoin Block
A generic block in a Bitcoin blockchain
Bitcoin Block Height
The incremental block number in the block ch
Bitcoin Transaction
A transaction in a Bitcoin blockchain
Cryptocurrency Address
Cryptocurrency Address
Cryptocurrency Block
Cryptocurrency Block
Cryptocurrency Block Height
The incremental block number in the block ch
Cryptocurrency Transaction
Cryptocurrency Transaction
Home
New Graph (1)
Layout
Freeze
View
Run Transforms
Transforms
All Transforms
Standard Transforms CE
Censys
Farsight DNSDB
PassiveTotal
Shodan
urlscan.io
VirusTotal (Public API)
ZETAlytics Massive Passive
Machines
146.148.77.200
35.224.176.166
45.79.65.60
69.89.31.96
74.220.219.68
23.253.120.254
50.116.39.12
35.185.107.161
NOT FOR COMMERCIAL USE
Output - Transform Output
Running transform [PT] Get Passive DNS with Time on 1 entities (from entity "gijn.org")
Transform [PT] Get Passive DNS with Time returned with 12 entities (from entity "gijn.org")
Transform [PT] Get Passive DNS with Time done (from entity "gijn.org")
Overview
Machines
Detail View
Domain
maltego.Domain
gijn.org
Relationships
Outgoing
35.224.176.166
146.148.77.200
104.197.208.225
50.116.50.26
69.89.31.96
45.79.65.60
34.122.151.197
50.116.7.232
23.253.120.254
74.220.219.68
35.185.107.161
50.116.39.12
Property View
Hub Trans...
<No Hub Item Global Transform Inputs>

Maltego

FEATURES INCLUDED	COMMUNITY	PRO
Maltego Desktop Application ⓘ	✓	✓
Self-hosted servers ⓘ	×	×
Multi-device usage ⓘ	×	×
VM deployment supported ⓘ	×	×
Enterprise Machines ⓘ	×	×
Results per Transform ⓘ	Up to 12 results per Transform and 10,000 Entities per graph	Up to 64,000 results per Transform and 1 million Entities per graph

A first list of platforms

https://gist.github.com/Te-k/2a5a1885249cfd07f417b47d291c4b98

Real Life Examples

1 - Endless Mayfly

Endless MayFly

Burned After Reading

Endless Mayfly's Ephemeral Disinformation Campaign

By Gabrielle Lim, Etienne Maynier, John Scott-Railton, Alberto Fittarelli, Ned Moran, and Ron Deibert

May 14, 2019

Download Disinformation Bibliography

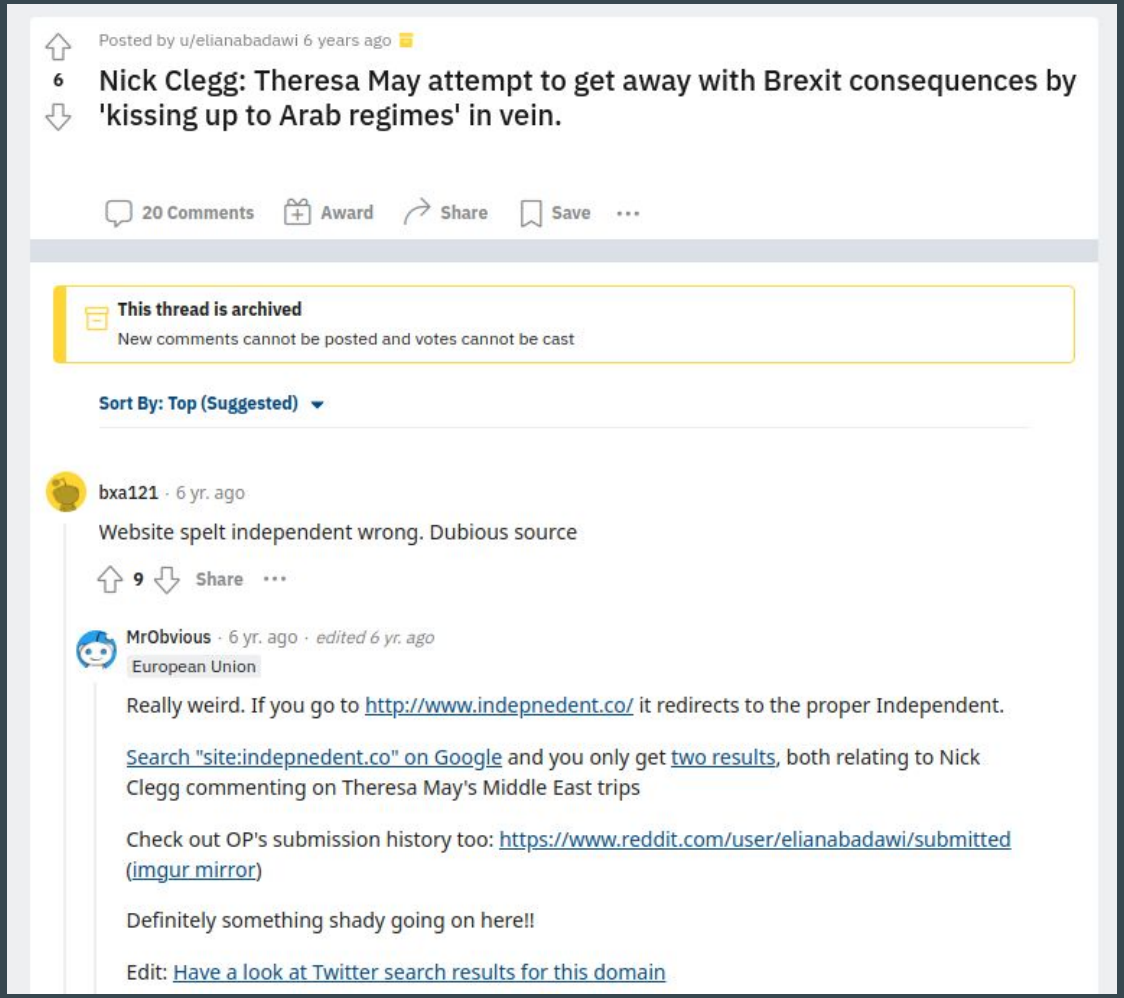
Endless Mayfly [1] *is an Iran-aligned network of inauthentic websites and online personas used to spread false and divisive information primarily targeting Saudi Arabia, the United States, and Israel. Using this network as an illustration, this report highlights the challenges of investigating and addressing disinformation from research and policy perspectives.*

Key Findings

- Endless Mayfly is an Iran-aligned network of inauthentic personas and social media accounts that spreads falsehoods and amplifies narratives critical of Saudi Arabia, the United States, and Israel.
- Endless Mayfly publishes divisive content on websites that impersonate legitimate media outlets. Inauthentic personas are then used to amplify the content into social media conversations. In some cases, these personas also privately and publicly engage journalists, political dissidents, and activists.
- Once Endless Mayfly content achieves social media traction, it is deleted and the links are redirected to the domain being impersonated. This technique creates an appearance of legitimacy, while obscuring the origin of the false narrative. We call this technique "ephemeral disinformation".

https://citizenlab.ca/2019/05/burned-after-reading-endless-mayflys-ephemeral-disinformation-campaign/

Weird Reddit Blogpost



Posted by u/elianabadawi 6 years ago

6

Nick Clegg: Theresa May attempt to get away with Brexit consequences by 'kissing up to Arab regimes' in vein.

20 Comments Award Share Save ...

This thread is archived

New comments cannot be posted and votes cannot be cast

Sort By: Top (Suggested)

bxa121 · 6 yr. ago

Website spelt independent wrong. Dubious source

9 Share ...

MrObvious · 6 yr. ago · *edited 6 yr. ago*

European Union

Really weird. If you go to http://www.indepnedent.co/ it redirects to the proper Independent.

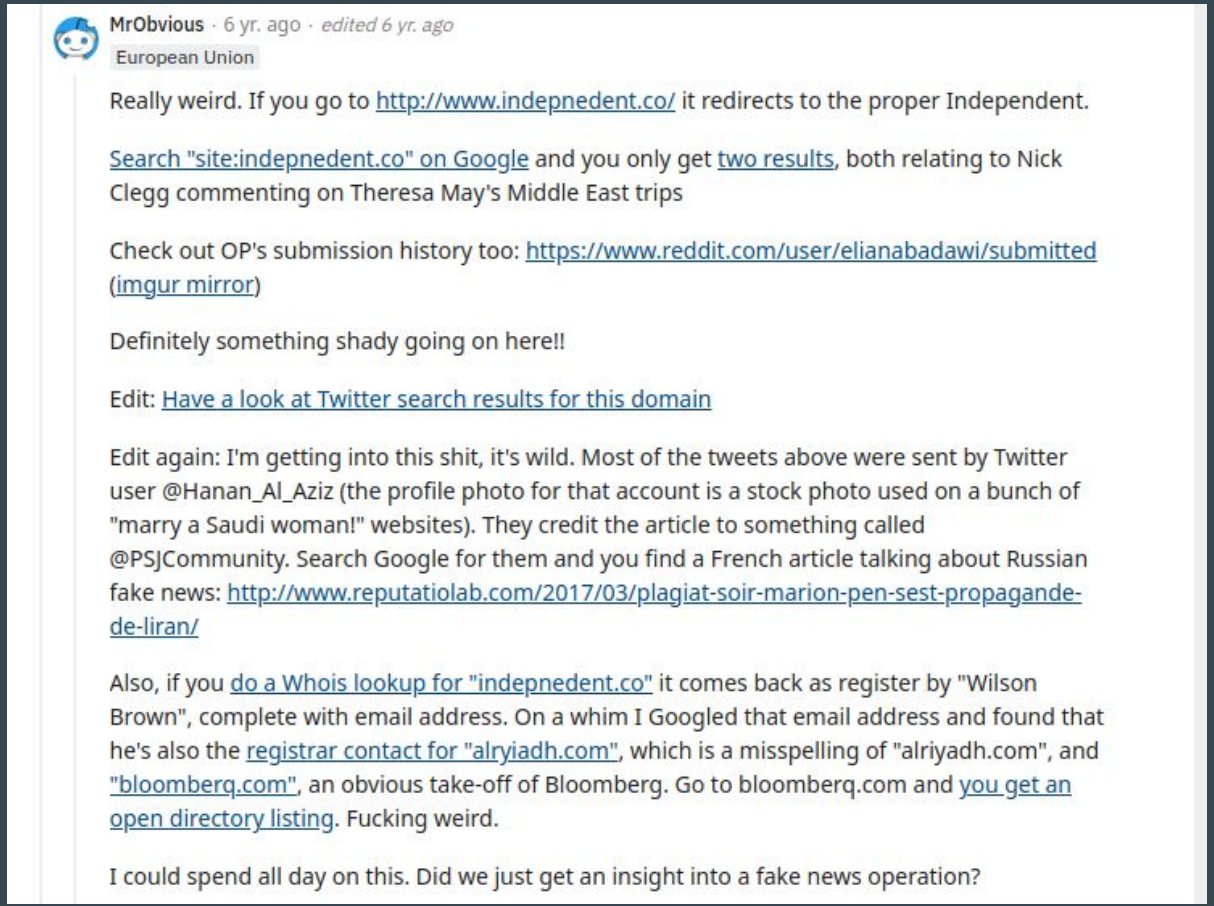
Search "site:indepnedent.co" on Google and you only get two results, both relating to Nick Clegg commenting on Theresa May's Middle East trips

Check out OP's submission history too: https://www.reddit.com/user/elianabadawi/submitted (imgur mirror)

Definitely something shady going on here!!

