

Hunting with Passive DNS

Ben April – CTO Farsight Security, Inc.

FIRST Regional Symposium Latin America & Caribbean
Punta Cana (DO), May 8th, 2019

Copyright 2019 Farsight Security, Inc.

Agenda

- I. Passive DNS in 5 minutes
- II. Examples
 - I. Phishing
 - II. Fake-Pharma
 - III. Counterfeit [Currency|Identification|Merchandise|Etc]
- III. Limits to Passive DNS
- IV. Key Takeaways

Tools - 3 ways to use the same API

- **DNSDB Scout** - Found in the Chrome or Firefox add-on stores.
- **Maltego** – <https://paterva.com/> part of the transform hub.
- **Dnsdbq** – <https://github.com/dnsdb/dnsdbq>

Disclaimers

- Query results based on live data presented as I found it. Might not be polite.
- The data in this deck is a snapshot in time. It is already outdated.
- Don't use DNS on it's own to convict. (Sinkholes etc)
- TPL: White

Passive DNS in 5 minutes

Everything begins with DNS ...

DNS as Map

- Most everything we do on the Internet...
 - B2B Web, B2B Web, E-mail, I-M, *<your idea here>*
 - ...relies on TCP/IP*, and begins with a DNS lookup
- Mobile Internet is dominated by search ...
 - ... but search itself relies extensively upon DNS
- DNS has a rigorous internal structure
 - Things that are in fact related, *are* related in DNS
 - You can have *Whois* privacy, but not DNS privacy

Internal Infrastructure

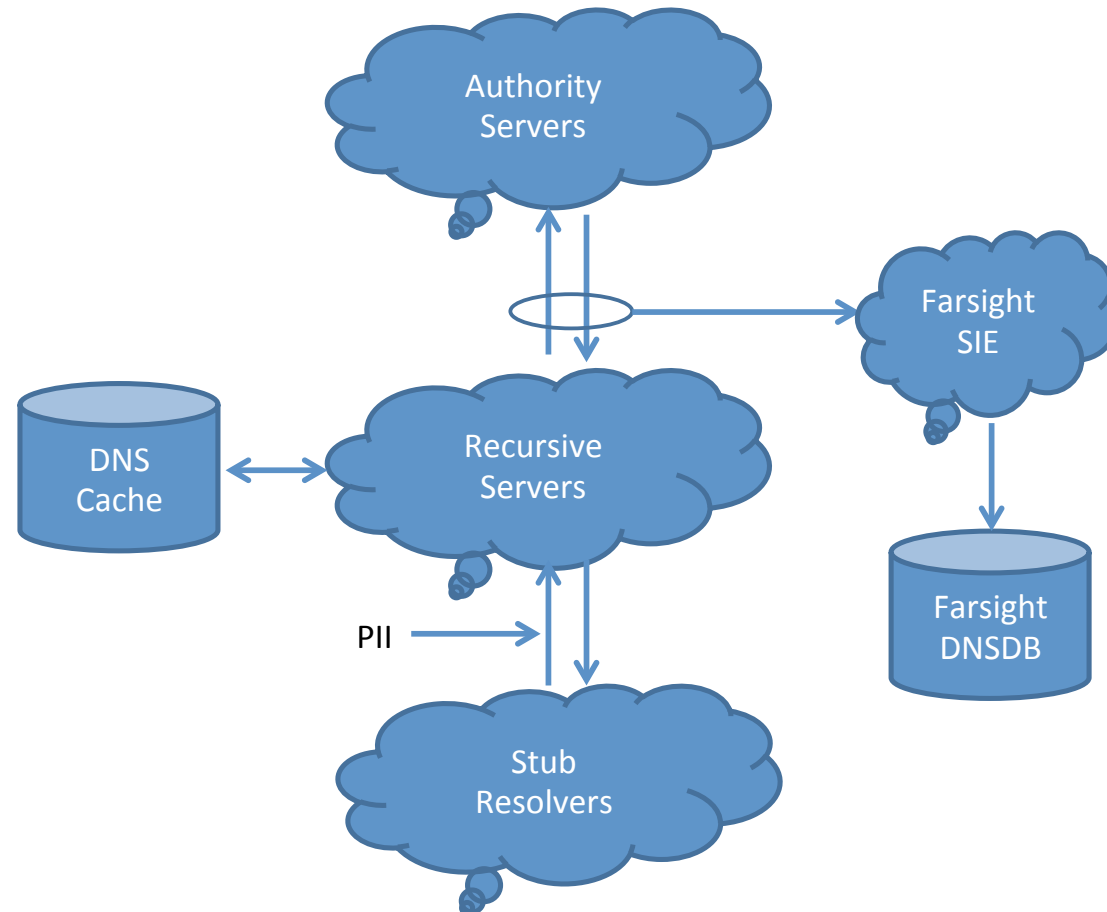
- Domain names are grouped into zones
 - Like *root* zone, or “COM”, or “EXAMPLE.COM”
- A *zone* has one or more *name servers*
 - Like “COM. NS a.gtld-servers.net”
- Each *name server* has one or more *addresses*
 - Like “a.gtld-servers.net A. 192.5.6.30”
- Other domain names also have *addresses*
 - Like “www.apnic.net A. 203.119.102.244”
- IP *addresses* are grouped into *netblocks*
 - Like “192.5.6.0/24” or “203.119.103.240/28”

