
NARCOS, COUNTERFEITERS & SCAMMERS
An Approach to
Visualize Illegal Markets using pDNS
FARSIGHT
SECURITY
CybelAngel

Introduction

Andrew Lewman

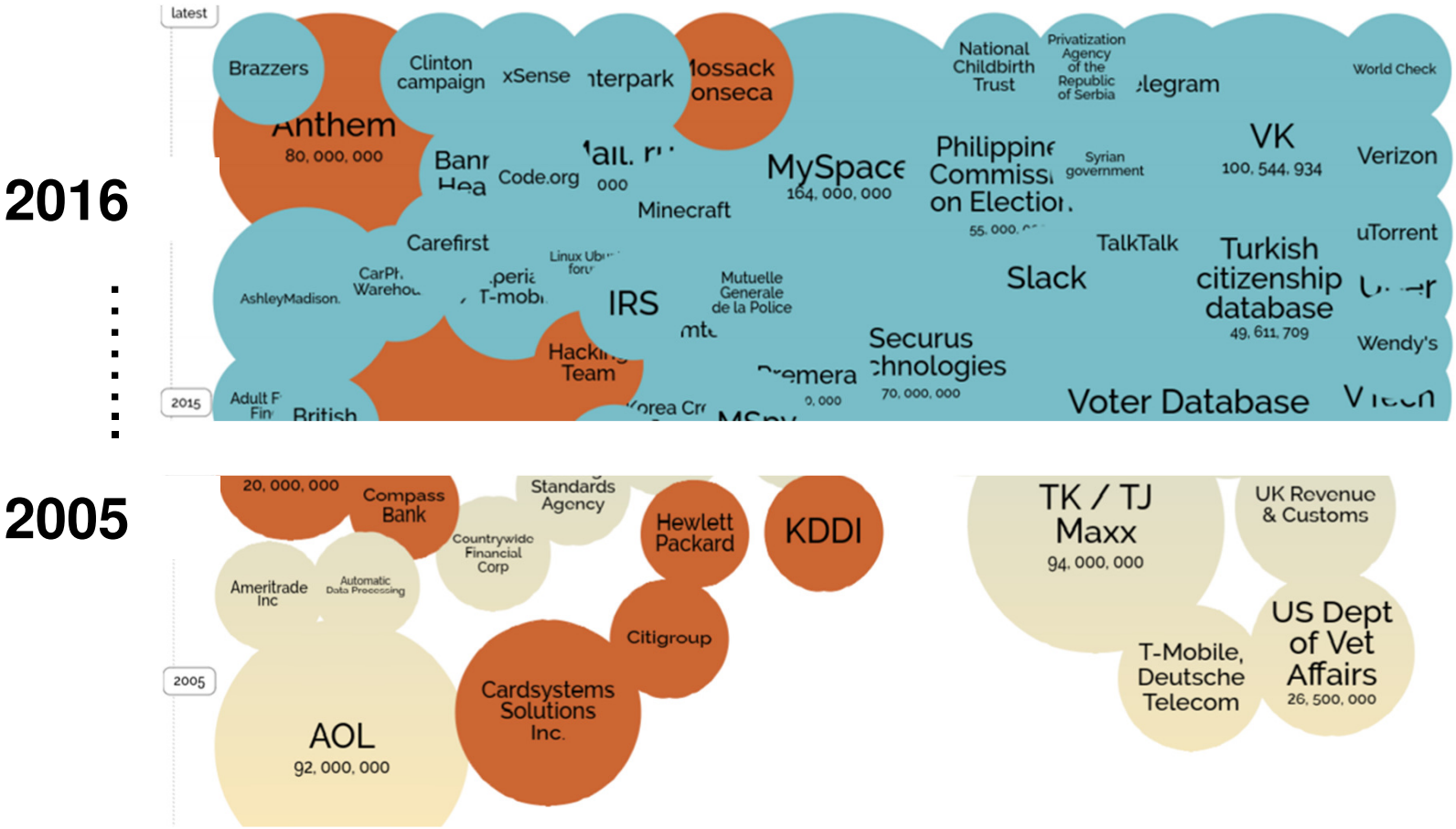
- Farsight Security CRO
- Renown cybersecurity and privacy expert
- Tor Project, CEO

Stevan Keraudy

- CybelAngel CTO
- MSc in Machine Learning and Data Mining

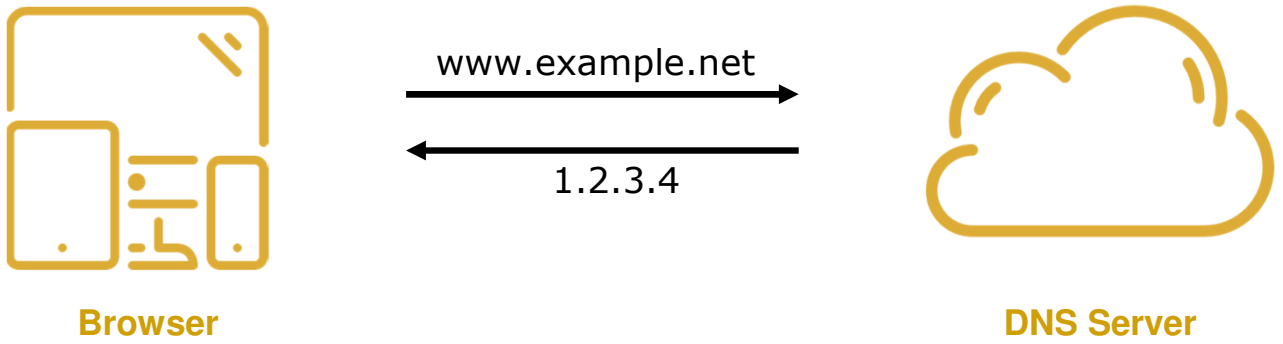
FARSIGHT SECURITY CybelAngel

Threat Landscape is vast and growing



FORSIGHT SECURITY CybelAngel

In the beginning



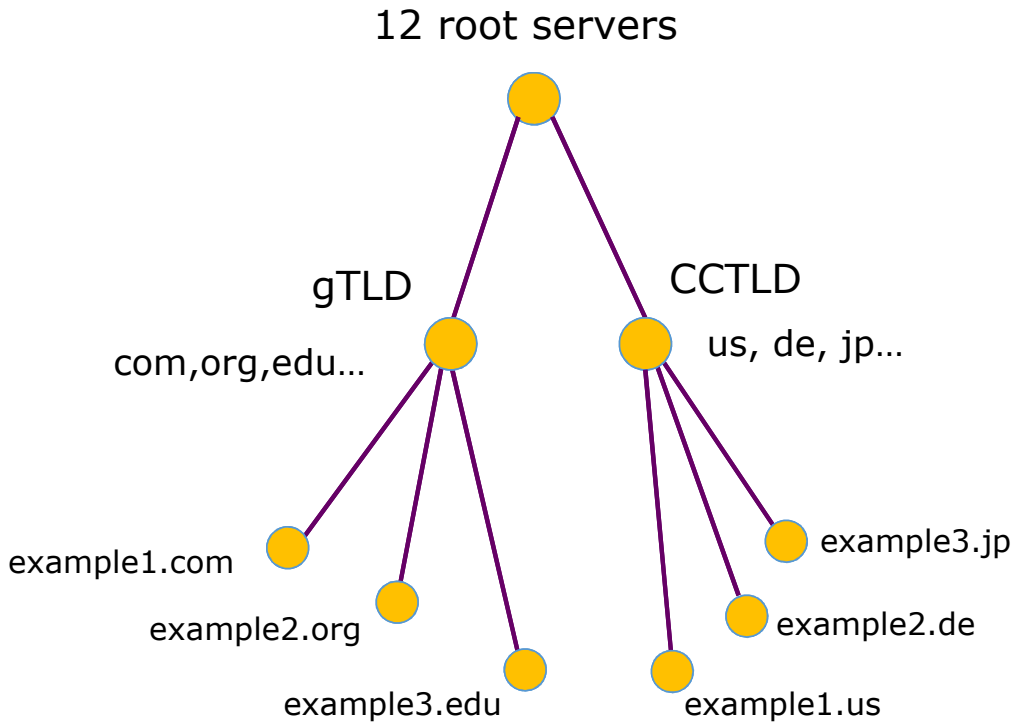
Nearly every online transaction – good or bad -- begins with a DNS lookup

IPs or domain names provide a starting point and initial clue to the crime

Classical approach

Zone File Analysis

Lots of Limitations



FARSIGHT SECURITY CybelAngel

Pulling back the curtains

Not interested in long-lived domain names

Domains are “free” & short-lived assets; using 100s/day

AND…there's free domain/free subdomain/free domain name redirection services out there...

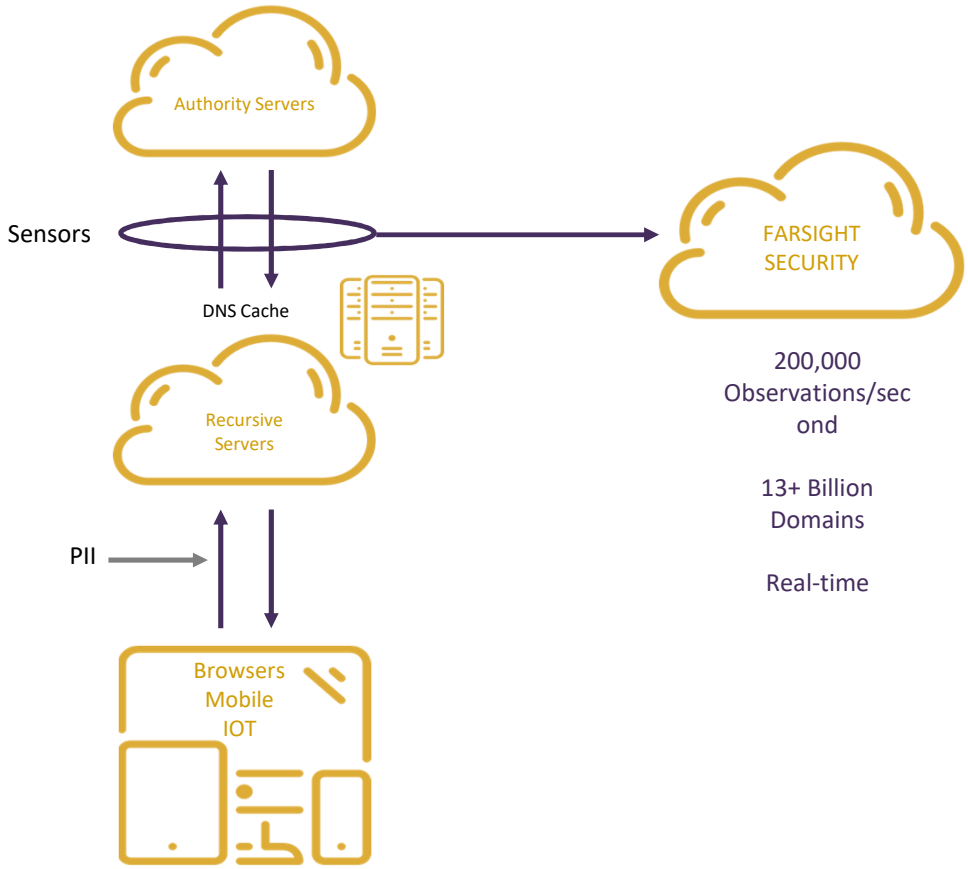
What is Passive DNS

Observations of global Domain to IP address transaction flows

Visibility into the evolving configurations of the DNS

Collection of query-answer pairs as detected on recursive name servers –
NO Personally Identifiable Information(PII)

Is most valuable when collected and published in real-time



FARSIGHT SECURITY CybelAngel

Whis is pDNS useful ?