Edit: Have a look at Twitter search results for this domain

Weird Reddit Blogpost



MrObvious · 6 yr. ago · *edited 6 yr. ago*
European Union

Really weird. If you go to http://www.indepnedent.co/ it redirects to the proper Independent.

Search "site:indepnedent.co" on Google and you only get two results, both relating to Nick Clegg commenting on Theresa May's Middle East trips

Check out OP's submission history too: https://www.reddit.com/user/elianabadawi/submitted (imgur mirror)

Definitely something shady going on here!!

Edit: Have a look at Twitter search results for this domain

Edit again: I'm getting into this shit, it's wild. Most of the tweets above were sent by Twitter user @Hanan_Al_Aziz (the profile photo for that account is a stock photo used on a bunch of "marry a Saudi woman!" websites). They credit the article to something called @PSJCommunity. Search Google for them and you find a French article talking about Russian fake news: http://www.reputatiolab.com/2017/03/plagiat-soir-marion-pen-sest-propagande-de-liran/

Also, if you do a Whois lookup for "indepnedent.co" it comes back as register by "Wilson Brown", complete with email address. On a whim I Googled that email address and found that he's also the registrar contact for "alryiadh.com", which is a misspelling of "alriyadh.com", and "bloomberq.com", an obvious take-off of Bloomberg. Go to bloomberq.com and you get an open directory listing. Fucking weird.

I could spend all day on this. Did we just get an insight into a fake news operation?

eliana badawi
@eliana_badawi

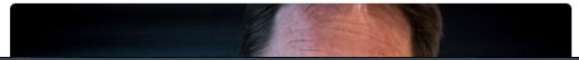
TWEETS	FOLLOWING	FOLLOWERS	LIKES
773	87	127	492

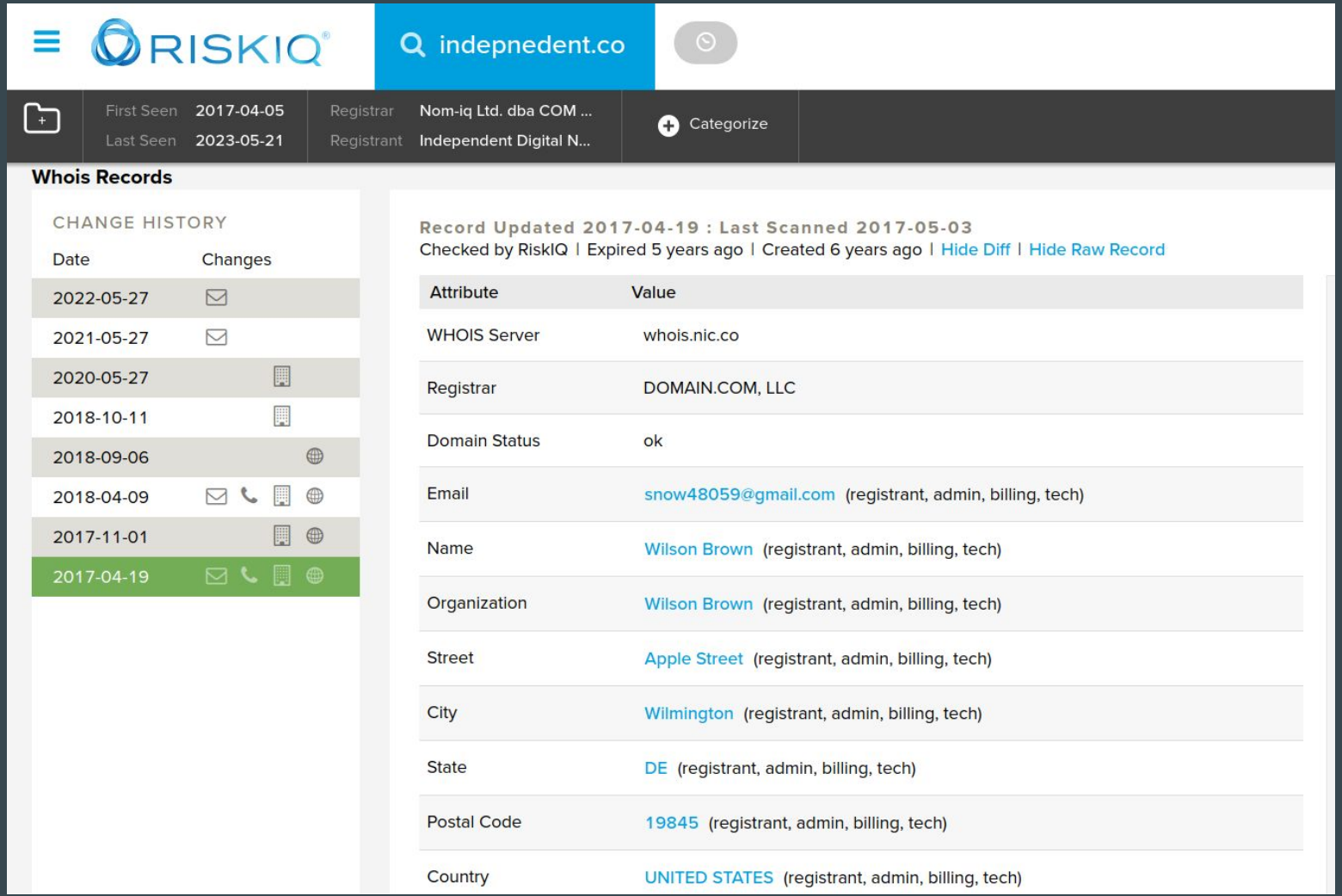
Clegg: Theresa May's trip to KSA politically motivated, in line with Ara...
Nick Clegg attacks PM May as she is paying a visit to Jordan and Saudi Arabia, calling the visit 'dancing to the tune' of the Arab regimes Getty.
indepnedent.co

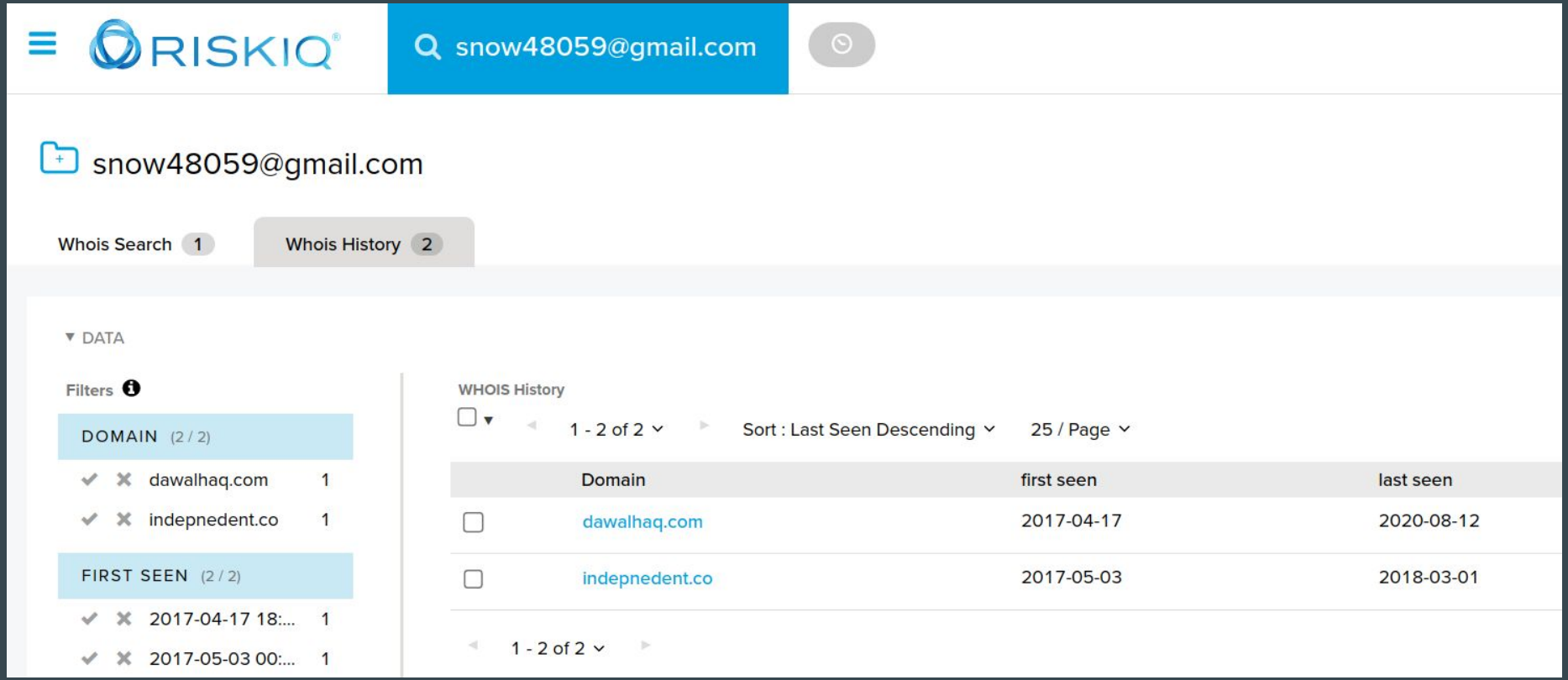
eliana badawi @eliana_badawi · 6h
@NYTimesCohen Hi. Please take a look at this! Clegg says May can't get away w/ Brexit by kissing up to Arabs!