Passive DNS: Lots of Keys/Many values

```
;; bailiwick: farsightsecurity.com.  
;;      count: 26,394  
;; first seen: 2015-04-01 14:17:52 -0000  
;; last seen: 2017-09-05 06:31:07 -0000  
farsightsecurity.com. IN A 104.244.13.104
```

- DNS Key = {QNAME, QCLASS, QTYPE}
- pDNS key = {QNAME, QCLASS, QTYPE, RDATA, bailiwick}
- Output based on an open standard draft <https://tools.ietf.org/id/draft-dulaunoy-dnsop-passive-dns-cof-03.html>

Passive DNS Architecture

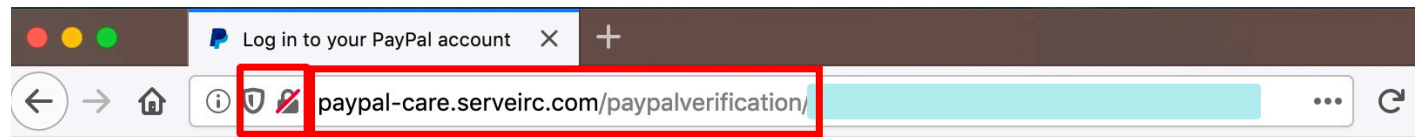


Passive DNS Data Options


- CERT.at/Aconet Passive DNS (inquire: kaplan@cert.at or lendl@cert.at)
- <https://www.farsightsecurity.com/solutions/dnsdb/>
- <https://www.passivedns.cn/help/>
- <https://www.opendns.com/enterprise-security/resources/data-sheets/investigate/>
- <https://www.riskiq.com/products/passivetotal/>
- <https://securitytrails.com/corp/feeds>
- <https://www.virustotal.com/#search>
- <https://zetalytics.com/>
- <http://www.circl.lu/services/passive-dns/>
- <http://passivedns.mnemonic.no/search/>
- <https://www.cs.auckland.ac.nz/research/groups/sde/dhdb-index.php>

Threat Hunting Using DNS

Example I. Phishing



This is "probably" **NOT** PayPal!



Email address

Enter your password

Log In

Having trouble logging in?

Sign Up

[Contact Us](#) [Privacy](#) [Legal](#) [Worldwide](#)

Let's Check Domain Whois For The Base Domain Name...

\$ whois serveirc.com

[...]

Registrant Name: Dan Durrer

Registrant Organization: **No-IP.com**

Registrant Street: 425 Maestro Dr. Second Floor

Registrant City: Reno

Registrant State/Province: NV

Registrant Postal Code: 89511

Registrant Country: US

Registrant Phone: +1.7758531883

Registrant Email: **domains@no-ip.com**

[...]