Discover associations among threat actors in real-time

Accelerate incident research

Perform risk assessment of domain names & IPs

Uncover all domains using the same name servers

Reveal IPs used to conceal activity to avoid takedowns

Conduct third-party audits of DNS configurations

FORSIGHT SECURITY CybelAngel

Passive DNS: unmatched visibility

Farsight Security partner, CybelAngel, will illustrate how passive DNS is used to expose narcos, counterfeiters and scammers

FARSIGHT SECURITY

CybelAngel

Methodology

A process to convert a passive DNS data feed into a human-readable visualization the threats.

FORESIGHT SECURITY CybelAngel

Technical stack

redis

available at redis.io

Doing magic with Redis

- Key-value store for multi-process-communication

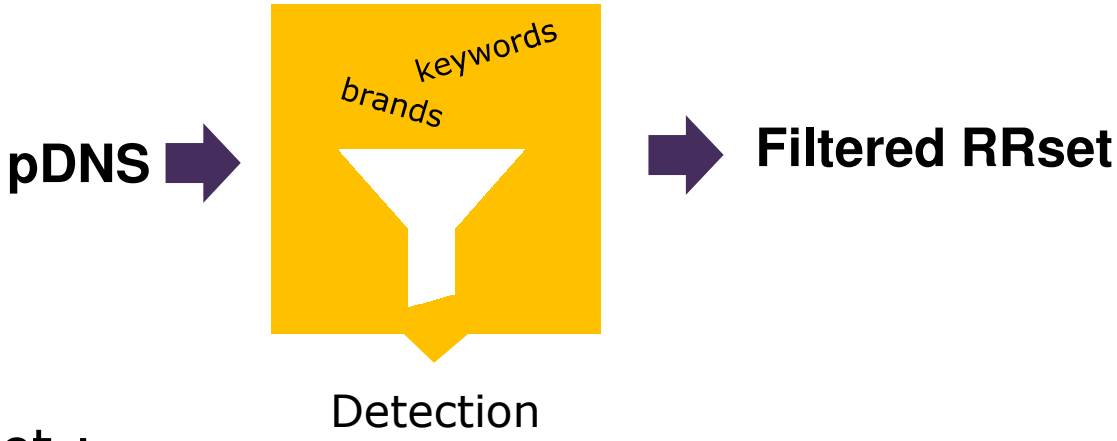
- DIY message broker and load balancer

- Real-time events and statistics

FORESIGHT SECURITY CybelAngel

Passive DNS

5,000 RRset/s



Example of a Resource Record set :

{count: 1, time_first: 1398714180, time_last: 1398714182, rrname: "**cybelangel.com**.",
rrtype: "A", rdata: ["91.xxx.xxx.xxx"]}

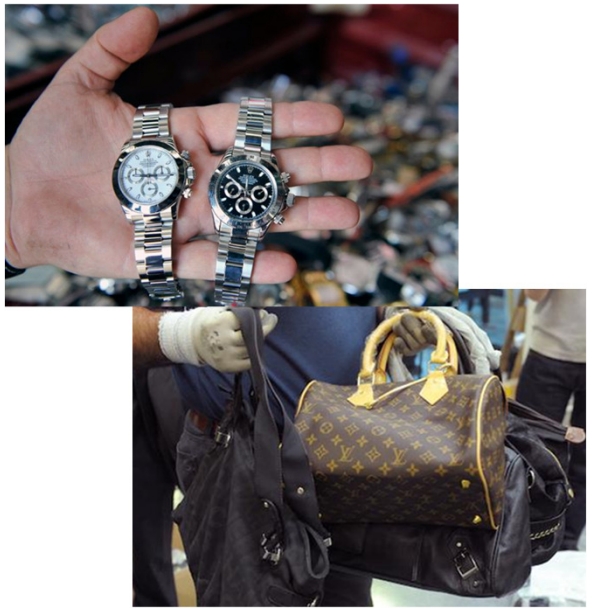
{count: 1, time_first: 1349432137, time_last: 1349432143, rrname: "**cybelangel.com**.",
rrtype: "A", rdata: ["94.xxx.xxx.xxx"]}

FORSIGHT SECURITY CybelAngel

Brand-specific filtering

Narcos

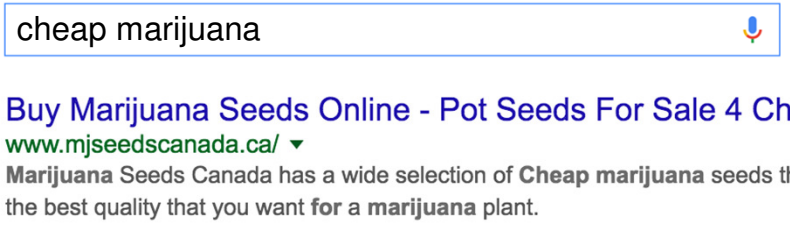
Counterfeiters

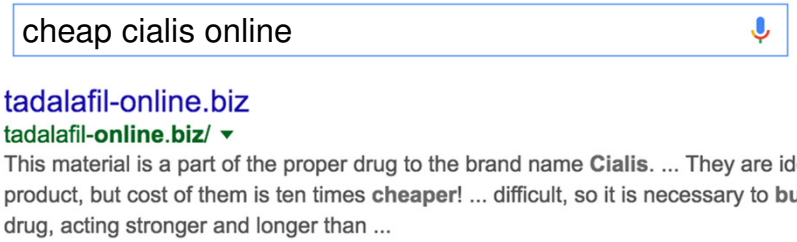


Scammers

FORESIGHT SECURITY CybelAngel

Generic keyword filtering





FORSIGHT SECURITY CybelAngel

Filtering Passive DNS

200µs to match a RRset

Perfect Matching (quick & easy)

secure.cybelangelcom.cyberthreatintelfeed.biz

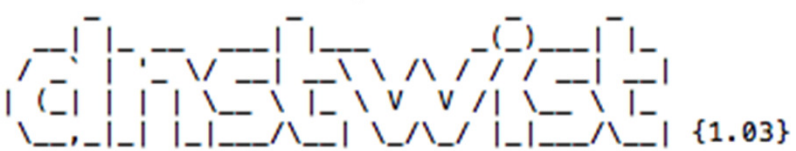
Fuzzy matching (time-consuming & difficult)

sybelangel.org.me cybellangel.ir mycybe1angel.ua

FARSIGHT SECURITY CybelAngel

Solving the fuzzy matching problem

Pre-generate DNS variations and run a perfect match



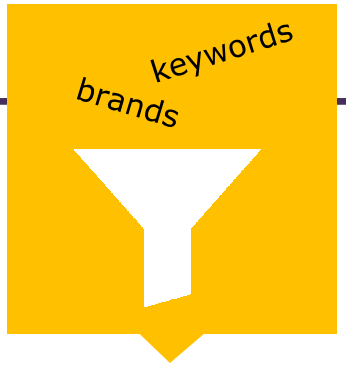
elceef/dnstwist

Awesome project by

DNSTwists of cybelangel.com

Addition	cybelangell.com
Bitsquatting	cybelangen.com
Homoglyph	cybe1angel.com
Insertion	cybelangwel.com
Omission	cybelanel.com
Repetition	cybellangel.com
Replacement	cybelangrl.com
Subdomain	cy.belangel.com
Transposition	cybelanegl.com
Various	wwwcybelangel.com
Various	cybelangelcom.com

5,000 RRset/s



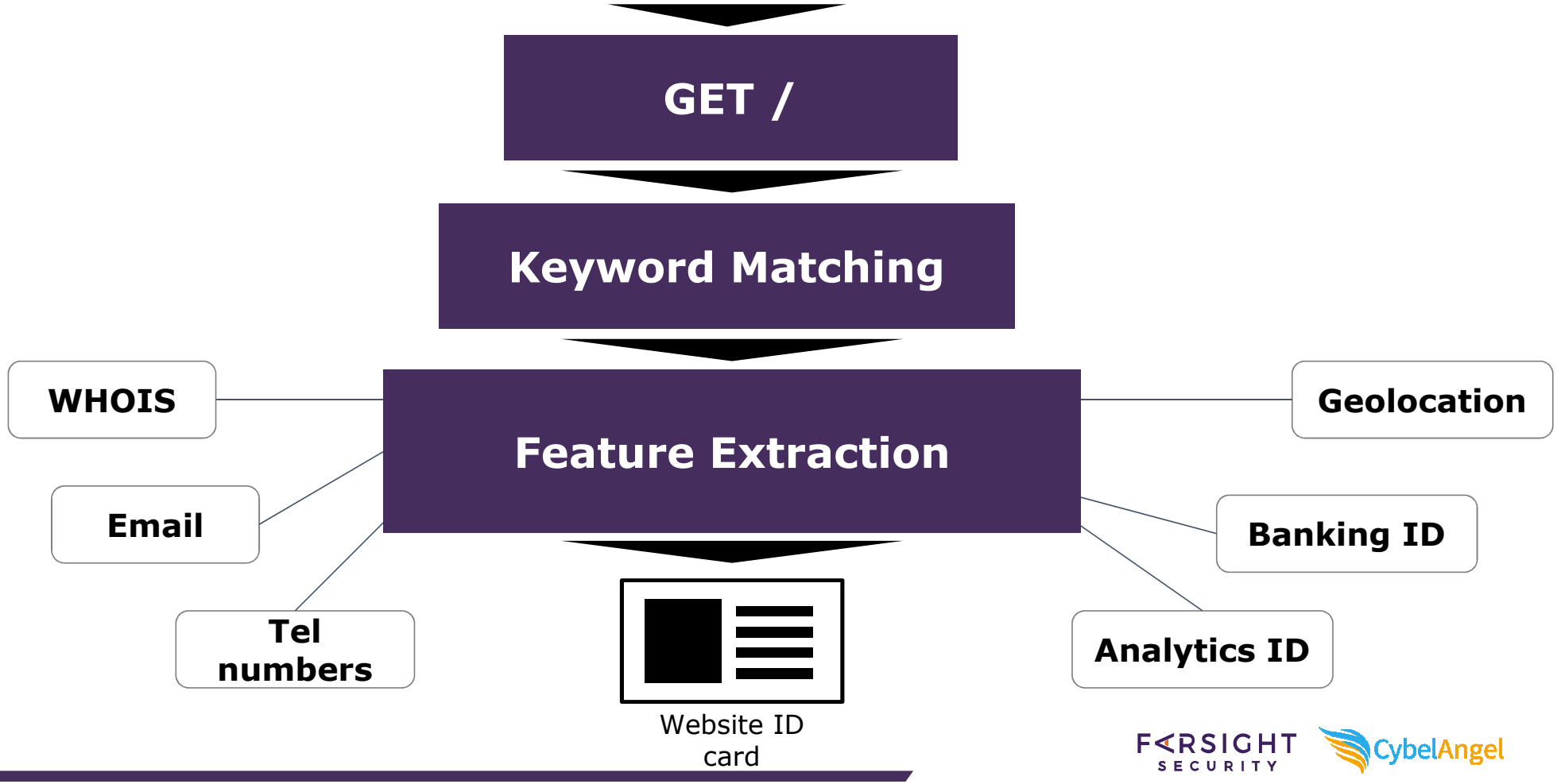
Detection

50 filtered RRsets/s
(99.0% reduction)