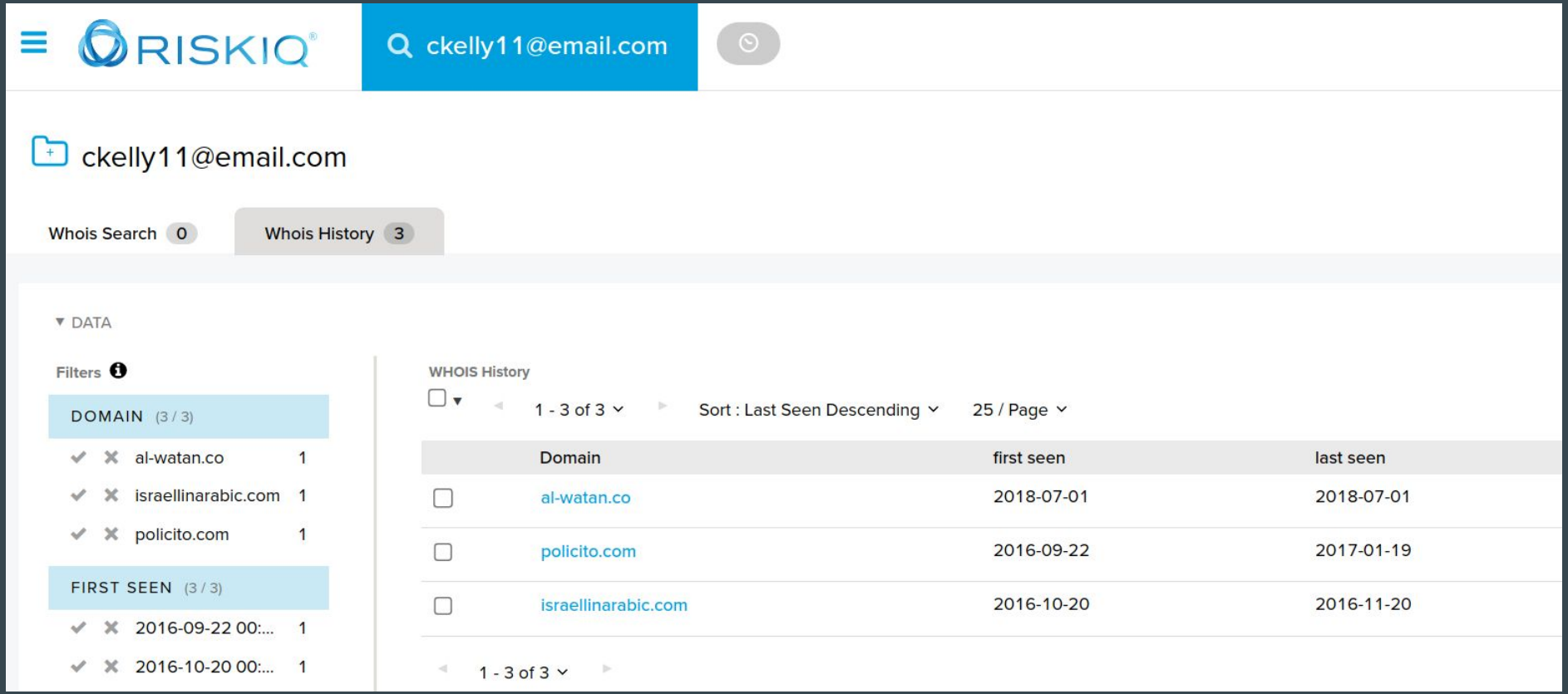
Clegg: Theresa May's trip to KSA politically motivated, in line with Ara...
Nick Clegg attacks PM May as she is paying a visit to Jordan and Saudi Arabia, calling the visit 'dancing to the tune' of the Arab regimes Getty.
indepnedent.co

eliana badawi @eliana_badawi · 6h
Replying to @khaproperty @Brexit @business
Hi. Please take a look at this! Clegg says May can't get away w/ Brexit by kissing up to Arabs!




RISKIQ
indepnedent.co
First Seen 2017-04-05
Last Seen 2023-05-21
Registrar Nom-iq Ltd. dba COM ...
Registrant Independent Digital N...
Categorize
Whois Records
CHANGE HISTORY
Date Changes
2022-05-27
2021-05-27
2020-05-27
2018-10-11
2018-09-06
2018-04-09
2017-11-01
2017-04-19
Record Updated 2017-04-19 : Last Scanned 2017-05-03
Checked by RiskIQ | Expired 5 years ago | Created 6 years ago | Hide Diff | Hide Raw Record
Attribute Value
WHOIS Server whois.nic.co
Registrar DOMAIN.COM, LLC
Domain Status ok
Email snow48059@gmail.com (registrant, admin, billing, tech)
Name Wilson Brown (registrant, admin, billing, tech)
Organization Wilson Brown (registrant, admin, billing, tech)
Street Apple Street (registrant, admin, billing, tech)
City Wilmington (registrant, admin, billing, tech)
State DE (registrant, admin, billing, tech)
Postal Code 19845 (registrant, admin, billing, tech)
Country UNITED STATES (registrant, admin, billing, tech)


RISKIQ
snow48059@gmail.com
snow48059@gmail.com
Whois Search 1
Whois History 2
DATA
Filters
DOMAIN (2 / 2)
dawalhaq.com 1
indepnedent.co 1
FIRST SEEN (2 / 2)
2017-04-17 18:... 1
2017-05-03 00:... 1
WHOIS History
1 - 2 of 2
Sort : Last Seen Descending
25 / Page
Domain
first seen
last seen
dawalhaq.com
2017-04-17
2020-08-12
indepnedent.co
2017-05-03
2018-03-01
1 - 2 of 2


RISKIQ
ckelly11@email.com
ckelly11@email.com
Whois Search 0
Whois History 3
DATA
Filters
DOMAIN (3 / 3)
al-watan.co 1
israellinarabic.com 1
policito.com 1
FIRST SEEN (3 / 3)
2016-09-22 00:... 1
2016-10-20 00:... 1
WHOIS History
1 - 3 of 3
Sort : Last Seen Descending
25 / Page
Domain
first seen
last seen
al-watan.co
2018-07-01
2018-07-01
policito.com
2016-09-22
2017-01-19
israellinarabic.com
2016-10-20
2016-11-20
1 - 3 of 3

Short URLS

Part 3: Content Consumption and Impact

This section describes the results of the network's activities in terms of content consumption and reactions from mainstream media.

Publicly available data from Twitter and link shorteners provide evidence that clicks and views were generated from the personas' activity. Based on the 44 short links identified in our investigation, 21,686 clicks were generated by Endless Mayfly content. The distribution of clicks, however, was not uniform with three links making up 76.5% of all clicks, one of which was promoted with the aid of Twitter bots.

Both Goo.gl and Bit.ly's APIs also provide data on the number of clicks by platform and country of origin. Based on the 44 short links, over half of the clicks originated from Saudi Arabia and approximately 20% from the United States. Regarding platforms, 68.2% of the clicks came from Twitter, 2.6% from Facebook, and 1.3% from iuvmpress.com, a pro-Iran media outlet we identified as part of the republishing network.

Short URLs

	Type	hash	Date	Domain	Redirection
2	bit.ly	2exP0Jd	10/27/2016 2:09:41	israellinarabic[.]com	http://israellinarabic[.]com/أسماء-ضباط-إسرائيلين-قاعدة-لملك-فيصل/
3	bit.ly	2exWPhu	11/5/2016 3:22:37	alryiadh[.]com	hxxp://alryiadh[.]com/1545748/
4	goo.gl	ZyqkTU	09/20/2017 13:10:10	theatlatnic[.]com	hxxp://theatlatnic[.]com/international/archive/2017/09/shocking-document-shameful-acts-saudi-emiratis-cover-human-rights-abus
5	goo.gl	7pCH25	8/12/2017 11:10:28	xn--theguardan-4ub[.]com	hxxp://xn--theguardan-4ub[.]com/world/2017/aug/12/former-mi6-chief-admits-defeat-putin-russia-fragmentation-strategic-plan/
6	bit.ly	2tWlQfw	7/31/2017 6:24:37	alarabyia[.]org	hxxp://alarabyia[.]org/ar/last-page/2017/07/31/المملكة-خالفت-المشروع-الذي-قدمته-دولة-الإمارات-لاجتماع-الرباعية-العربية.html
7	goo.gl	NQbUVT	2/13/2017 11:01:56	alryiadh[.]com	hxxp://www.alryiadh[.]com/1571713/
8	goo.gl	MJSbQU	8/9/2017 11:35:16	theatlatnic[.]com	hxxp://theatlatnic[.]com/international/archive/2017/08/crown-prince-mohammed-bin-salman-appoints-his-brother-as-saudi-fm/538
9	bit.ly	2f5cese	8/1/2017 9:58:10	alnaḥaregypt[.]com	hxxp://alnaḥaregypt[.]com/t~541873/
10	goo.gl	vLzyjJ	2/18/2017 5:41:04	lesoir[.]info	hxxp://lesoir[.]info/1445748/article/actualite/france/2017-02-16/emmanuel-macron-candidat-prefere-de-arabie-saoudite/
11	goo.gl	BD4dvN	7/30/2017 5:05:33	xn--emaraalyoum-1b9e[.]com	hxxp://xn--emaraalyoum-1b9e[.]com/local-section/other/2017-07-29-1.1015498/index.html
12	bit.ly	2fquXyx	11/1/2016 8:27:49	mintpressnevvs[.]com	hxxp://mintpressnevvs[.]com/qatar-oiled-german-firm-palm-to-pull-out-of-tanks-deal-with-saudi-arabia/221898/
13	bit.ly	2lcSlNe	2/26/2017 6:05:40	mintpressnevvs[.]com	hxxp://mintpressnevvs[.]com/merkel-expresses-her-concerns-over-eu-future/225418/
14	bit.ly	2eJqxCv	10/20/2016 5:06:00	israellinarabic[.]com	hxxp://www.israellinarabic[.]com/الحاخام-الدول العربية-تعزية بيرز/
15	bit.ly	2dm2lA6	10/17/2016 6:00:10	bundesergierung[.]de	hxxp://bundesergierung[.]de/Content/EN/2016/10_en/2016-10-17-beziehung-saudi-arabien-vereinigte-staaten_en.html
16	bit.ly	2rcr6dC	06/10/2017 14:32:08	alettehad[.]net	hxxp://alettehad[.]net/details.php_id=34752_y=2017/
17	goo.gl	ShQ1l6	10/20/2016 7:23:25	israellinarabic[.]com	hxxp://www.israellinarabic[.]com/%D8%A7%D9%84%D8%B3%D8%B9%D9%88%D8%AF%D9%8A%D8%A9%20%E2%80%93%20%D8%
18	bit.ly	2gYkjzM	7/25/2017 1:23:40	xn--theguardia-dq2e[.]com	hxxp://theguardiaṇ[.]com/us-news/2017/july/25/us-house-put-middle-east-parties-on-terrorist-list/index.html
19	goo.gl	bu7jFb	2/14/2017 14:25:50	alryiadh[.]com	hxxp://www.alryiadh[.]com/1571724/
20	bit.ly	2vqRe2i	7/16/2017 8:36:25	xn--sraelinarabic-29b[.]com	hxxp://ısraelinarabic[.]com/مسعود-بارزاني-اجتمع-مع-السلطات-الإسرائيلية-أثناء-زيارته-في-الأردن/

2 - Phishing from Uzbekistan

SHARE

< RESEARCH

March 12, 2020

Targeted Surveillance Attacks in Uzbekistan: An Old Threat with New Techniques

Introduction

A new Amnesty International investigation has identified a campaign of phishing and spyware attacks targeting Human Rights Defenders (HRDs) from Uzbekistan.