Maltego Transforms

Maltego Community Edition 4.1.14

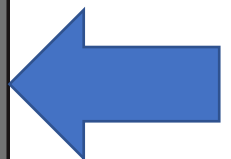
Investigate View Entities Collections Transforms Machines Collaboration Import | Export Windows

Transform Hub Transform Manager New Local Transform... Certificate Manager Manage Services Run View

Home X Start Page Transform Hub

Refresh Transform Hub Update Transforms

	PATERVA CTAS CE Paterva Standard Paterva Transforms FREE INSTALLED	CaseFile Entities Paterva Additional entities from CaseFile FREE INSTALLED	Cisco Threat Grid Cisco Threat Grid Query Threat Grid's database of threat intelligence. PURCHASED SEPARATELY
Kaspersky Lab Kaspersky Lab Query Kaspersky Threat Intelligence Data Feeds. Note that Dat... PURCHASED SEPARATELY	Shodan Paterva Query Shodan data from within Maltego! FREE INSTALLED	ZETAnalytics Massive Passive ZETAnalytics Pivots include billions of records for historical domains, email... FREE	Hybrid-Analysis Hybrid Analysis This set of transforms are based on the Hybrid Analysis (HA) ... FREE
VirusTotal Public API Malformity Labs Query the VirusTotal Public API FREE	ThreatMiner ThreatMiner Query and pivot on data from ThreatMiner.org. FREE	PassiveTotal PassiveTotal Query PassiveTotal source and account data. FREE	Farsight DNSDB Farsight Security, Inc. Query the largest DNS Intelligence database, 100+ Billion rec... FREE INSTALLED
Blockchain.info (Bitcoin) Paterva For visualizing the Bitcoin blockchain. FREE INSTALLED	SocialLinks CE SocialLinks SocialLinks CE FREE	The Movie Database Paterva Transforms that visualize the movie database (TMDB) FREE	Have I been Pwned? Christian Heinrich Pwned Password v3 Support FREE
People Mon People Mon Queries peoplemon.com FREE	CipherTrace CipherTrace Cryptocurrency forensics and anti money laundering (AML) i... FREE	FullContact Christian Heinrich 360 insights into the people who matter most. FREE	Clearbit Christian Heinrich Enrich sign-ups, identify prospects and gain customer insights FREE
SocialLinks SocialLinks Social Networks, Search Engines, People and Companies PURCHASED SEPARATELY	Recorded Future Inc. Recorded Future Inc. Query Recorded Future for threat intelligence information PURCHASED SEPARATELY	ThreatConnect ThreatConnect ThreatConnect Platform Transform Set PURCHASED SEPARATELY	Palo Alto Networks AutoFocus Palo Alto Networks Query Palo Alto Networks' AutoFocus API. PURCHASED SEPARATELY
ThreatGRID by Malformity Labs Malformity Labs No longer accepting new customers, please use the official Cl... PURCHASED SEPARATELY	Flashpoint Flashpoint Business Risk Intelligence (BRI) from the Deep and DarkWeb. PURCHASED SEPARATELY	Intel 471 Intel 471 Query Intel 471 for actor-centric intelligence information. PURCHASED SEPARATELY	CrowdStrike Intel CrowdStrike CrowdStrike Intelligence API Transforms PURCHASED SEPARATELY
CrowdStrike ThreatGraph CrowdStrike CrowdStrike ThreatGraph API Transforms PURCHASED SEPARATELY	SocialNet ShadowDragon Social Media Investigative Intelligence Tool PURCHASED SEPARATELY	AliasDB ShadowDragon Database of Defacements and the Aliases that took attribution PURCHASED SEPARATELY	NewsLink Paul@Paterva Transforms for monitoring and analyzing news from different... FREE
Digital Shadows Digital Shadows Query the Digital Shadows cyber threat intelligence database. PURCHASED SEPARATELY	Cofense Intelligence Cofense Search and visualize relationships between phishing attacks a... PURCHASED SEPARATELY	MalNet with ProofPoint ShadowDragon Maps malware intelligence. Great for IR and analysts. PURCHASED SEPARATELY	FireEye iSIGHT Intelligence FireEye iSIGHT Intelligence Query FireEye iSIGHT Intelligence holdings. PURCHASED SEPARATELY



Maltego Community Edition 4.1.14

InvestigateViewEntitiesCollectionsTransformsMachinesCollaborationImport | ExportWindows

Transform Hub

Transform Manager

New Local Transform...