FORESIGHT SECURITY CybelAngel

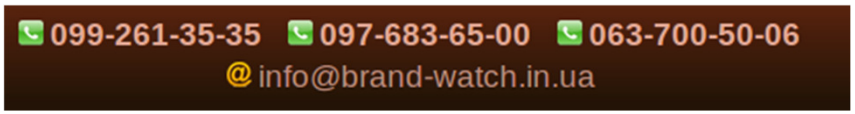
In-depth analysis pipe

50 filtered RRset/s (type A)



Feature extraction

```
        <!-- AddThis Button BEGIN -->
<div class="addthis_toolbox addthis_default_style addthis_32x32_style"><a class="addthis_button_preferred_1"></a> <a cl
<script src="http://s7.addthis.com/js/300/addthis_widget.js#pubid=xa-50c89e5741eda95a" type="text/javascript"></script>
<!-- AddThis Button END -->      </div>
```

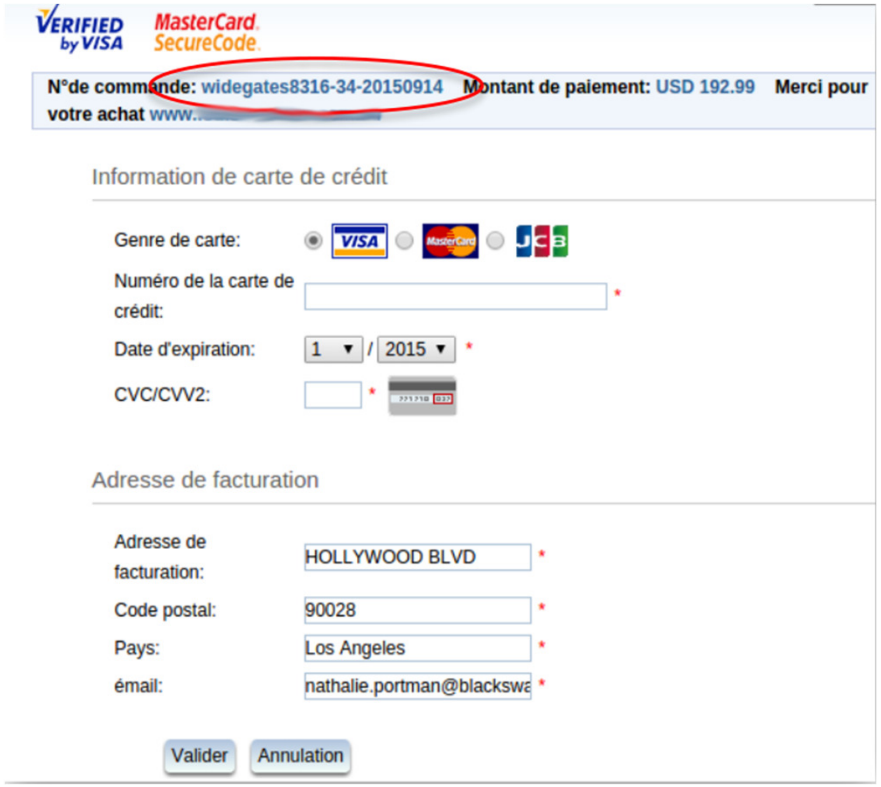



```
        <!-- BEGIN GOOGLE ANALYTICS CODE -->
        <script type="text/javascript">
        //<![CDATA[
            var _gaq = _gaq || [];

_gaq.push(['_setAccount', 'UA-67228409-1']);

_gaq.push(['_trackPageview']);

            (function() {
                var ga = document.createElement('script');
                ga.src = ('https:' == document.location.prc
                var s = document.getElementsByTagName('scri
            })();

        //]]>
        </script>
        <!-- END GOOGLE ANALYTICS CODE -->
```

```
The Registry database contains ONLY .COM, .NET, .EDU domains
Registrars.
Domain Name: WRISTWATCHSPOT.COM
Registry Domain ID: 1946543850_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.name.com
Registrar URL: http://www.name.com
Updated Date: 2016-06-21T17:00:42Z
Creation Date: 2015-07-13T05:41:49Z
Registrar Registration Expiration Date: 2017-07-13T05:41:49Z
Registrar: Name.com, Inc.
Registrar IANA ID: 625
Reseller:
Domain Status: clientTransferProhibited
Registry Registrant ID:
Registrant Name: Jason Lee
Registrant Organization:
Registrant Street: Mosan Juru No.204
Registrant City: Nanjing
Registrant State/Province: Jiangsu
Registrant Postal Code: 541875
Registrant Country: CN
Registrant Phone: +86.02047518754
Registrant Email: karrenservice@hotmail.com
Registry Admin ID:
```

FORESIGHT SECURITY CybelAngel

Feature extraction



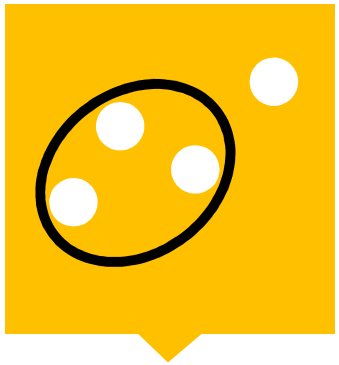

```
<input type="hidden" name="BrowserDate" id="BrowserDate" value="201591414715">
<input type="hidden" name="BrowserDateTimezone" id="BrowserDateTimezone" value
<input type="hidden" name="BrowserUserAgent" id="BrowserUserAgent" value="Mozi
<input type="hidden" name="BrowserName" id="BrowserName" value="Chrome">
<input type="hidden" name="BrowserLanguage" id="BrowserLanguage" value="fr">
<input type="hidden" name="BrowserSystemLanguage" id="BrowserSystemLanguage" v
<input type="hidden" name="BrowserSystem" id="BrowserSystem" value="Linux">
<input type="hidden" name="CardCopy" id="CardCopy">
<input type="hidden" name="Resolution" id="Resolution" value="1920x1080">
<input type="hidden" id="CTime" name="CTime" value="Mon Sep 14 2015 14:07:13 G
<input type="hidden" name="Cookie" value="3r24nte77ra6up6vua2eohc443">
<input type="hidden" value="01" name="TxnType">
<input type="hidden" value="V5.0" name="IVersion">
<input type="hidden" value="widegates8316" name="AcctNo">
<input type="hidden" value="widegates8316-34-20150914" name="OrderID">
<input type="hidden" value="840" name="CurrCode">
<input type="hidden" value="19299" name="Amount">
<input type="hidden" value="EEBCWd1cbWfZQ2mp9wCM2w==" name="HashValue">
<input type="hidden" value="www.[redacted]" name="RetURL">
<input type="hidden" value="HOLLYWOOD BLVD" name="BAddress">
<input type="hidden" value="nathalie.portman@blackswan.com" name="Email">
<input type="hidden" value="Los Angeles" name="BCity">
<input type="hidden" value="90028" name="PostCode">
<input type="hidden" value name="Telephone">
<input type="hidden" value="United States" name="Bcountry">
<input type="hidden" value="Nathalie Portman" name="CName">
<input type="hidden" value="Lockit,#;" name="PName">
```

FORSIGHT SECURITY CybelAngel

Clustering – Why ?

Problem

Taking down 1000s of websites one-by-one is costly and inefficient



Clustering

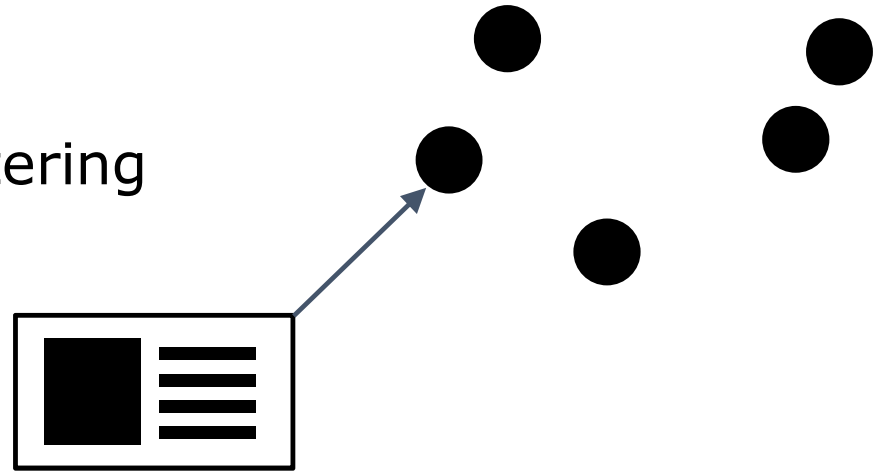
Solution

- Clustering websites belonging to the same actor
- Ranking them using traffic estimation

FORESIGHT SECURITY CybelAngel

Clustering – How?

Use the extracted features for clustering



Hypothesis :

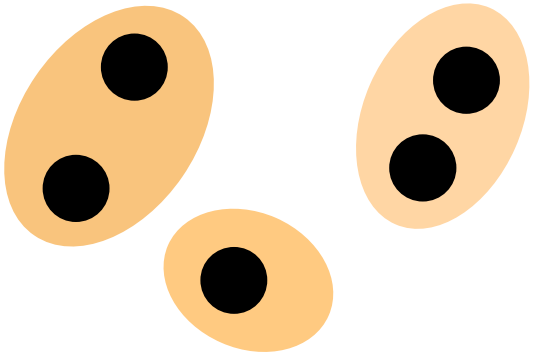
The more features two website share, the more likely they belong to the same actor.

This looks like an **Unsupervised Machine Learning** problem.