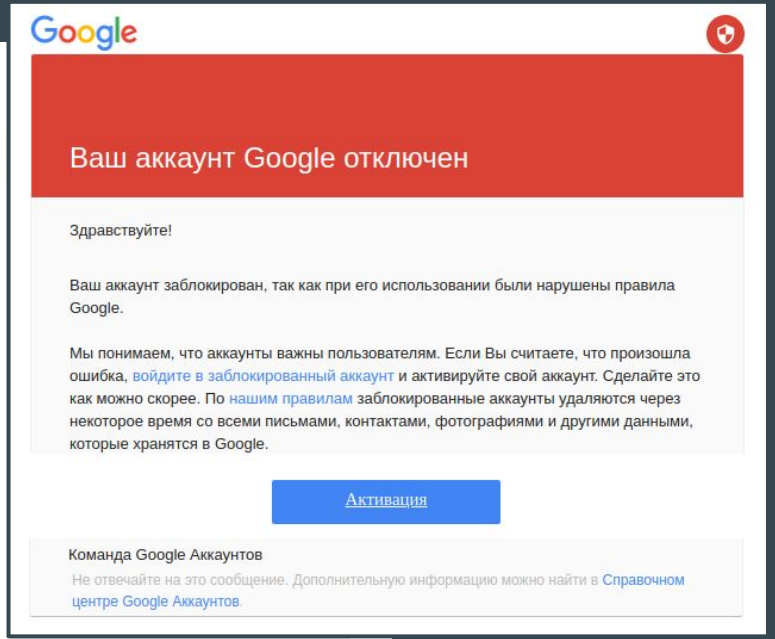
In May 2019, the Canadian non-profit organisation eQualitie released **a report** describing an attack campaign using web and phishing attacks against journalists and activists working on Uzbekistan. Based on this report, we began tracking the group that was behind these attacks. We identified a broader infrastructure along with new Windows and Android spyware used by the attackers.

During the investigation, we identified a partial list of targets that confirmed that activists and journalists were targeted by this campaign. This report documents a worrying evolution in the surveillance threat facing HRDs in Uzbekistan, which now appear more sophisticated than previously documented, and able to bypass some security tools HRDs use to protect themselves against surveillance.

Human Rights and Surveillance in Uzbekistan

Amnesty International has documented serious human rights violations, including **pervasive torture by security forces and arbitrary detention**, in Uzbekistan. Impunity for past abuses continues to prevail despite recent reforms of the criminal justice system and **the closure of detention centers notorious for torture**. While more independent media outlets have now been able to operate inside Uzbekistan, the rights to freedom of expression, association and peaceful assembly continue to be tightly regulated, and civil society activists face reprisals for their peaceful activities.

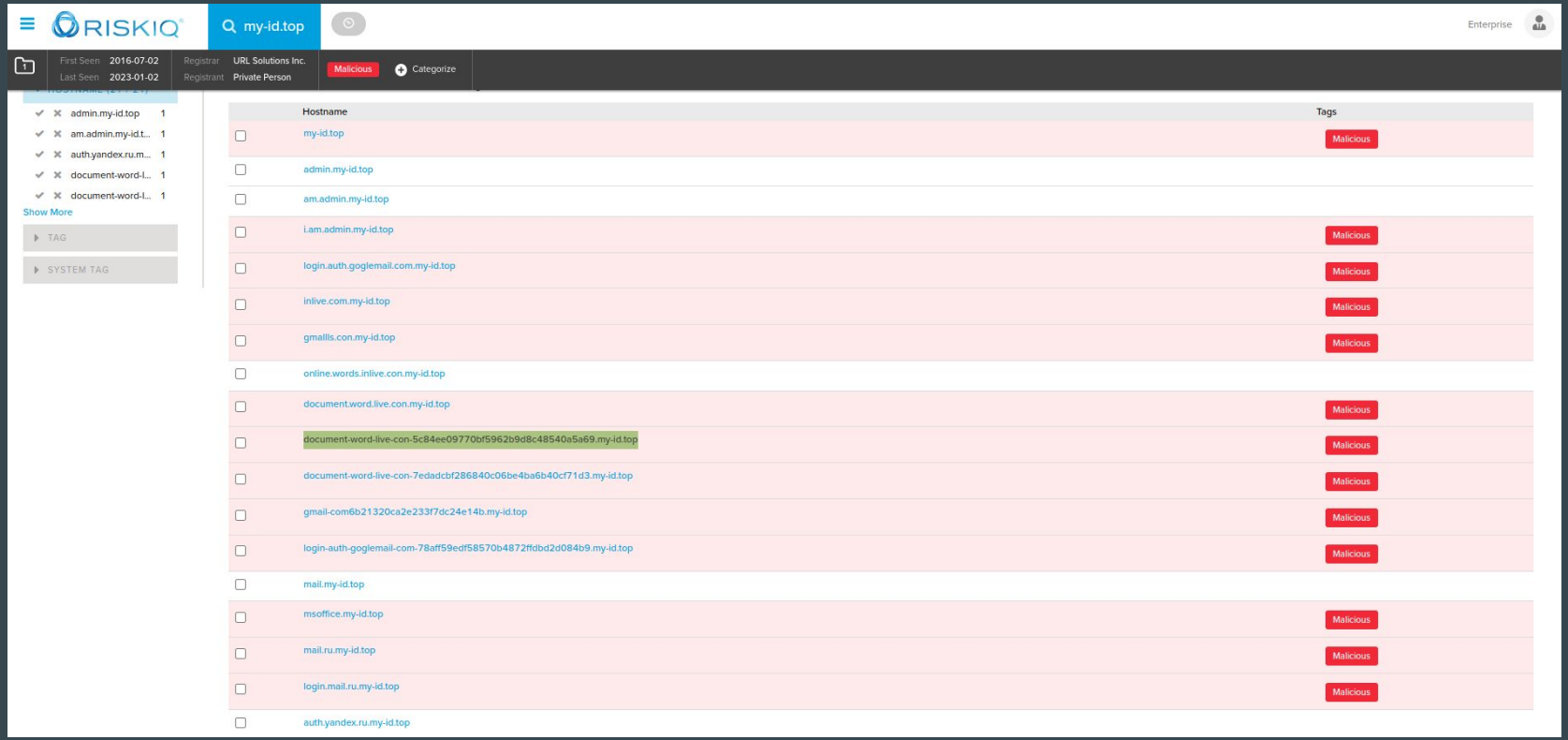
The threat of torture, its actual use and sexual violence, have forced many HRDs, government critics and independent journalists to leave Uzbekistan. The few who remain in the country, including activists and

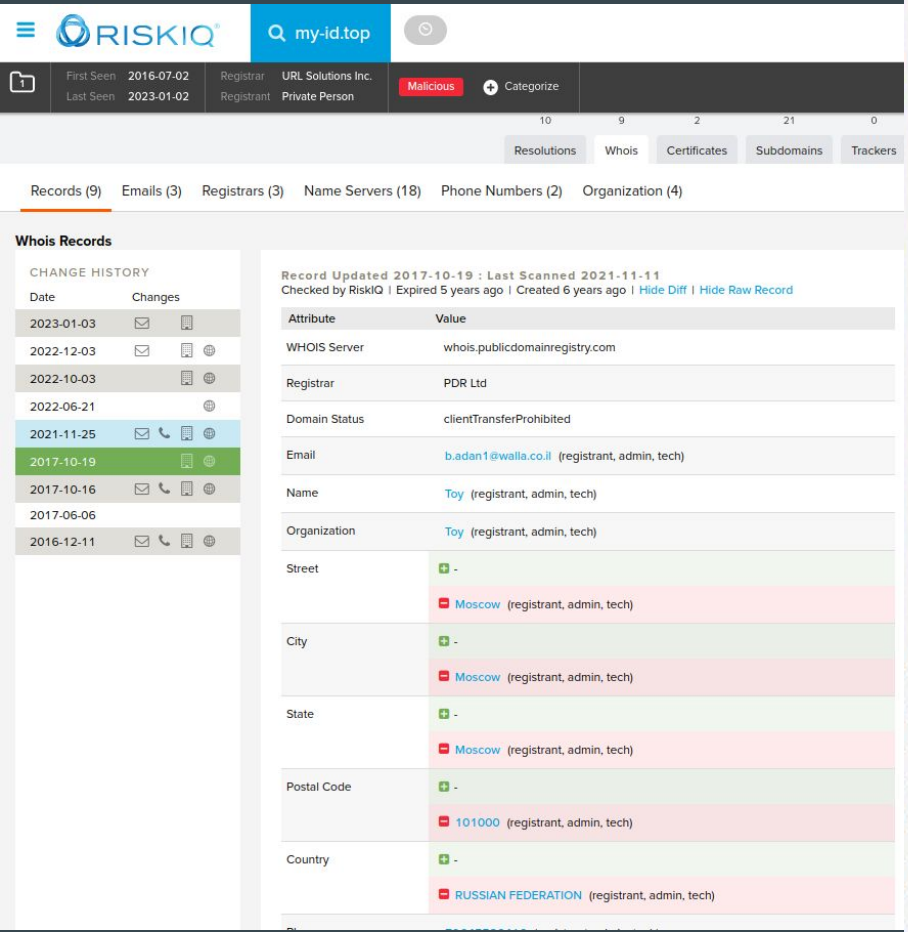


Chad: Still No Reparations for Hissène Habré's Victims

https://www.amnesty.org/en/latest/research/2020/03/targeted-surveillance-attacks-in-uzbekistan-an-old-threat-with-new-techniques/

document-word-live-con-5c84ee09770bf5962b9d8c48540a5a69.my-id.top used in the email -> my-id.top





Domain Name: my-id.top
Registry Domain ID: D20171017G10001G_25378536-top
Registrar WHOIS Server: whois.publicdomainregistry.com
Registrar URL: http://publicdomainregistry.com
Updated Date: 2017-10-19T06:01:15Z
Creation Date: 2017-10-16T20:51:28Z
Registry Expiry Date: 2018-10-16T20:51:28Z
Registrar: PDR Ltd
Registrar IANA ID: 303
Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com
Registrar Abuse Contact Phone: +91.2013775952
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: C20171017C_22881075-top
Registrant Name: Toy
Registrant Organization: Toy
Registrant Street: Moscow
Registrant City: Moscow
Registrant State/Province: Moscow
Registrant Postal Code: 101000
Registrant Country: RU
Registrant Phone: +7.9645536416
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: b.adan1@walla.co.il
Registry Admin ID: C20171017C_22881075-top
Admin Name: Toy
Admin Organization: Toy
Admin Street: Moscow
Admin City: Moscow
Admin State/Province: Moscow
Admin Postal Code: 101000
Admin Country: RU
Admin Phone: +7.9645536416
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: b.adan1@walla.co.il
Registry Tech ID: C20171017C_22881075-top

RISKIQ b.adan1@walla.co.il Enterprise

b.adan1@walla.co.il

Whois Search 2 | Whois History 13

DATA

Filters

DOMAIN (13 / 13)
- auth-mail.com 1
- auth-mail.me 1
- fixerman.top 1
- m-youtube.org 1
- m-youtube.top 1

Show More

FIRST SEEN (11 / 13)
- 2017-10-04 07:... 2
- 2017-10-17 07:... 2
- 2016-12-08 00:... 1
- 2016-12-08 12:... 1
- 2016-12-22 14:... 1