Certificate Manager

Manage Services

Run View

Entity Palette

HomeNew Graph (1)

100%

Detail View

Search:

Layout

Freeze

View

Recently Used

DNS Name

Domain

IPv4 Address

Phrase

URL

Cryptocurrency

Bitcoin Address

Bitcoin Transaction

Cryptocurrency Owner

Ethereum Address

Ethereum Transaction

Devices

Desktop Computer

Device

Mobile Computer

Mobile Phone

Smartphone

Events

Conversation (Email)

Conversation (Phone)

Incident

paypal-care.serveirc.com

Run Transform(s)

Farsight DNSDB

[DNSDB] Domains using this MX

[DNSDB] Domains using this NS

[DNSDB] Lookup \$dnsname.*

[DNSDB] Lookup \$dnsname.*/A

[DNSDB] Lookup \$dnsname.*/AAAA

[DNSDB] Lookup \$dnsname.*/CNAME

[DNSDB] Lookup *.\$dnsname

[DNSDB] Lookup *.\$dnsname/A

[DNSDB] Lookup *.\$dnsname/AAAA

[DNSDB] Lookup *.\$dnsname/CNAME

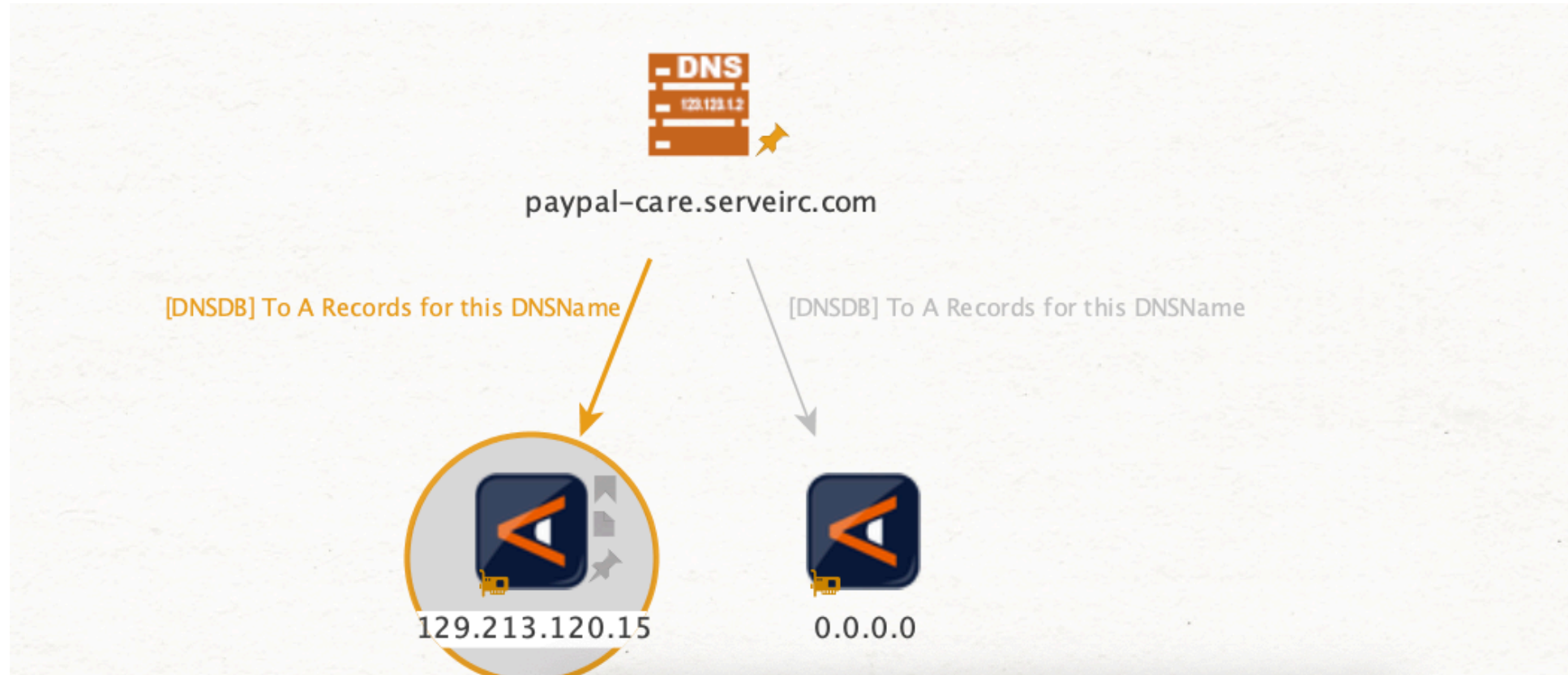
[DNSDB] Records with this value