Clustering – The unsupervised learning approach

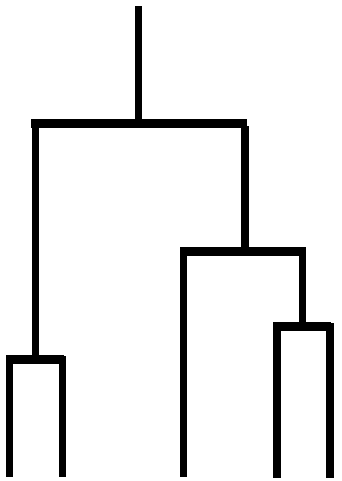
We tried several algorithms :

- K-Means
- Hierarchical Clustering



Problems:

- Unknown number of clusters
- Definition of a distance



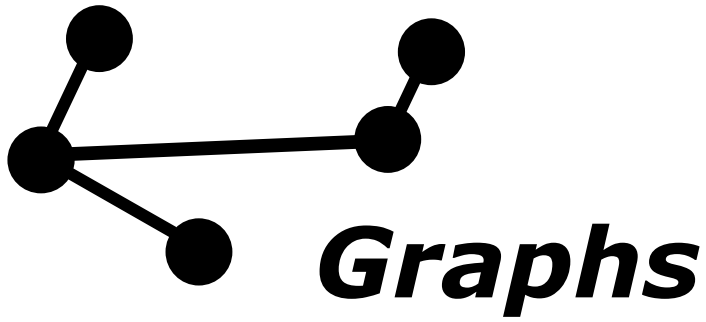
→ Find a **representation** that is :

- Human Readable
- Machine Readable

FORESIGHT SECURITY CybelAngel

Clustering – The graph approach

We tried another approach :

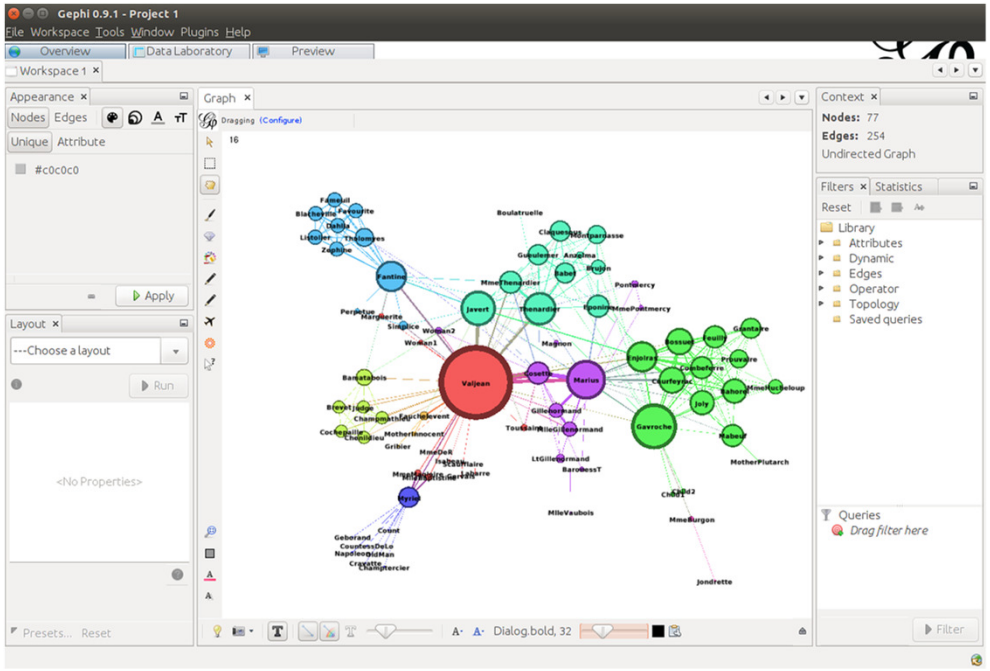


Advantages

- No vectorization needed
- A natural representation of linked websites
- Human readable visualization

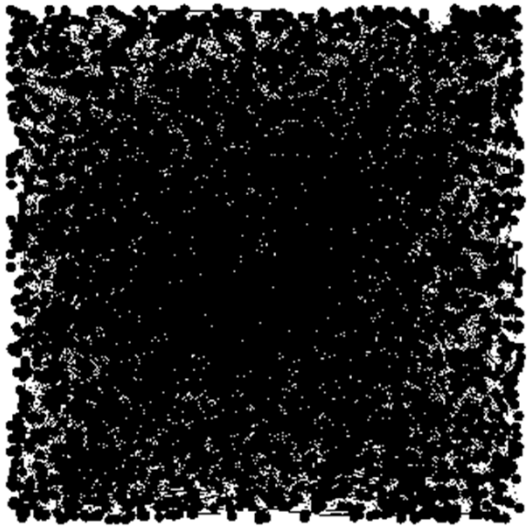
Gephi

Gephi is a visualization and exploration software for graphs.
It is open source (GPLv3) and available at [gephi.org.](gephi.org)

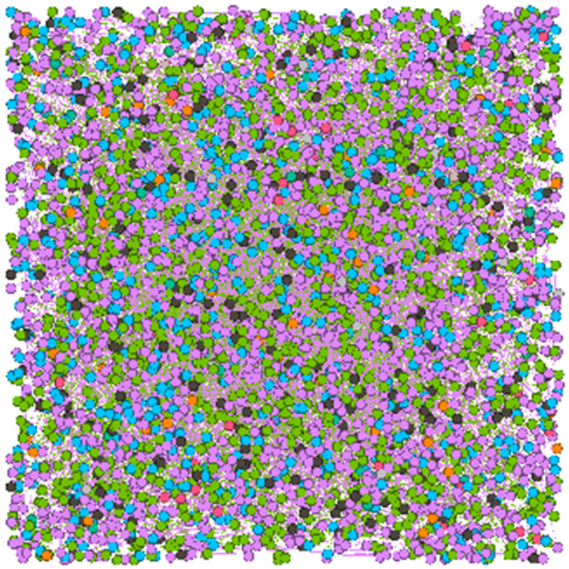


FORESIGHT SECURITY CybelAngel

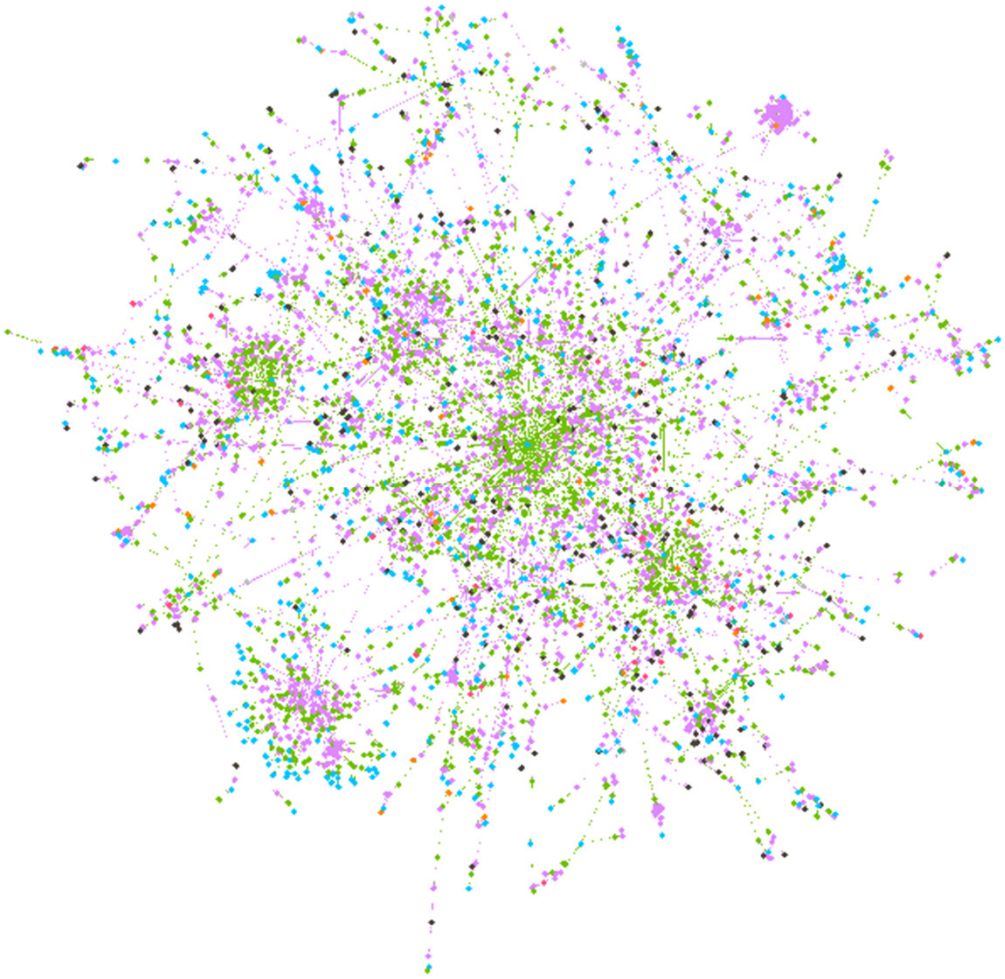
Network spatialization with Force Atlas 2