Show More

LAST SEEN (10 / 13)
- 2018-10-04 07:... 4
- 2017-03-10 00:... 1
- 2017-12-28 00:... 1
- 2018-05-06 10:... 1
- 2018-07-02 16:... 1

Show More

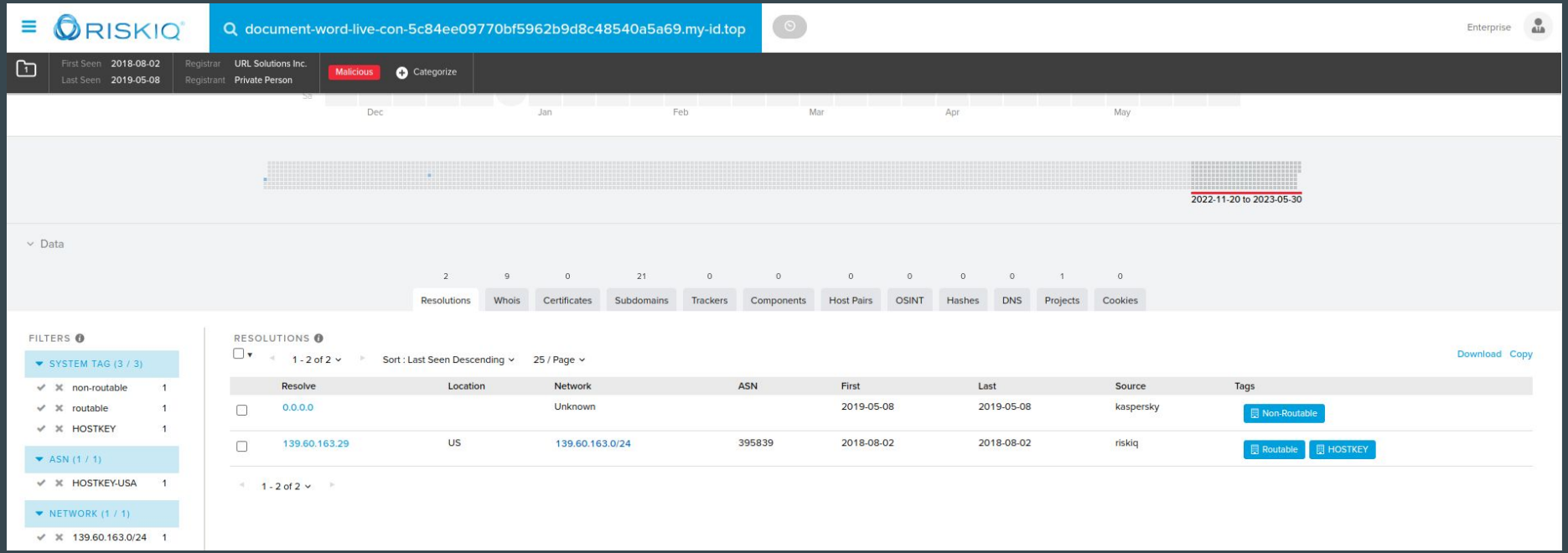
WHOIS History

1 - 13 of 13 | Sort : Last Seen Descending | 25 / Page | Download | Copy

Domain	first seen	last seen	Tags
my-id.top	2017-10-17	2021-11-11	Malicious
msoffice365-online.org	2016-12-08	2020-12-15	
m-youtube.top	2018-11-26	2020-12-15	
auth-mail.com	2017-08-08	2018-11-28	Malicious
mail-auth.top	2017-10-17	2018-10-17	
fixerman.top	2017-10-10	2018-10-04	
vzlom.top	2017-10-04	2018-10-04	
pochta.top	2017-10-04	2018-10-04	
secretonline.top	2017-10-10	2018-10-04	
msoffice365.win	2016-12-08	2018-07-02	Malicious, phishing
mail-support.info	2016-12-27	2018-05-06	Malicious
auth-mail.me	2017-08-07	2017-12-28	
m-youtube.org	2016-12-22	2017-03-10	

1 - 13 of 13

Also using Passive DNS data



RISKIQ 139.60.163.29 Enterprise

First Seen 2017-10-12 | Last Seen 2022-07-14 | ASN AS395839 - HOSTKEY-USA | Organization HOSTKEY | Netblock 139.60.163.0/24 | US | Routable | HOSTKEY | Categorize

☐	www.donna-girls.space	2019-02-27	2019-02-28	riskiq	
☐	www.donna--girls.space	2019-02-02	2019-02-27	riskiq	
☐	my-cabinet.com	2017-10-19	2018-09-17	riskiq, kaspersky	
☐	mail-auth.top	2017-10-21	2018-09-16	riskiq	
☐	my-id.top	2017-10-22	2018-09-13	riskiq	Malicious
☐	inlive.com.my-id.top	2018-08-08	2018-09-10	riskiq, kaspersky	Malicious
☐	www.mail-auth.top	2018-08-20	2018-08-20	riskiq	Malicious
☐	mycabinet.xyz	2017-10-21	2018-08-08	riskiq	Malicious
☐	document.word.live.con.my-id.top	2018-08-02	2018-08-02	riskiq	Malicious
☐	document-word-live-con-5c84ee09770bf5962b9d8c48540a5a69.my-id.top	2018-08-02	2018-08-02	riskiq	Malicious
☐	ftp.my-cabinet.com	2018-08-01	2018-08-01	riskiq	Malicious
☐	document-word-live-con-7edadcbf286840c06be4ba6b40cf71d3.my-id.top	2018-07-30	2018-07-30	riskiq	Malicious
☐	i.am.admin.my-id.top	2018-07-23	2018-07-23	riskiq	Malicious
☐	login.auth.goglemail.com.my-id.top	2018-07-13	2018-07-13	riskiq	Malicious
☐	login-auth-goglemail-com-78aff59edf58570b4872ffdbd2d084b9.my-id.top	2018-07-12	2018-07-13	riskiq	Malicious
☐	gmallls.con.my-id.top	2018-07-10	2018-07-10	riskiq	Malicious
☐	gmail-com6b21320ca2e233f7dc24e14b.my-id.top	2018-07-05	2018-07-05	riskiq	Malicious
☐	www.my-id.top	2018-06-25	2018-06-25	riskiq	Malicious

3 - Lavina Pulse

Lavina Pulse

CYBERSECURITY • DAILY COVER

Exclusive: Meet Russia's Cambridge Analytica, Run By A Former KGB Agent Turned YouTube Influencer

https://www.forbes.com/sites/thomasbrewster/2023/03/21/andrei-masalovich-avalanche-russia-cambridge-analytica/?sh=3a9fdfb8424a

Nicaraguans have also been targeted by Avalanche, according to Meta. Web domain records also show a working Avalanche login page referencing the country's capital, Managua. Nicaragua's regime under President Daniel Ortega has been criticized by the U.S. State Department and nonprofits like Human Rights Watch for detaining government critics and barring opposition political parties ahead of the 2021 elections. Masalovich would neither confirm nor deny if Ortega's country was a customer. The Nicaraguan government did not respond to requests for comment.

How would you do?

Find all domains related with Lavina Pulse

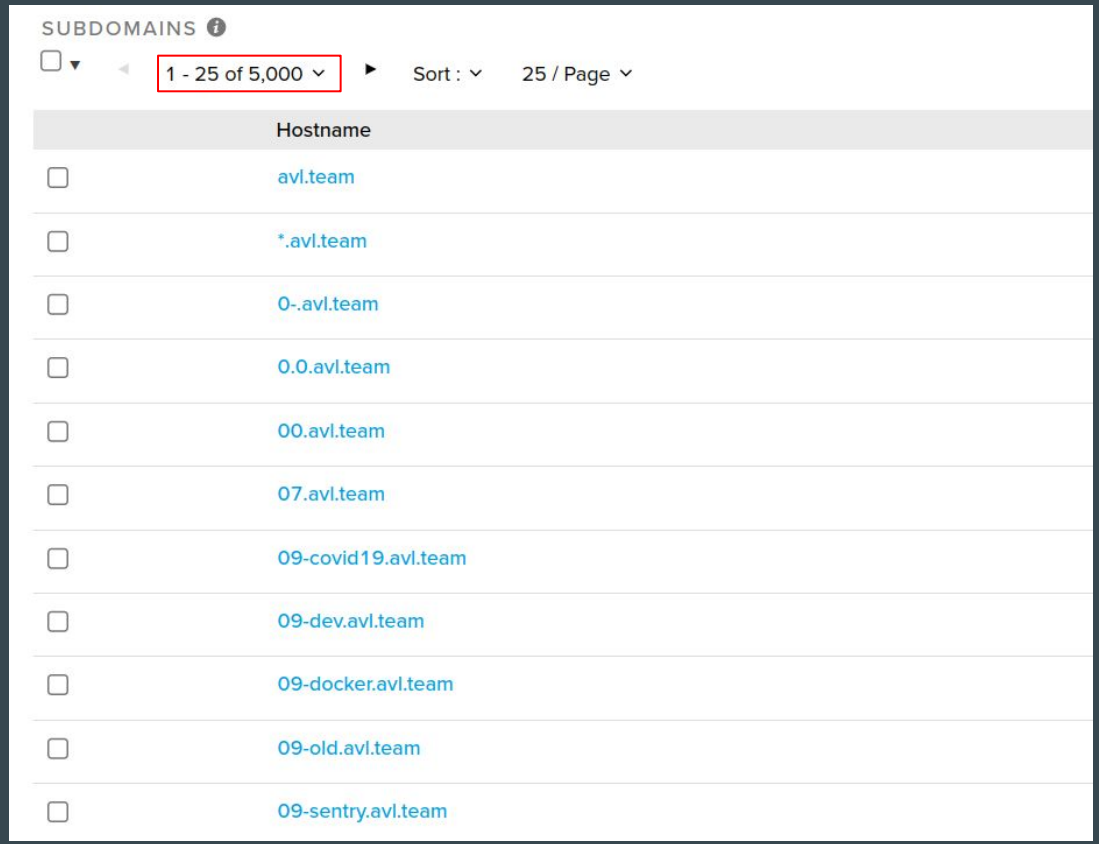
Website : avalanche.su

```
% TCI Whois Service. Terms of use:
% https://tcinet.ru/documents/whois_ru_rf.pdf (in Russian)
% https://tcinet.ru/documents/whois_su.pdf (in Russian)

domain:         AVALANCHE.SU
nserver:        dnsproxy1.fm.nic.ru.
nserver:        dnsproxy2.fm.nic.ru.
state:          REGISTERED, DELEGATED
org:            JSC INFORUS
phone:          +79857671667
e-mail:         info@avl.team
registrar:      RUCENTER-SU
created:        2022-04-28T20:55:04Z
paid-till:      2023-04-28T20:55:04Z
free-date:      2023-05-31
source:         TCI

Last updated on 2023-05-12T09:36:30Z
```

Passive DNS data



5000+ subdomains? What could have happened there?