[DNSDB] To A Records for this DNSName

[DNSDB] To AAAA Records for this DNSN...

Output

Maltego



DNSDB Scout

Successful Query for: paypal-care.serveirc.com ANY (Limit 2000)

EXPORT AS CSV

EXPORT AS JSON

API DOCS

Show entries

Time Last Seen ▼	Time First Seen	Count	Bailiwick	RRname	RRtype	Rdata
2019-04-22 22:25:34	2019-04-12 18:15:29	9	serveirc.com.	paypal-care.serveirc.com.	A	0.0.0.0
2019-04-10 18:21:00	2019-03-22 18:38:05	32	serveirc.com.	paypal-care.serveirc.com.	A	129.213.120.15

Showing 1 to 2 of 2 entries

dnsdbq

```
bapril@rd2:~$ dnsdbq -r paypal-care.serveirc.com
;; record times: 2019-04-12 18:15:29 .. 2019-04-22 22:25:34
;; count: 9; bailiwick: serveirc.com.
paypal-care.serveirc.com.  A  0.0.0.0

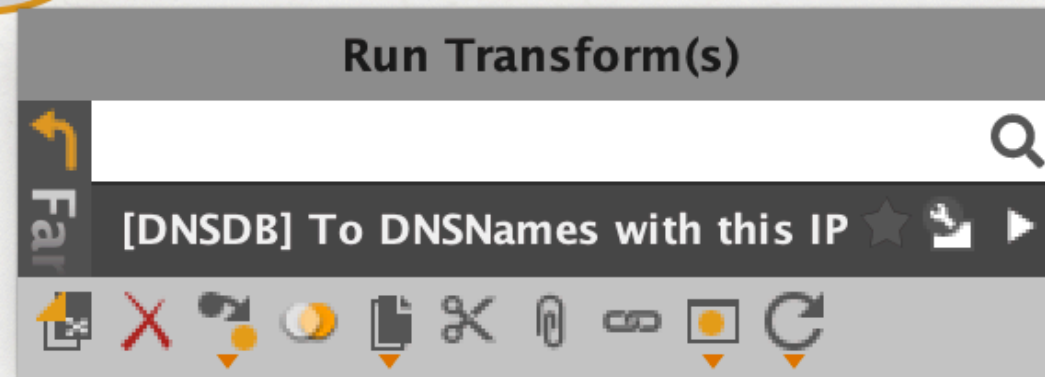
;; record times: 2019-03-22 18:38:05 .. 2019-04-10 18:21:00
;; count: 32; bailiwick: serveirc.com.
paypal-care.serveirc.com.  A  129.213.120.15
```