Network spatialization with Force Atlas 2

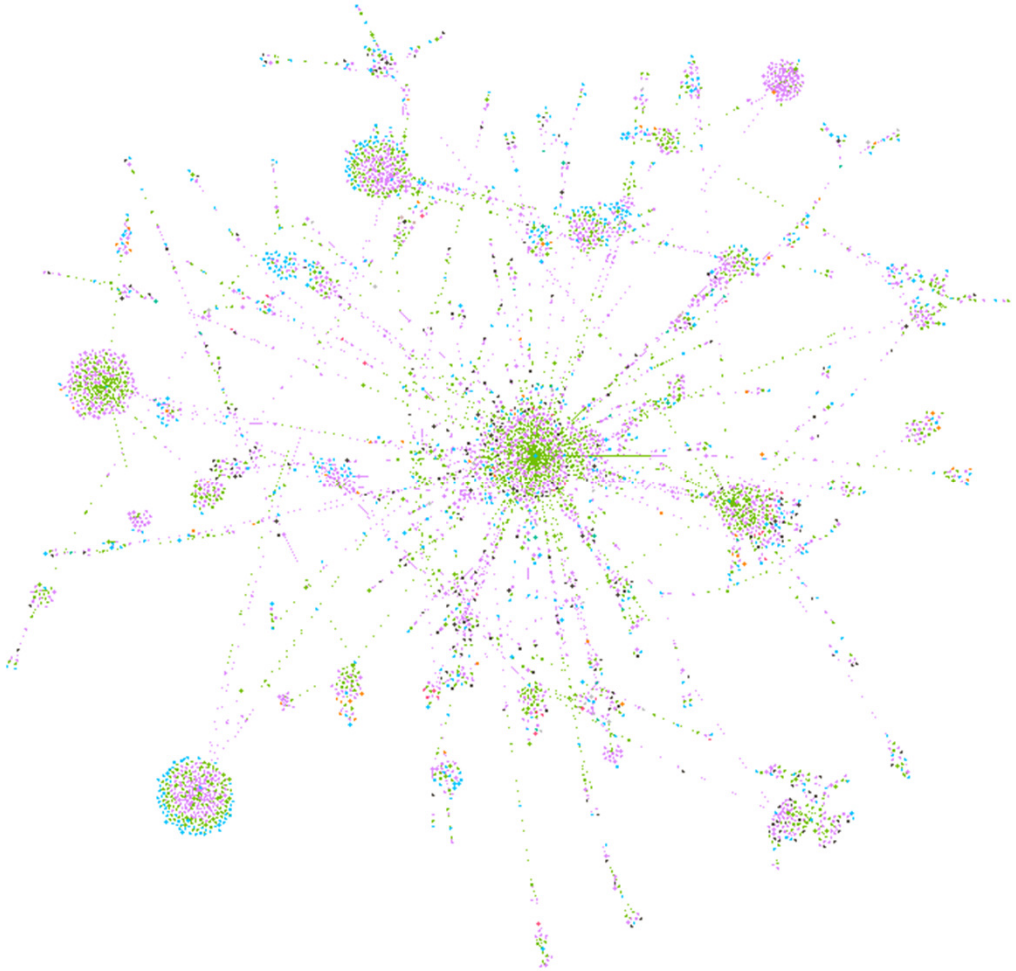


Network spatialization with Force Atlas 2



RSIGHT SECURITY CybelAngel

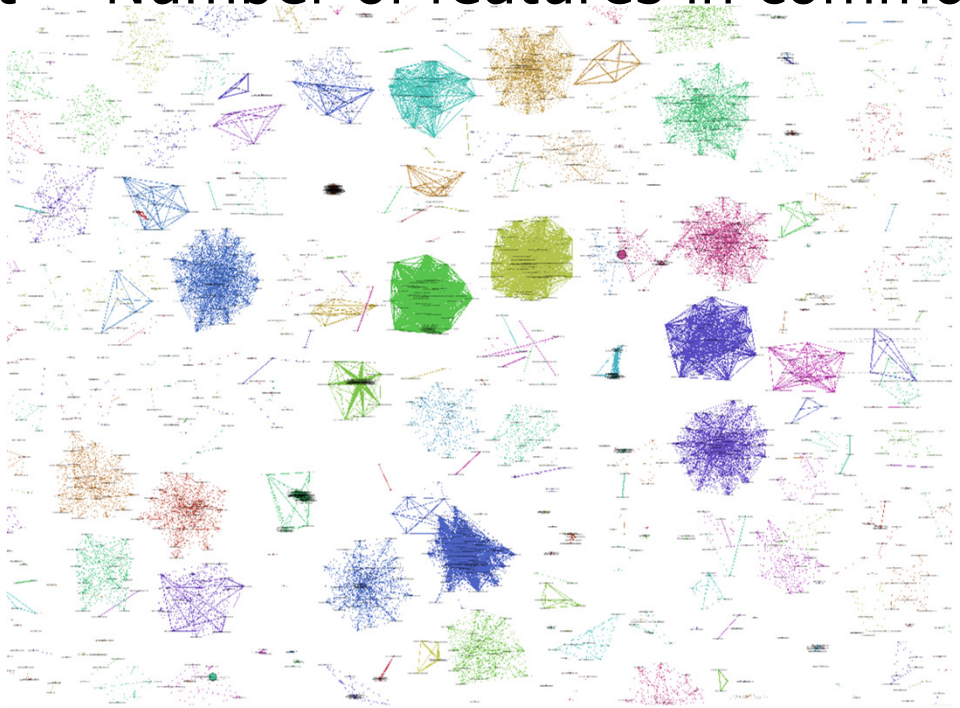
Network spatialization with Force Atlas 2



FORESIGHT SECURITY CybelAngel

Naive graph construction

- Node = website
- Edge = common feature shared by 2 websites
- Edge weight = Number of features in common



FORESIGHT SECURITY CybelAngel

Naive graph construction

Pros

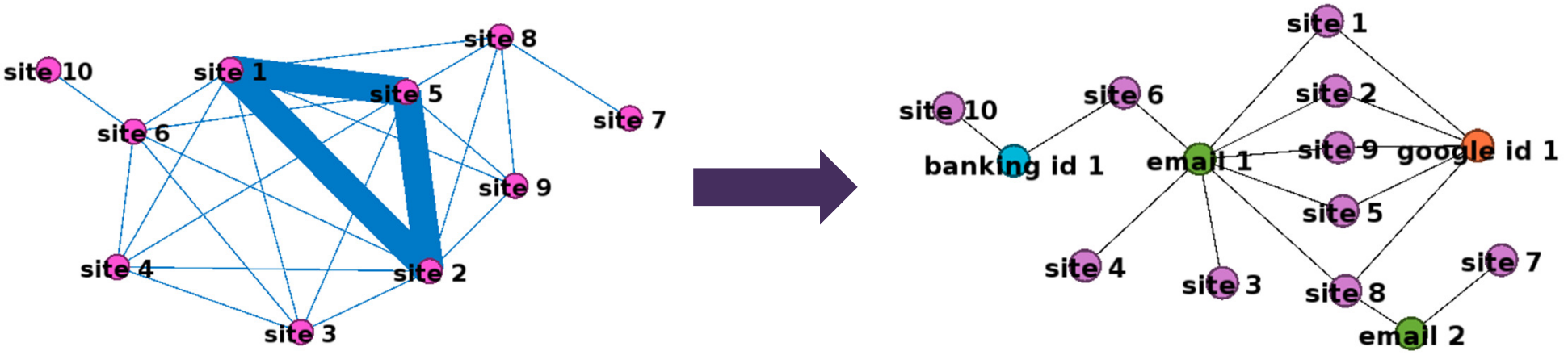
- Nodes represents **homogeneous data** (every node is a website)
- **Clusters tend to be dense**, so easily spotted by computing modularity classes

Cons

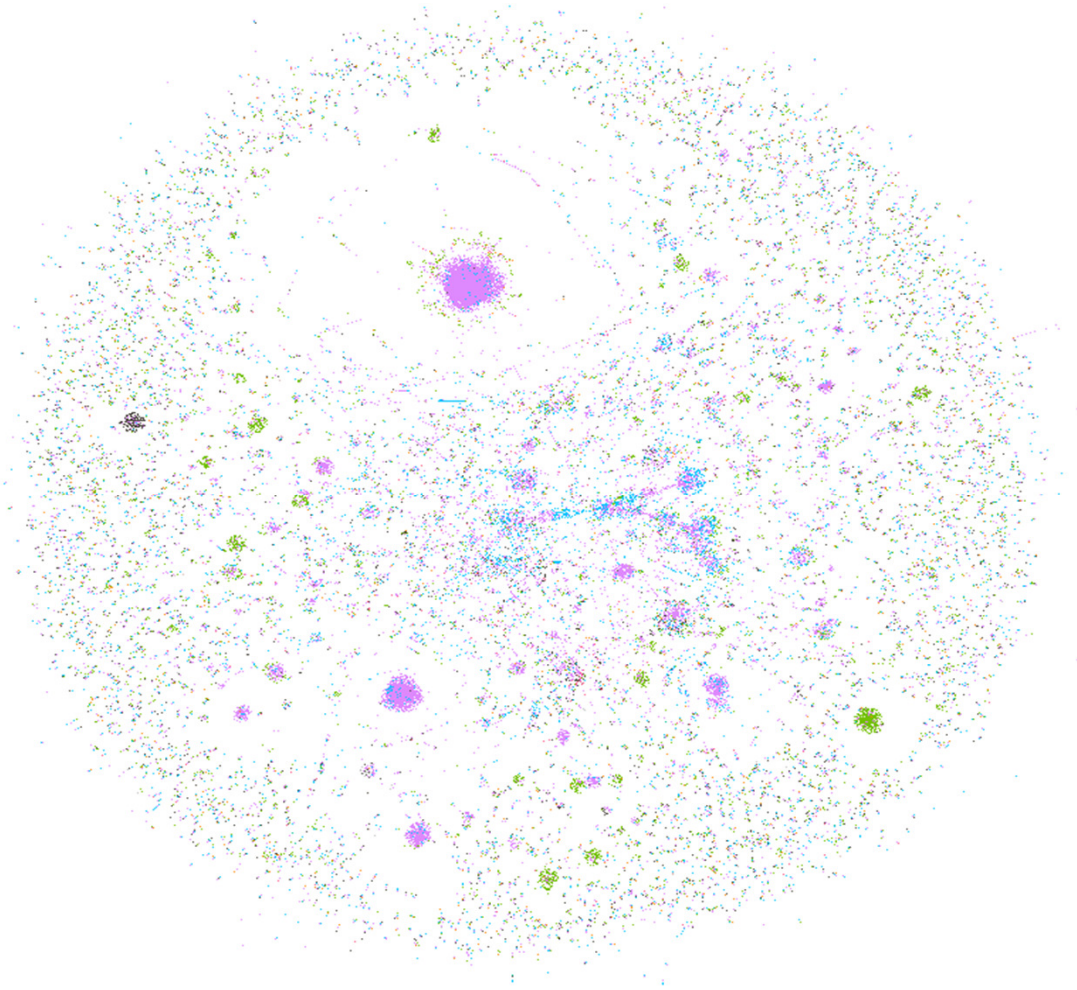
- Cluster density leads to **heavy graphs** (worst-case: $O(n^2)$ edges)
- **Difficult to see** the relationship behind edges

A more appropriate representation

- Node = website OR feature
- Edge = feature's presence in the website
- Unweighted edges
- Average: O(n) number of edges



Clusters overview



FORESIGHT SECURITY CybelAngel

Ranking threats

Once the clusters are built, it is easy to rank them by number of websites/aggregated traffic. This is a precious information for takedowns.

Rank	Traffic indicator (aggregated)	Nbr of domains	Leader domain
33	6086	1	shop24.ru
34	5539	74	fr.fashionmag.com
35	5261	1	www.cheaprooms.com
36	5234	1	101shopbuy.com
37	5229	107	parfumeram.ru
38	5163	3	www.kellyfind.com
39	4791	52	www.parfumidee.ch
40	4780	4	raven.cam.ac.uk

Looking for a counterfeit luxury watch

We will see how this methodology helped us map the websites selling counterfeit watches of a famous luxury brand.