Wildcard DNS record

```
$ host foobar.avl.team
foobar.avl.team has address 188.43.55.8
$ host fjsfndsknfkjfnkdf.avl.team
fjsfndsknfkjfnkdf.avl.team has address 188.43.55.8
```

Certificates

crt.sh Identity Search  Group by Issuer

Criteria	Type: Identity	Match: ILIKE	Search: 'avl.team'

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Common Name	Matching Identities	Issuer Name
9491149571	2023-05-26	2023-05-26	2023-08-24	lk.avl4.avl.team	lk.avl4.avl.team	C=US, O=Let's Encrypt, CN=R3
9489611490	2023-05-26	2023-05-26	2023-08-24	kk.avl4.avl.team	kk.avl4.avl.team	C=US, O=Let's Encrypt, CN=R3
9506085387	2023-05-24	2023-05-24	2023-08-22	demo.avl.team	demo.avl.team	C=US, O=Let's Encrypt, CN=R3
9475251273	2023-05-24	2023-05-24	2023-08-22	demo.avl.team	demo.avl.team	C=US, O=Let's Encrypt, CN=R3
9442165660	2023-05-18	2023-05-17	2023-08-15	conf.avl.team	conf.avl.team	C=US, O=Let's Encrypt, CN=R3
9417258645	2023-05-18	2023-05-17	2023-08-15	conf.avl.team	conf.avl.team	C=US, O=Let's Encrypt, CN=R3
9438307775	2023-05-17	2023-05-17	2023-08-15	sentry.sc.avl.team	sentry.sc.avl.team	C=US, O=Let's Encrypt, CN=R3
9414164948	2023-05-17	2023-05-17	2023-08-15	sentry.sc.avl.team	sentry.sc.avl.team	C=US, O=Let's Encrypt, CN=R3
9433439320	2023-05-17	2023-05-17	2023-08-15	pr.avl4.avl.team	pr.avl4.avl.team	C=US, O=Let's Encrypt, CN=R3
9433439068	2023-05-17	2023-05-17	2023-08-15	am.avl4.avl.team	am.avl4.avl.team	C=US, O=Let's Encrypt, CN=R3
9410968570	2023-05-17	2023-05-17	2023-08-15	pr.avl4.avl.team	pr.avl4.avl.team	C=US, O=Let's Encrypt, CN=R3
9409808131	2023-05-17	2023-05-17	2023-08-15	am.avl4.avl.team	am.avl4.avl.team	C=US, O=Let's Encrypt, CN=R3
9433438921	2023-05-17	2023-05-17	2023-08-15	gr.avl4.avl.team	gr.avl4.avl.team	C=US, O=Let's Encrypt, CN=R3
9409807786	2023-05-17	2023-05-17	2023-08-15	gr.avl4.avl.team	gr.avl4.avl.team	C=US, O=Let's Encrypt, CN=R3
9412443740	2023-05-15	2023-05-15	2023-08-13	test.sc.avl.team	test.sc.avl.team	C=US, O=Let's Encrypt, CN=R3
9395262049	2023-05-15	2023-05-15	2023-08-13	test.sc.avl.team	test.sc.avl.team	C=US, O=Let's Encrypt, CN=R3
9411743173	2023-05-15	2023-05-15	2023-08-13	globus.avl.team	globus.avl.team	C=US, O=Let's Encrypt, CN=R3
9396198009	2023-05-15	2023-05-15	2023-08-13	globus.avl.team	globus.avl.team	C=US, O=Let's Encrypt, CN=R3
9345838244	2023-05-08	2023-05-08	2023-08-06	vkui.sc.avl.team	vkui.sc.avl.team	C=US, O=Let's Encrypt, CN=R3
9339262045	2023-05-08	2023-05-08	2023-08-06	vkui.sc.avl.team	vkui.sc.avl.team	C=US, O=Let's Encrypt, CN=R3
9345838253	2023-05-08	2023-05-08	2023-08-06	vkapi.sc.avl.team	vkapi.sc.avl.team	C=US, O=Let's Encrypt, CN=R3
9339619647	2023-05-08	2023-05-08	2023-08-06	vkapi.sc.avl.team	vkapi.sc.avl.team	C=US, O=Let's Encrypt, CN=R3
9318320702	2023-05-05	2023-05-05	2023-08-03	rosatom.avl.team	rosatom.avl.team	C=US, O=Let's Encrypt, CN=R3
9314217986	2023-05-05	2023-05-05	2023-08-03	rosatom.avl.team	rosatom.avl.team	C=US, O=Let's Encrypt, CN=R3
9301929861	2023-05-03	2023-05-03	2023-08-01	vk.sc.avl.team	vk.sc.avl.team	C=US, O=Let's Encrypt, CN=R3
9294265018	2023-05-03	2023-05-03	2023-08-01	vk.sc.avl.team	vk.sc.avl.team	C=US, O=Let's Encrypt, CN=R3
9287232271	2023-05-01	2023-05-01	2023-07-30	tango.avl.team	tango.avl.team	C=US, O=Let's Encrypt, CN=R3
9280615443	2023-05-01	2023-05-01	2023-07-30	tango.avl.team	tango.avl.team	C=US, O=Let's Encrypt, CN=R3
9286573446	2023-05-01	2023-05-01	2023-07-30	api.sc.avl.team	api.sc.avl.team	C=US, O=Let's Encrypt, CN=R3
9280196851	2023-05-01	2023-05-01	2023-07-30	api.sc.avl.team	api.sc.avl.team	C=US, O=Let's Encrypt, CN=R3
9286571522	2023-05-01	2023-05-01	2023-07-30	auth.sc.avl.team	auth.sc.avl.team	C=US, O=Let's Encrypt, CN=R3
9286572224	2023-05-01	2023-05-01	2023-07-30	ui.sc.avl.team	ui.sc.avl.team	C=US, O=Let's Encrypt, CN=R3
9279843656	2023-05-01	2023-05-01	2023-07-30	ui.sc.avl.team	ui.sc.avl.team	C=US, O=Let's Encrypt, CN=R3
9279843691	2023-05-01	2023-05-01	2023-07-30	auth.sc.avl.team	auth.sc.avl.team	C=US, O=Let's Encrypt, CN=R3
9286571201	2023-05-01	2023-05-01	2023-07-30	kk.sc.avl.team	kk.sc.avl.team	C=US, O=Let's Encrypt, CN=R3
9279843324	2023-05-01	2023-05-01	2023-07-30	kk.sc.avl.team	kk.sc.avl.team	C=US, O=Let's Encrypt, CN=R3
9278078822	2023-04-30	2023-04-30	2023-07-29	jk.avl4.avl.team	jk.avl4.avl.team	C=US, O=Let's Encrypt, CN=R3
9269369069	2023-04-30	2023-04-30	2023-07-29	jk.avl4.avl.team	jk.avl4.avl.team	C=US, O=Let's Encrypt, CN=R3
9253967124	2023-04-26	2023-04-26	2023-07-25	panel.avl4.avl.team	panel.avl4.avl.team	C=US, O=Let's Encrypt, CN=R3
9253967136	2023-04-26	2023-04-26	2023-07-25	countrole.avl4.avl.team	countrole.avl4.avl.team	C=US, O=Let's Encrypt, CN=R3
9253967149	2023-04-26	2023-04-26	2023-07-25	auth.avl4.avl.team	auth.avl4.avl.team	C=US, O=Let's Encrypt, CN=R3
9239202832	2023-04-26	2023-04-26	2023-07-25	countrole.avl4.avl.team	countrole.avl4.avl.team	C=US, O=Let's Encrypt, CN=R3
9238721910	2023-04-26	2023-04-26	2023-07-25	auth.avl4.avl.team	auth.avl4.avl.team	C=US, O=Let's Encrypt, CN=R3
9238721917	2023-04-26	2023-04-26	2023-07-25	panel.avl4.avl.team	panel.avl4.avl.team	C=US, O=Let's Encrypt, CN=R3
9253965671	2023-04-26	2023-04-26	2023-07-25	login.avl4.avl.team	login.avl4.avl.team	C=US, O=Let's Encrypt, CN=R3
9238721837	2023-04-26	2023-04-26	2023-07-25	login.avl4.avl.team	login.avl4.avl.team	C=US, O=Let's Encrypt, CN=R3
9253967146	2023-04-26	2023-04-26	2023-07-25	main.avl4.avl.team	main.avl4.avl.team	C=US, O=Let's Encrypt, CN=R3
9238721506	2023-04-26	2023-04-26	2023-07-25	main.avl4.avl.team	main.avl4.avl.team	C=US, O=Let's Encrypt, CN=R3

```
$ python get_crtsh_subdomains.py avl.team
alertmanager.swarm.avl.team
am.avl4.avl.team
api.sc.avl.team
app.sc.avl.team
ast.avl.team
astra.avl.team
auth.avl4.avl.team
auth.avl.team
auth.sc.avl.team
auth.swarm.avl.team
bf.avl.team
bridge.avl.team
call.avl.team
conf2.avl.team
conf.avl.team
conf.sc.avl.team
count-role.avl4.avl.team
countrole.avl4.avl.team
countrole.avl.team
covid19.avl.team
covid.avl.team
ctrl.avl.team
dag.avl.team
dagestan.avl.team
deep.avl.team
demo.avl.team
```

Among these:

- dagestan.avl.team
- managua.avl.team
- rosatom.avl.team
- tuva.avl.team
- vietnam.avl.team
- severstal.avl.team

crt.sh Identity Search  Group by Issuer

Criteria	Type: Identity Match: ILIKE Search: 'managua.avl.team'

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Common Name	Matching Identities	Issuer Name
5494147655	2021-10-27	2021-10-27	2022-01-25	managua.avl.team	managua.avl.team	C=US, O=Let's Encrypt, CN=R3
5494148351	2021-10-27	2021-10-27	2022-01-25	managua.avl.team	managua.avl.team	C=US, O=Let's Encrypt, CN=R3
5122756610	2021-08-28	2021-08-28	2021-11-26	managua.avl.team	managua.avl.team	C=US, O=Let's Encrypt, CN=R3
5122757287	2021-08-28	2021-08-28	2021-11-26	managua.avl.team	managua.avl.team	C=US, O=Let's Encrypt, CN=R3
5064475104	2021-08-18	2021-08-18	2021-11-16	managua.avl.team	managua.avl.team	C=US, O=Let's Encrypt, CN=R3
5064471027	2021-08-18	2021-08-18	2021-11-16	managua.avl.team	managua.avl.team	C=US, O=Let's Encrypt, CN=R3
4553931619	2021-05-19	2021-05-19	2021-08-17	managua.avl.team	managua.avl.team	C=US, O=Let's Encrypt, CN=R3
4553931824	2021-05-19	2021-05-19	2021-08-17	managua.avl.team	managua.avl.team	C=US, O=Let's Encrypt, CN=R3
4519339604	2021-05-13	2021-05-13	2021-08-11	managua.avl.team	managua.avl.team	C=US, O=Let's Encrypt, CN=R3
4519336324	2021-05-13	2021-05-13	2021-08-11	managua.avl.team	managua.avl.team	C=US, O=Let's Encrypt, CN=R3

4 - Pegasus

9. Unravelling the Pegasus attack infrastructure over the years

The set of domain names, servers and infrastructure used to deliver and collect data from NSO Group's Pegasus spyware has evolved several times since first publicly disclosed by Citizen Lab in 2016.