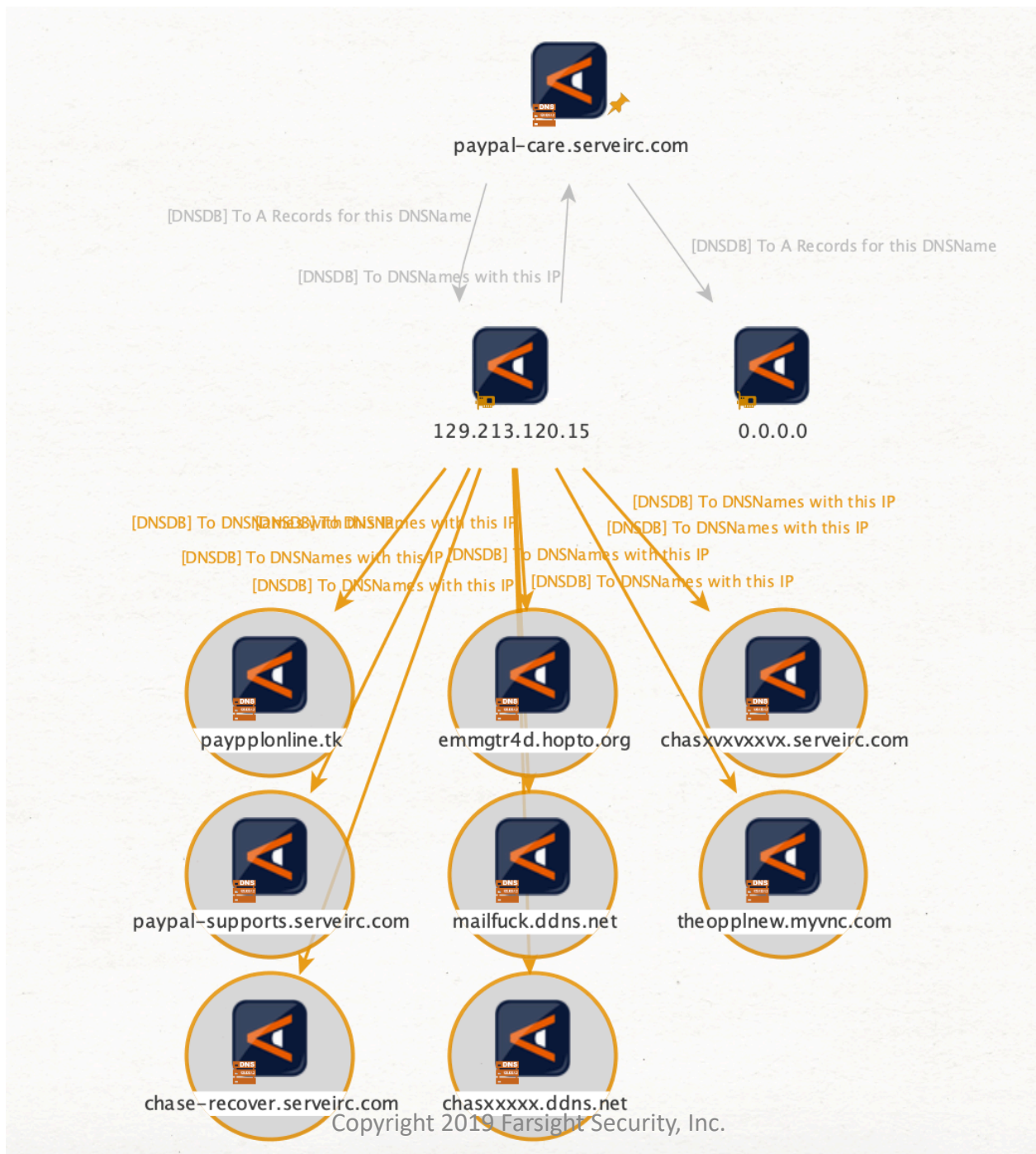



paypal-care.serveirc.com

[DNSDB] To A Records for this DNSName

[DNSDB] To A Records for this DNSName





Detail View



IPv4 Address
maltego.IPv4Address
129.213.120.15

- Relationships

- Incoming

paypal-care.serveirc.com

- Outgoing

chasxvxxvxxv.serveirc.com

paypal-care.serveirc.com

chasxxxxx.ddns.net

paypal-supports.serveirc.com

emmgtr4d.hopto.org

theopplnew.myvnc.com

paypplonline.tk

mailfuck.ddns.net

chase-recover.serveirc.com