FORESIGHT SECURITY CybelAngel

Filtering pDNS

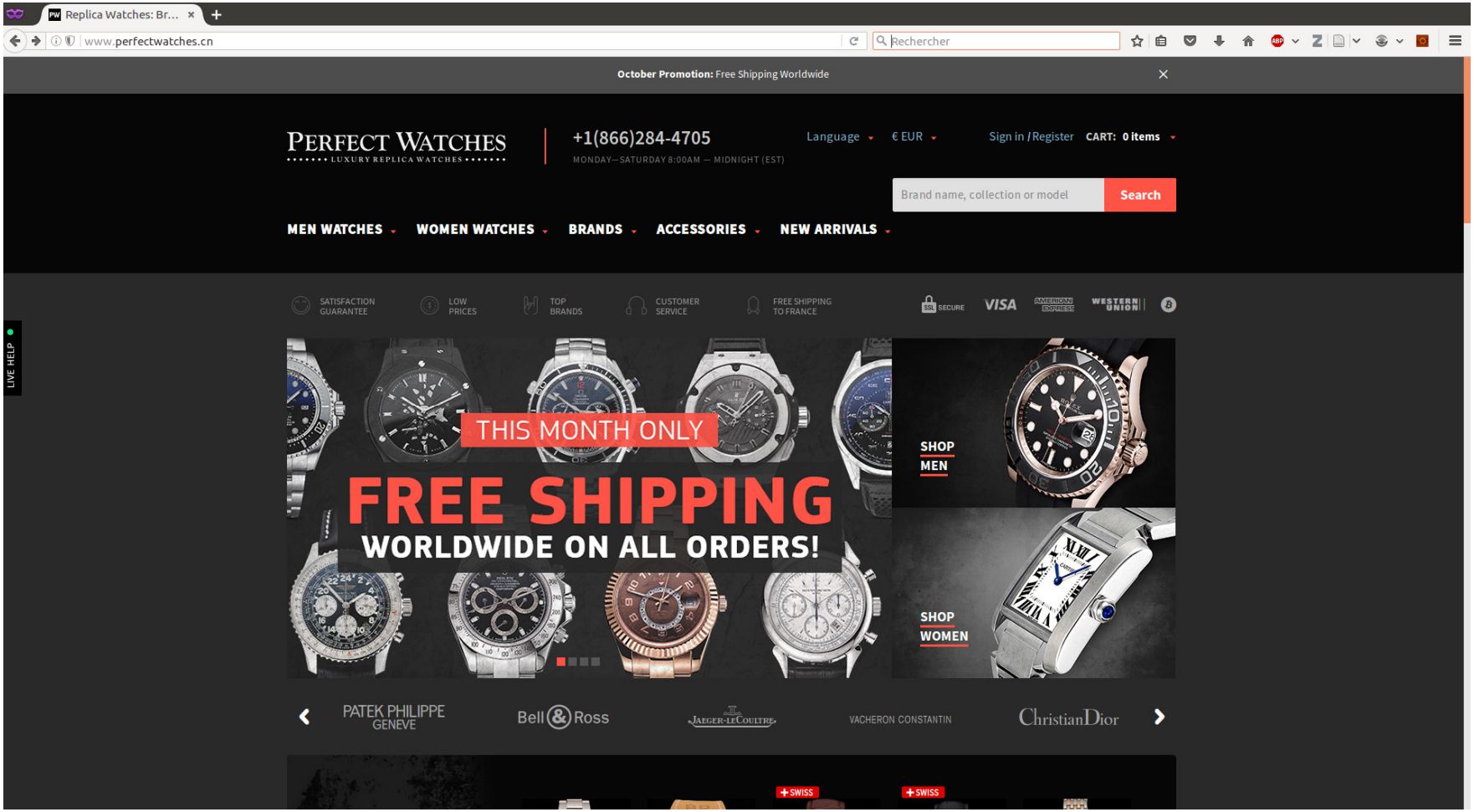

```
{"rrclass": "IN", "count": 3, "rrtype": "NS", "time_first": 1477272302, "rdata": ["ns0.dnsmadeeasy.com.", "ns1.dnsmadeeasy.com.", "ns2.dnsmadeeasy.com.", "ns3.dnsmadeeasy.com.", "ns4.dnsmadeeasy.com."], "type": "EXPIRATION", "rrname": "helser.com.", "bailiwick": "helser.com.", "time_last": 1477325407, "rrttl": 86400}
{"rrclass": "IN", "count": 1, "rrtype": "NS", "time_first": 1477313859, "rdata": ["ns3.internetwire.de.", "ns1.internetwire.de.", "ns2.internetwire.de.", "ns4.internetwire.de."], "type": "EXPIRATION", "rrname": "09495.de.", "bailiwick": "de.", "time_last": 1477313859, "rrttl": 86400}
{"rrclass": "IN", "count": 2, "rrtype": "A", "time_first": 1477277592, "rdata": ["91.240.85.236"], "type": "EXPIRATION", "rrname": "tetrabalt.ru.", "bailiwick": "tetrabalt.ru.", "time_last": 1477301753, "rrttl": 300}
{"rrclass": "IN", "count": 1, "rrtype": "CNAME", "time_first": 1477313860, "rdata": ["2-01-2824-00e7.cdx.cedexis.net."], "type": "EXPIRATION", "rrname": "ca.cartier.com.", "bailiwick": "cartier.com.", "time_last": 1477313860, "rrttl": 600}
{"rrclass": "IN", "count": 1, "rrtype": "CNAME", "time_first": 1477313859, "rdata": ["23.proddtg.com."], "type": "EXPIRATION", "rrname": "0941.tw.", "bailiwick": "0941.tw.", "time_last": 1477313859, "rrttl": 3600}
{"rrclass": "IN", "count": 14, "rrtype": "SOA", "time_first": 1477272200, "rdata": ["ns1.bluehost.com. root.box853.bluehost.com. 2014080102 86400 7200 3600000 300"], "type": "EXPIRATION", "rrname": "truefoodmovement.com.", "bailiwick": "truefoodmovement.com.", "time_last": 1477297093, "rrttl": 300}
{"rrclass": "IN", "count": 1, "rrtype": "MX", "time_first": 1477313831, "rdata": ["10 mx.yandex.ru."], "type": "EXPIRATION", "rrname": "glaus.ru.", "bailiwick": "glaus.ru.", "time_last": 1477313831, "rrttl": 600}
{"rrclass": "IN", "count": 1, "rrtype": "A", "time_first": 1477313831, "rdata": ["85.193.69.29"], "type": "EXPIRATION", "rrname": "asosh-klin.edusite.ru.", "bailiwick": "edusite.ru.", "time_last": 1477313831, "rrttl": 86400}
{"rrclass": "IN", "count": 2, "rrtype": "A", "time_first": 1477272291, "rdata": ["66.210.41.73", "66.210.41.64", "66.210.41.40", "66.210.41.81", "66.210.41.66", "66.210.41.50", "66.210.41.41", "66.210.41.57", "66.210.41.74"], "type": "EXPIRATION", "rrname": "a2047.g.akamai.net.", "bailiwick": "g.akamai.net.", "time_last": 1477272291, "rrttl": 20}
```

```
{"rrclass": "IN", "count": 1, "rrtype": "CNAME", "time_first": 1477313919, "rdata": ["ext-router.qloud.yandex.net."], "type": "EXPIRATION", "rrname": "8iqzz.pcloadletter.3087.ws.yandex.ru.", "bailiwick": "ws.yandex.ru.", "time_last": 1477313919, "rrttl": 300}
{"rrclass": "IN", "count": 1, "rrtype": "NS", "time_first": 1477313859, "rdata": ["pdns07.domaincontrol.com.", "pdns08.domaincontrol.com."], "type": "EXPIRATION", "rrname": "greplicawatches.com.", "bailiwick": "com.", "time_last": 1477313859, "rrttl": 172800}
{"rrclass": "IN", "count": 1, "rrtype": "NS", "time_first": 1477313826, "rdata": ["a.ns.mailclub.fr.", "c.ns.mailclub.com.", "b.ns.mailclub.eu."], "type": "EXPIRATION", "rrname": "ferdinand-berthoud.net.", "bailiwick": "net.", "time_last": 1477313826, "rrttl": 172800}
```