In August 2018, Amnesty International published a report ***"Amnesty International Among Targets of NSO-powered Campaign"*** which described the targeting of an Amnesty International staff member and a Saudi human rights defender. In this report, Amnesty International presented an excerpt of more than 600 domain names tied to NSO Group's attack infrastructure. Amnesty International published the **full list of domains** in October 2018. In this report, we refer to these domains as Pegasus network **Version 3 (V3)**.

The **Version 3** infrastructure used a network of VPS's and dedicated servers. Each Pegasus Installation server or Command-and-Control (C&C) server hosted a web server on port 443 with a unique domain and TLS certificate. These edge servers would then proxy connections through a chain of servers, referred to by NSO Group as the **"Pegasus Anonymizing Transmission Network" (PATN).**

It was possible to create a pair of fingerprints for the distinctive set of TLS cipher suites supported by these servers. The fingerprint technique is conceptually similar to the **JA3S fingerprint technique published by Salesforce in 2019**. With that fingerprint, Amnesty International's Security Lab performed Internet-wide scans to identify Pegasus Installation/infection and C&C servers active in the summer of 2018.

NSO Group made critical operational security mistakes when setting up their Version 3 infrastructure. Two domains of the previous Version 2 network were reused in their Version 3 network. These two Version 2 domains, **pine-sales[.]com** and **ecommerce-ads[.]org** had previously been identified by Citizen Lab. These mistakes allowed Amnesty International to link the attempted attack on our colleague to NSO Group's Pegasus product. These links were independently **confirmed by Citizen Lab in a 2018 report**.

NSO Group rapidly shutdown many of their Version 3 servers shortly after the Amnesty International and Citizen Lab's publications on 1 August 2018.

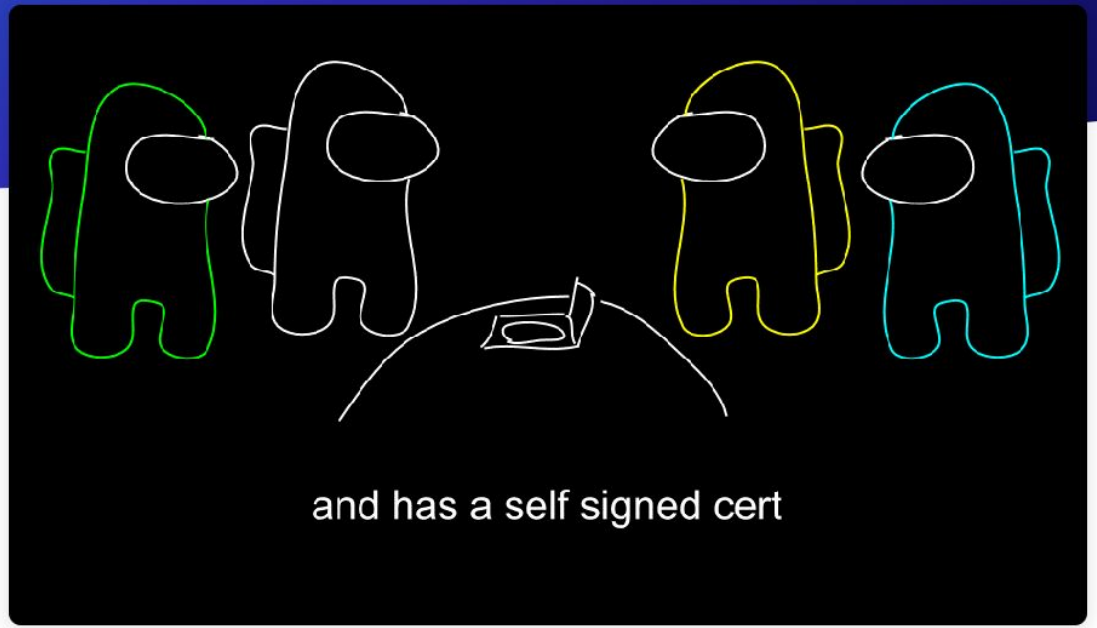
JARM

https://engineering.salesforce.com/easily-identify-malicious-servers-on-the-internet-with-jarm-e095edac525a/

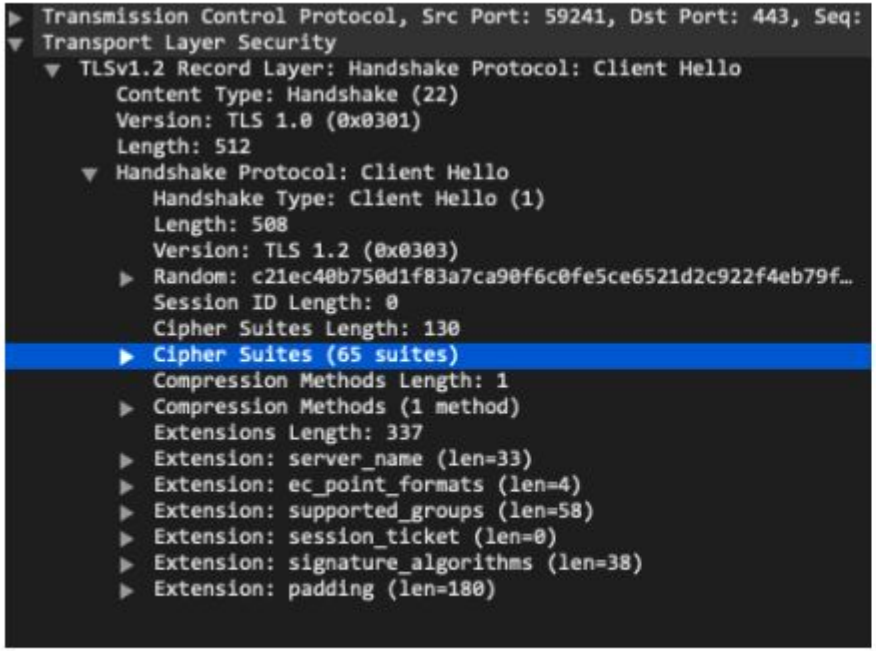
OPEN SOURCE

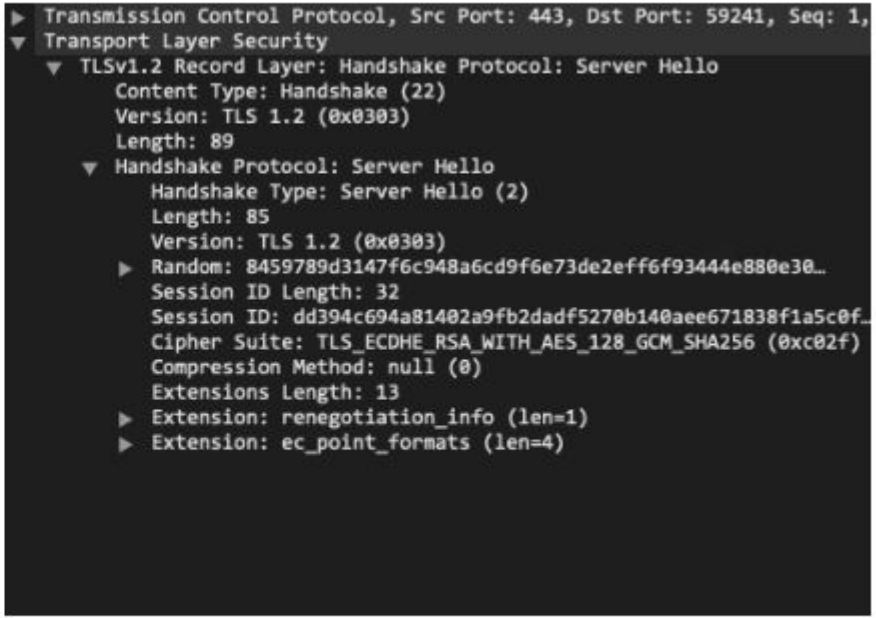
Easily Identify Malicious Servers on the Internet with JARM

John Althouse
Nov 17 - 10 min read



JARM





Example TLS Client Hello packet (left) and Server Hello response (right)

In Censys

443 / HTTP TCP

Observed May 29, 2023 at 3:19am UTC

VIEW ALL DATA GO

Software

nginx

Details

https://34.122.151.197

Request	GET /
Protocol	HTTP/1.1
Status Code	404
Status Reason	Not Found
Body Hash	sha1:5ea71b502e8ae7ce7c26d59626aa9bfd9bc8f000
HTML Title	Site Not Configured | 404 Not Found
Response Body	EXPAND

TLS

Fingerprint

JARM	2ad2ad0002ad2ad00042d42d0000005d86ccb1a0567e012264097a0315d7a7
JA3S	15af977ce25de452b96affa2addb1036

Handshake

Version Selected	TLSv1_3
Cipher Selected	TLS_AES_256_GCM_SHA384

Leaf Certificate

06a8d0764f1578615e732006cb7a087bab7084c80046a573cf1471dfe6bcbc3f

CN=*.wpengine.com

C=US, O=DigiCert\, Inc., CN=RapidSSL Global TLS RSA4096 SHA256 2022 CA1

Additional tips from 2018 report

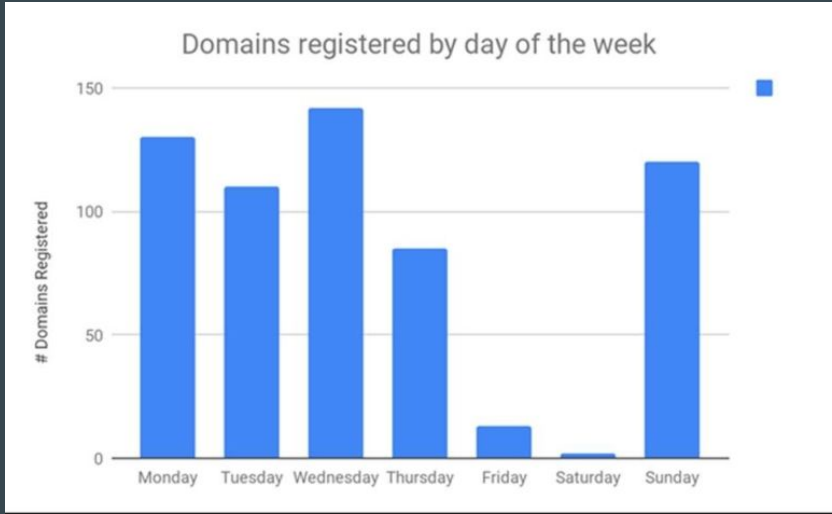
While speculative, we have also performed an analysis of the registration dates and times of the hundreds of PATN domains we identified. This analysis is based on publicly available data that domain registrars collect from their customers when selling any new domain name. This information (which can be accessed through any so-called **WHOIS lookup** service) can look something like the following:

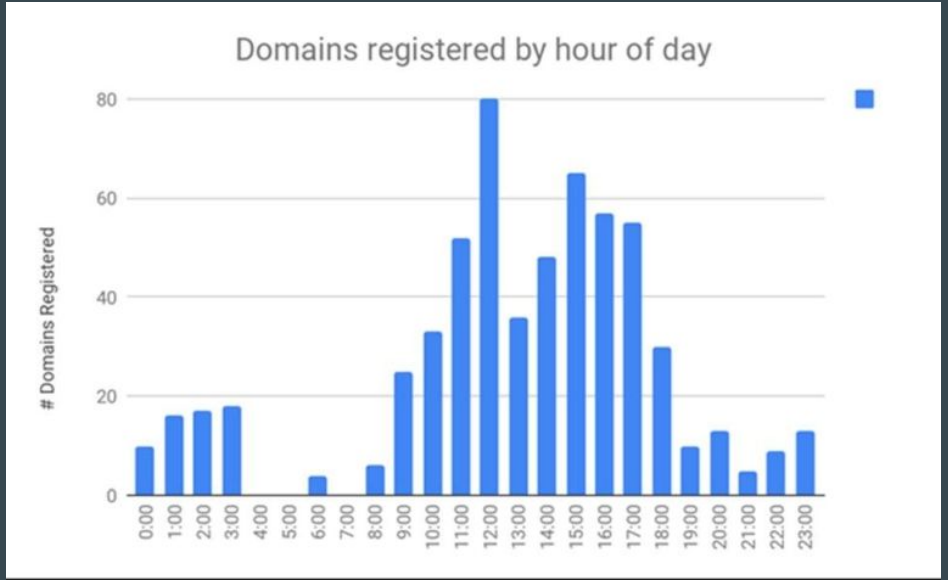
Raw WHOIS Record

```
Domain Name: AKHBAR-ARABIA.COM
Registry Domain ID: 2166759160_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.pananames.com
Registrar URL: http://www.pananames.com
Updated Date: 2018-01-05T16:16:02Z
Creation Date: 2017-09-24T09:26:26Z
Registrar Registration Expiration Date: 2018-09-24T09:26:26Z
Registrar: URL SOLUTIONS INC.
Registrar IANA ID: 1449
Registrar Abuse Contact Email: abuse@pananames.com
Registrar Abuse Contact Phone: +507.8339556
Reseller:
Domain Status: clientTransferProhibited -- https://icann.org
/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Private Whois
Registrant Organization: GLOBAL DOMAIN PRIVACY SERVICES INC
Registrant Street: Tower Financial Center Flr 35, 50th St y E. Mendez St
Registrant City: Panama
Registrant State/Province: NA
Registrant Postal Code: NA
Registrant Country: PA
Registrant Phone: +507.8365260
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: akhbar-arabia.com.t4tgjz771xdi@domains-anonymizer.com
```

From: https://www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/

Additional tips from 2018 report





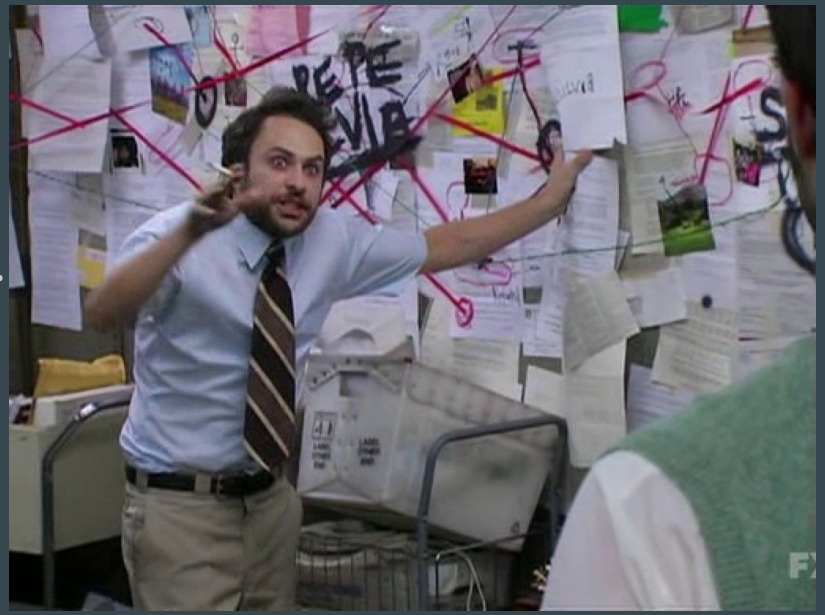
Some General Advices

Starting an investigation

- What do you know to start?
- What are you looking for?
- What would be the ideal case? (Help making trade-of time/interest)

Doing an investigation

- Take notes of everything
- Map things : graphs, lists, timelines...
- Think about TTP
- It’s okay to be lost



Finishing an investigation

- Take distance / time out of your research
- Make your conclusions
- Assess the hypothesis leading to your conclusion, are they all strong?
- Ask external people / tech export to review your conclusions

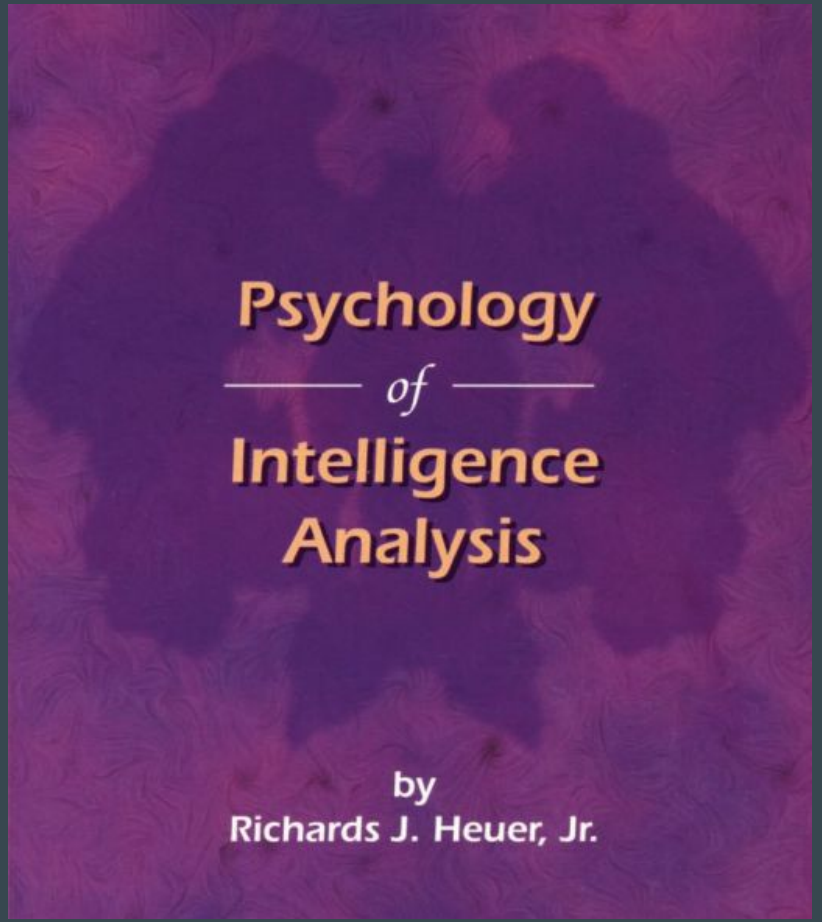
Analysis of competing hypotheses

Chapter 8

Analysis of Competing Hypotheses

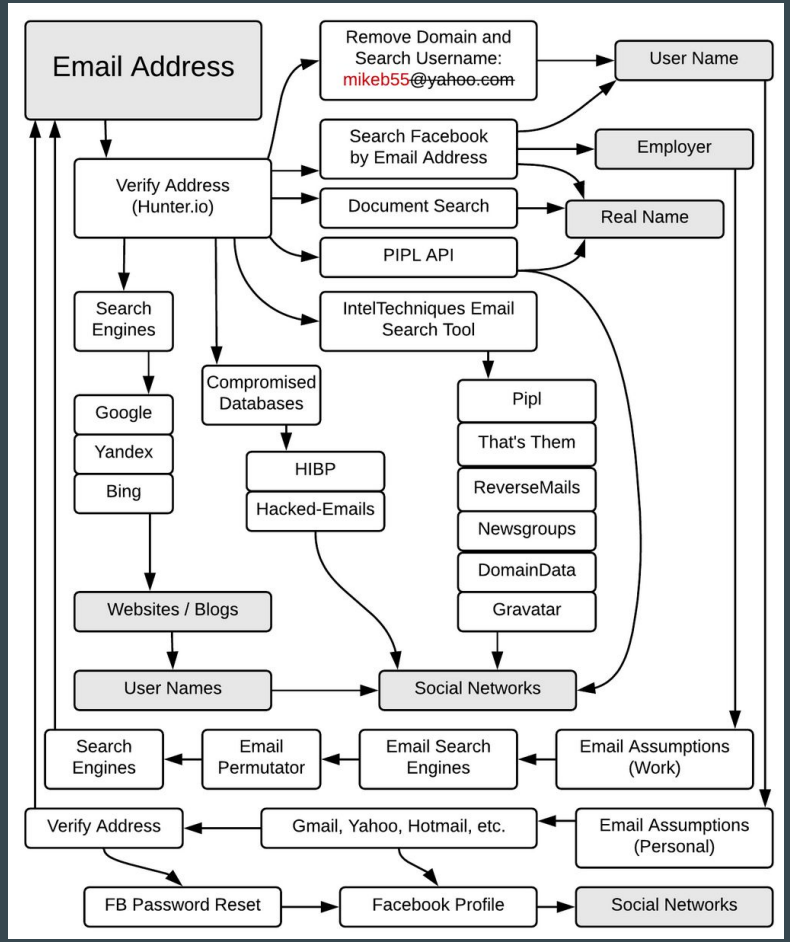
Analysis of competing hypotheses, sometimes abbreviated ACH, is a tool to aid judgment on important issues requiring careful weighing of alternative explanations or conclusions. It helps an analyst overcome, or at least minimize, some of the cognitive limitations that make prescient intelligence analysis so difficult to achieve.

ACH is an eight-step procedure grounded in basic insights from cognitive psychology, decision analysis, and the scientific method. It is a surprisingly effective, proven process that helps analysts avoid common analytic pitfalls. Because of its thoroughness, it is particularly appropriate for controversial issues when analysts want to leave an audit trail to show what they considered and how they arrived at their judgment.[85]



Getting better at investigations

- Practice, practice, practice
- Learn to see what's normal, to find weird
- Take notes on tips and tricks
- Develop your workflows



https://inteltechniques.com/osintbook/

Questions?

For Wednesday

Pick the website of the media you are working for. Try to gather as much evidence as possible about it :

- DNS/Passive DNS
- Whois / Historical Whois
- Certificates
- Technology used
- Anything else

Prepare a short summary to share with the group