- DNSDB Output

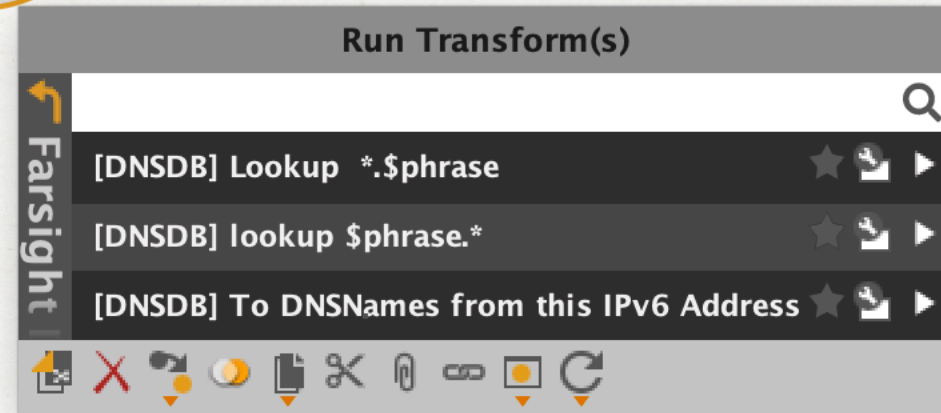
```
;; bailiwick: serveirc.com.  
;; count: 32  
;; first seen: 2019-03-22 18:38:05 -0000  
;; last seen: 2019-04-10 18:21:00 -0000  
paypal-care.serveirc.com. IN A 129.213.120.15
```

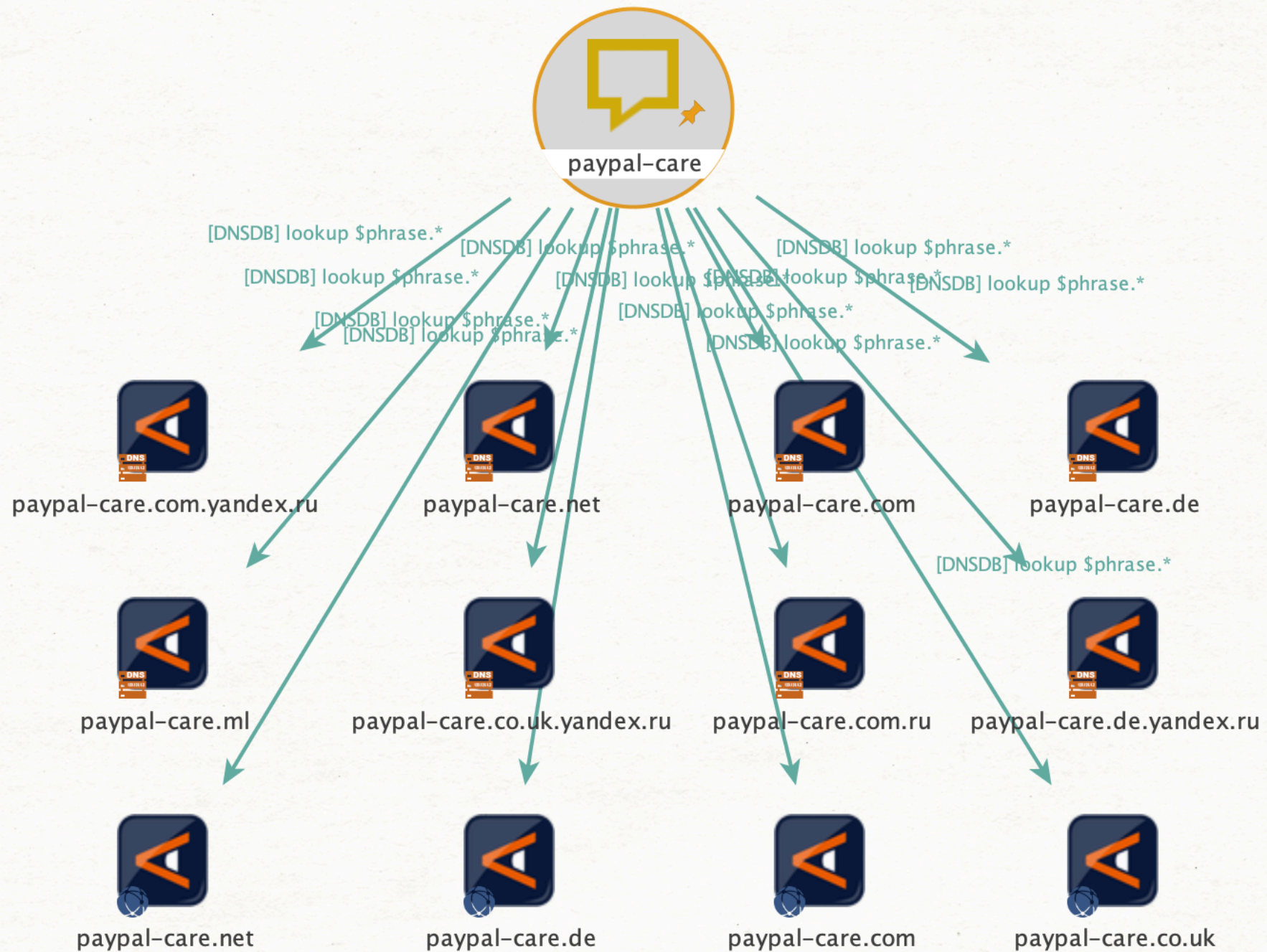
- DNSDB JSON Output

```
{"count": 32, "time_first": 1553279885, "rrtype": "A", "rrname": "paypal-care.serveirc.com.", "bailiwick": "serveirc.com.", "rdata": ["129.213.120.15"], "time_last": 1554920460}
```