50,000
websites

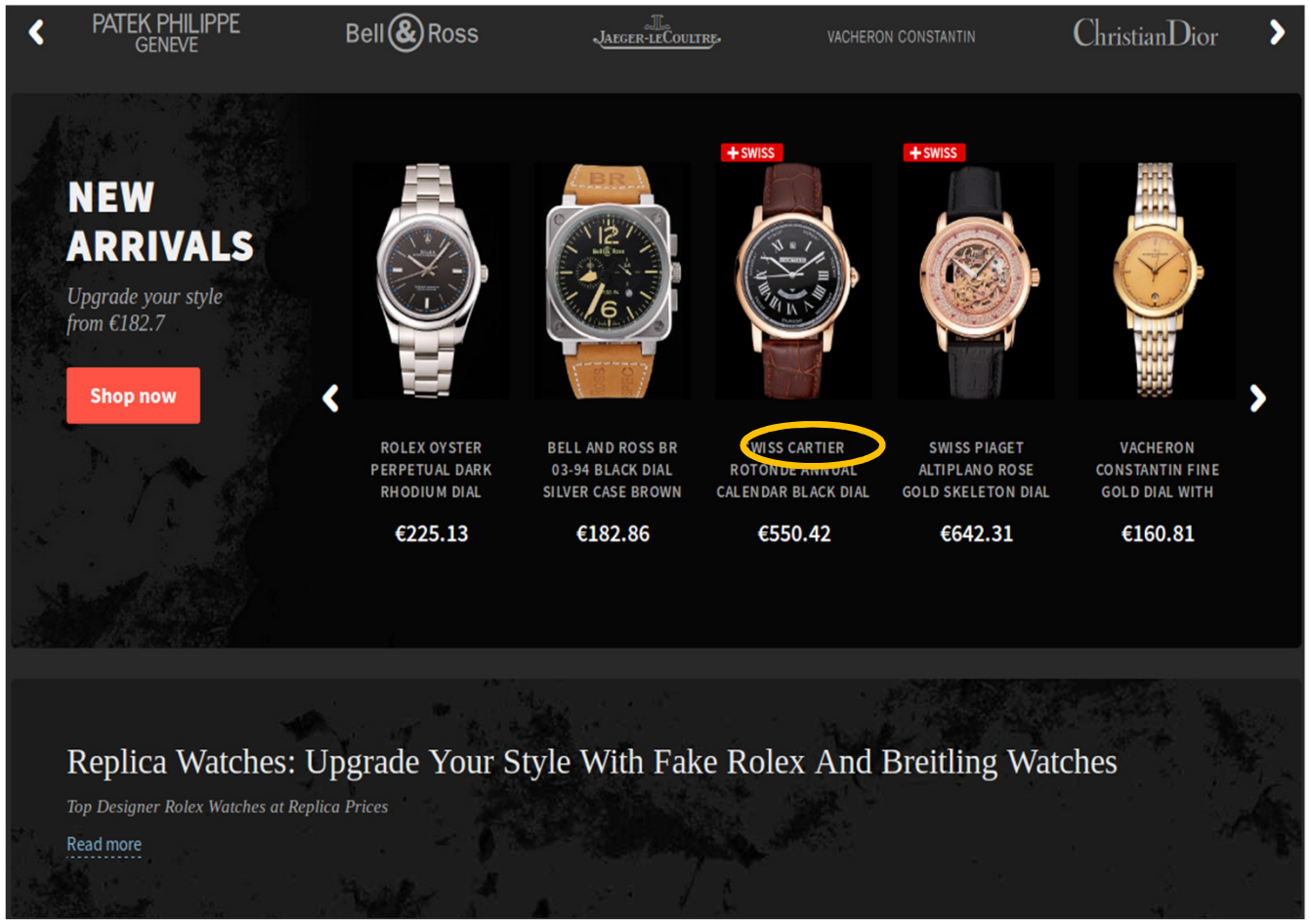
FARSIGHT SECURITY CybelAngel

In-depth analysis



FORSIGHT SECURITY CybelAngel

Keyword matching in page content



FORESIGHT SECURITY CybelAngel

Feature extraction

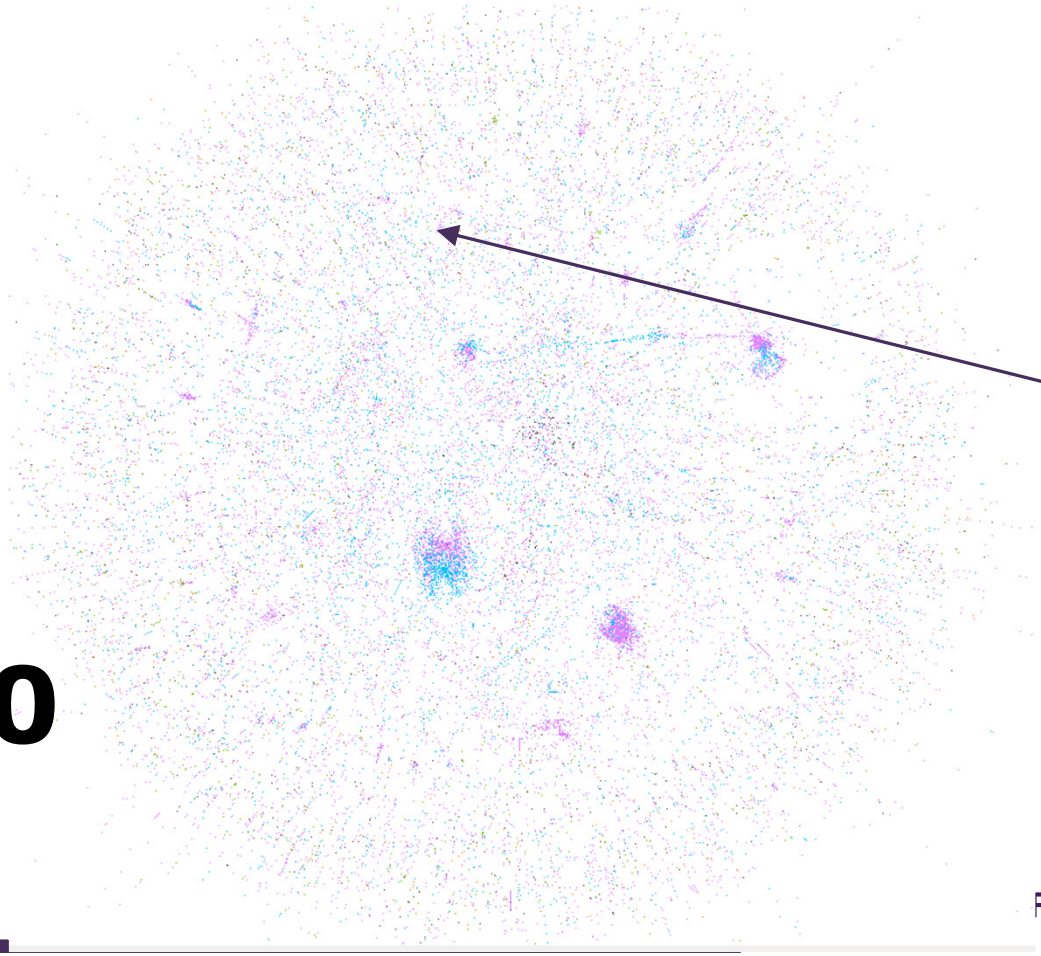
Telephone number

Analytics ID


```
<script type="text/javascript">window.NREUM||(NREUM={});NREUM.info={"beacon":"bam.nr-data.net","licenseKey":"c1ae3fb39c","applicationID":"24044340",
```


FORESIGHT SECURITY CybelAngel

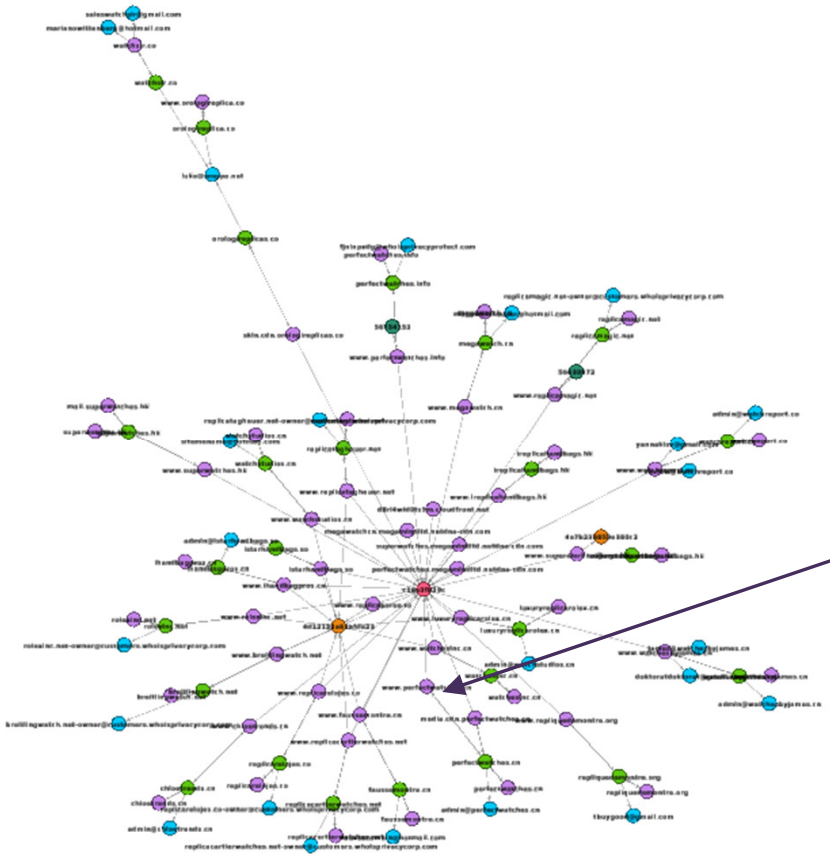
Graph **representation**



50,000
websites

FORESIGHT SECURITY CybelAngel

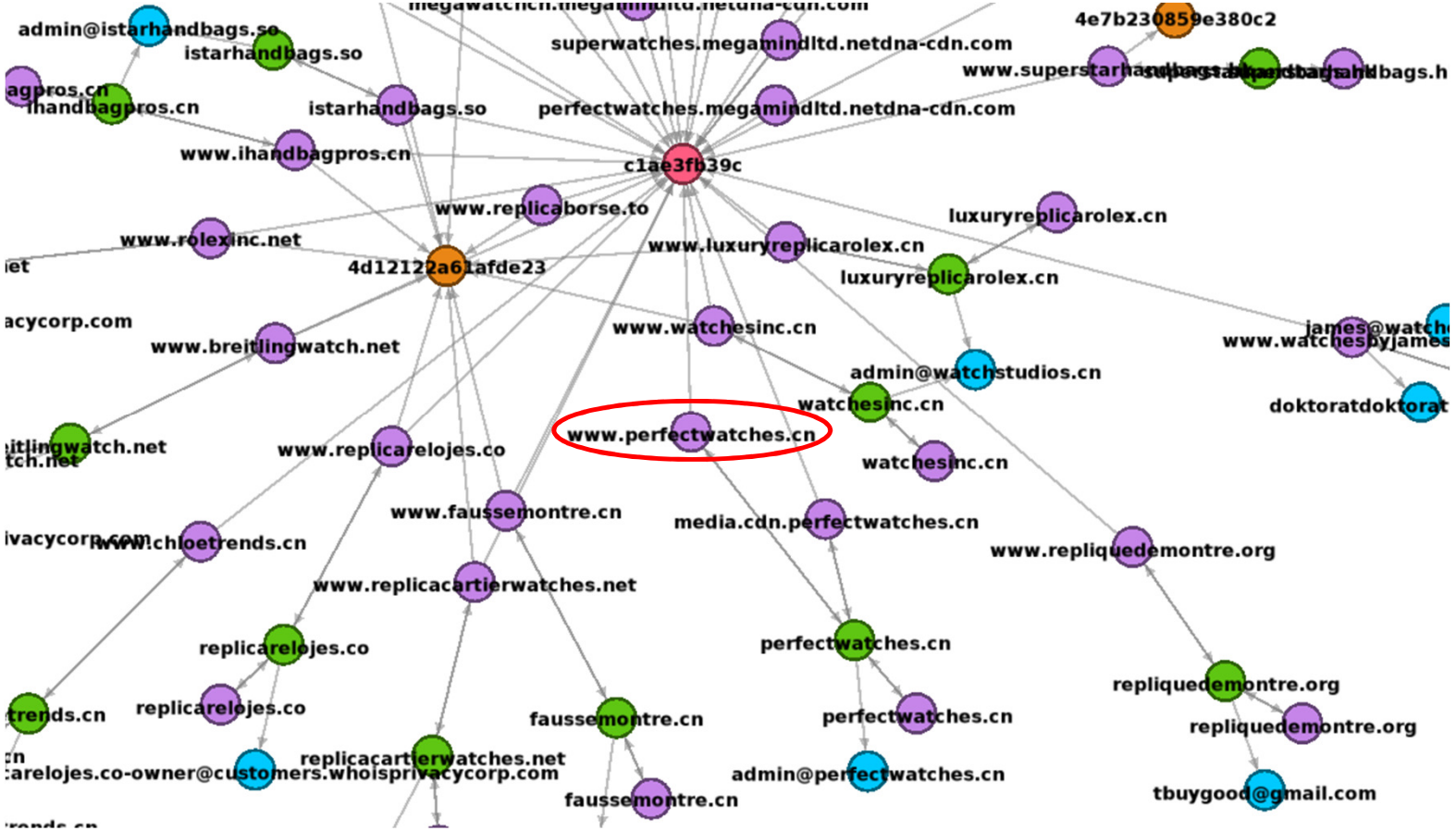
Hunting in the graph



Still our guy

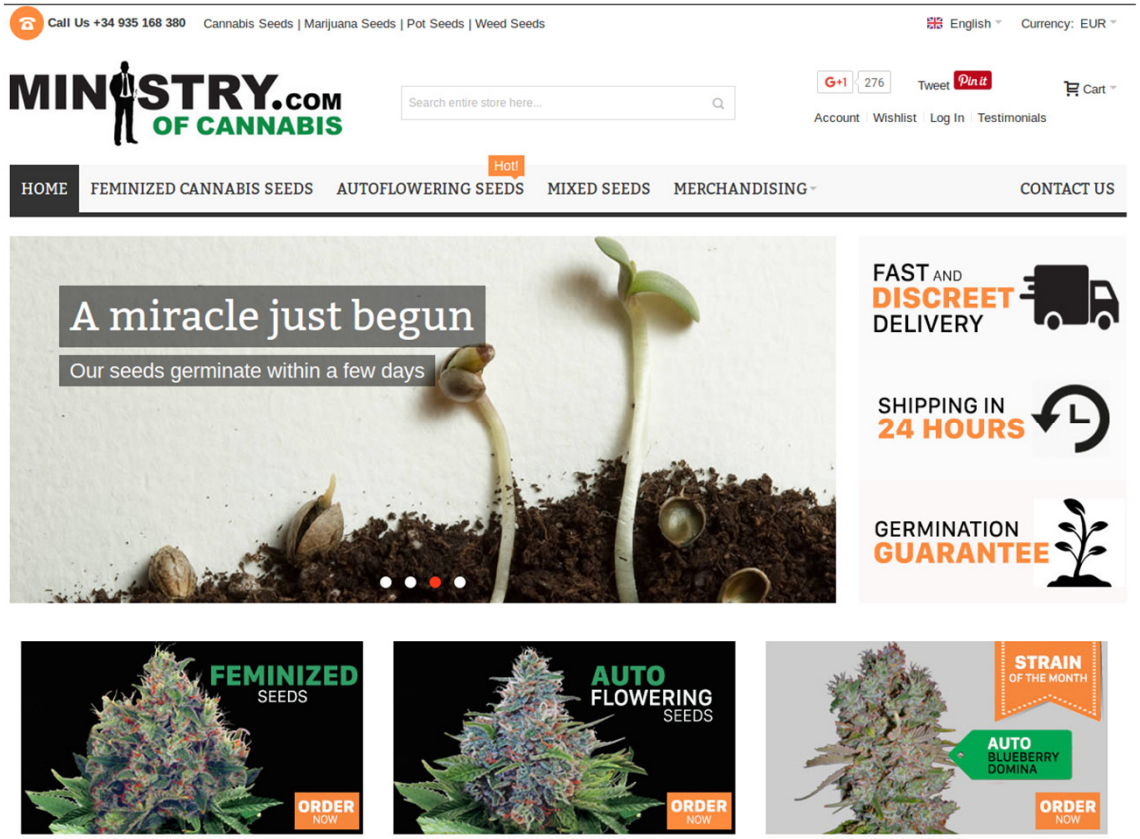
FORESIGHT SECURITY CybelAngel

Our well-connected guy



FORSIGHT SECURITY CybelAngel

It also works with narcotics



Weed Seed Shop

Growing Pot

Growing Marijuana Indoors

Best Guide, Ever.

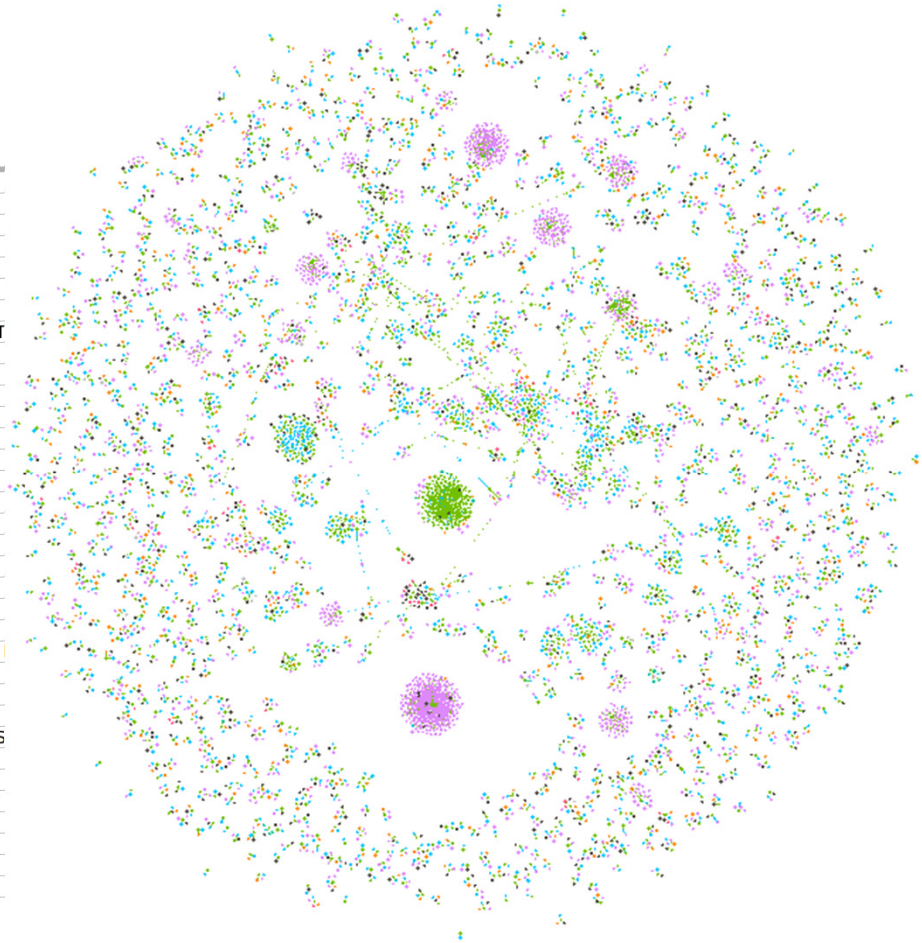
Growing Marijuana Indoors

- Growing Marijuana Outdoors - Sister guide
- Growing Weed - HowtoGrowWeedIndoors.com

FORESIGHT SECURITY CybelAngel

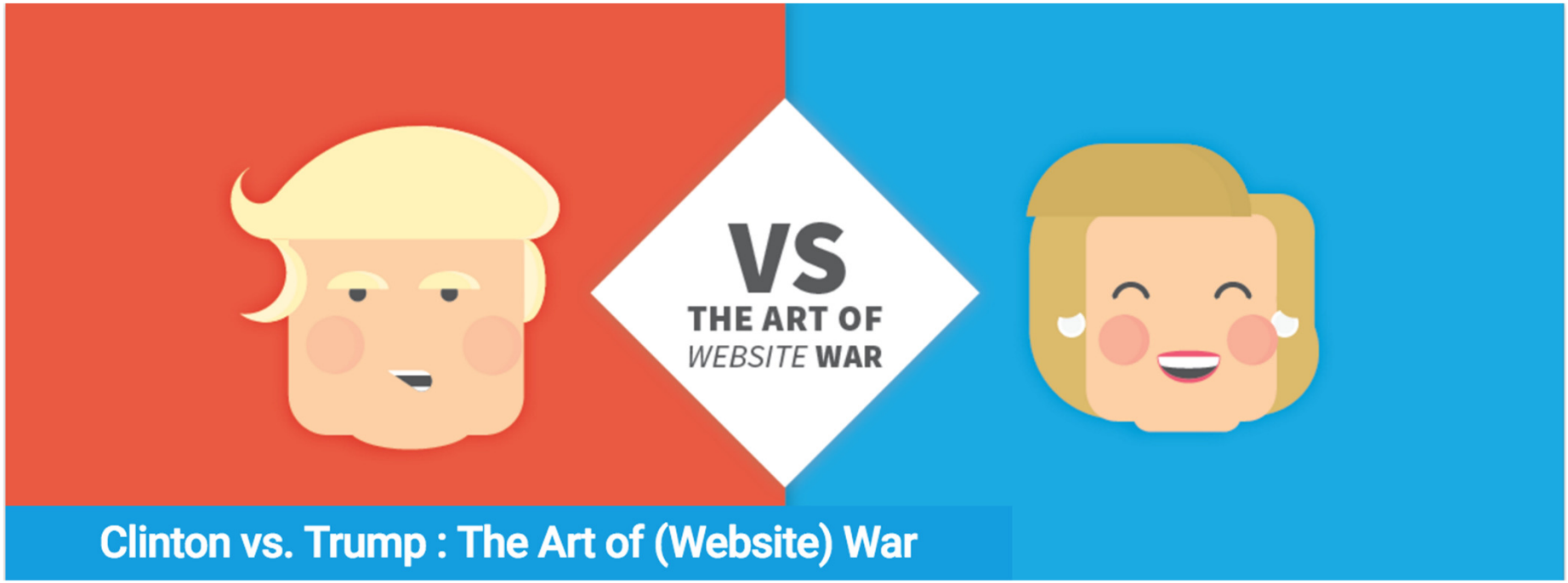
A representation of the marijuana business

Name	Traffic	Category	Cluster	IP	Registrar
howtogrowweed420.com	610		21	104.28.20.44, 104.28.21.4	ENOM, INC.
medcannabis.info	526		23	141.101.118.102, 141.101	DomainContext Inc.
d27dyzmil4j68i.cloudfront.net	526		24	54.239.158.104, 54.239.1	MARKMONITOR INC.
marijuanapolitics.com	424		27	72.52.161.62	GODADDY.COM, LLC
amsterdammarijuanaseeds.com	423		26	178.251.24.168	DNC HOLDINGS, INC.
onlybackpacks.com	404		29	192.96.207.44	GODADDY.COM, LLC
stfuconservatives.tumblr.com	403		30	66.6.41.21, 66.6.42.21, 6	CRAZY DOMAINS FZ-LLC
cannabisculture.hanf.ws	344		32	104.28.6.93, 104.28.7.93	GLOBAL DOMAINS INTERNAT
emarijuanaclones.com	310		25	50.63.75.1	GODADDY.COM, LLC
womenssundresses.net	301		33	192.185.231.200	GODADDY.COM, LLC
cannabisnowmagazine.com	292		34	50.62.111.113	GODADDY.COM, LLC
www.marijuana-anonymous.org	280		36	50.87.73.37	FastDomain Inc.
www.ministryofcannabis.com	269		37	87.76.27.58	GODADDY.COM, LLC
www.cannabisseeds.com	265		38	206.188.193.164	NETWORK SOLUTIONS, LLC.
almarijuana.com	257		15	45.79.200.8	GODADDY.COM, LLC
marijuanaonline007.com	248		39	217.116.232.226	REGISTER.COM, INC.
moviereviewshop.com	223		40	173.214.183.184	GODADDY.COM, LLC
himarijuana.com	174		15	45.79.200.8	GODADDY.COM, LLC
anteaterskinboots.com	171		43	50.63.85.200	WILD WEST DOMAINS, LLC
wamarijuana.com	169		15	161.47.4.161	GODADDY.COM, LLC
txmarijuana.com	168		15	45.79.200.8	GODADDY.COM, LLC
www.marijuanaselfies.com	160		45	107.170.156.236	GODADDY.COM, LLC
medicalmarijuana.com	157		46	64.156.29.222	MONIKER ONLINE SERVICES
marijuanaplantsonline.com	143		25	50.63.75.1	GODADDY.COM, LLC
www.coloradocannabistours.com	142		48	104.20.35.138	GODADDY.COM, LLC
michiganmedicalmarijuana.org	139		41	184.107.250.226	GoDaddy.com, LLC
nvmarijuana.com	137		51	161.47.4.161	GO MONTENEGRO DOMAINS
thenationalmarijuananews.com	136		52	104.25.160.32, 104.25.16	GODADDY.COM, LLC
www.legalmarijuanaheadshop.com	132		50	107.180.56.179	GODADDY.COM, LLC
www.speedweed.com	132		53	104.20.71.246	BLUE RAZOR DOMAINS, LLC
holisticcannabissummit.com	127		47	104.24.124.169, 104.24.1	1&1 INTERNET SE
www.regulatemarijuanainarizona.org	114		42	104.25.76.31, 104.25.77.3	Domain.com, LLC
www.cannabistutorials.com	114		55	104.27.137.205	GODADDY.COM, LLC
mamarijuana.com	114		15	161.47.4.161	GODADDY.COM, LLC
mari-juana.net	113		22	5.45.121.223	ENOM, INC.



FARSIGHT SECURITY CybelAngel

CybelAngel-Farsight Report: Pick A Side, Pick A Site



Check it out

http://blog.cybelangel.com/clinton-vs-trump-art-website-war/
https://www.farsightsecurity.com/Blog/20160921-farsight-cybelangel-2016campaign/

FARSIGHT SECURITY CybelAngel

Key Takeaways

- Counterfeiting is a significant and growing online threat
- Current solutions based on zonefiles lack efficiency
- pDNS + Feature Extraction + Graphs can be used to optimize takedown efforts
- This research could be derived to address other problems...

FARSIGHT SECURITY CybelAngel

Q&A

Thank you for your attention.

Free DNSDB Test Drive for Black Hat attendees

Farsightsecurity.com/BHEU

Special thanks for research assistance to:

Thomas Garnier & Paul Petit

FARSIGHT SECURITY CybelAngel