- Generator detail

Source	paypal-care.serveirc.com	(DNS Name)
Transform	[DNSDB] To A Records for this DNSName	
Gen. date	2019-05-08 11:53:22.663 -0400	



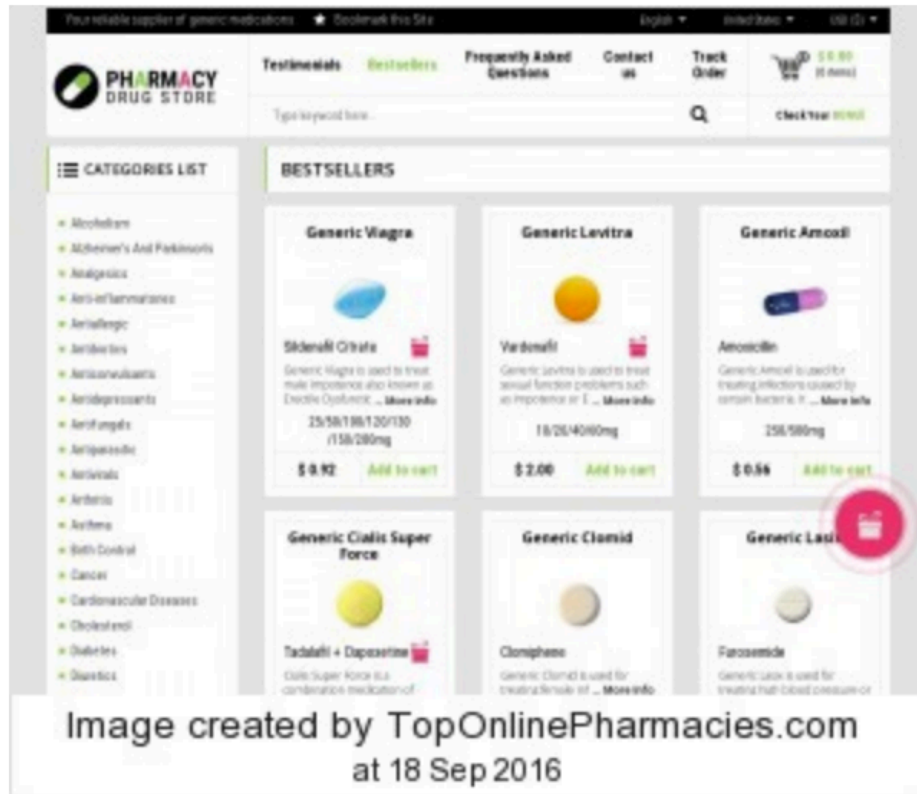


Threat Hunting Using DNS

Example II. Fake-Pharma

Pom-Pharmacy.com

No customer reviews yet
Be the first to [Write a Review](#)



Site Title

POM Pharmacy

Website

pom-pharmacy.com

Status

Unavailable, see **Alternatives**

Product Range

Wide Selection of Indian Generics

Shipping Area

Worldwide

Shipping Options

Standard Airmail, 14-21 days - \$10.00

Courier Service, 5-9 days - \$30.00

Payment Methods



Alexa Popularity

8488791

Site Self-Description

POM Pharmacy

Successful Query for: pom-pharmacy.com A (Limit 50000)

EXPORT AS CSV

EXPORT AS JSON

API DOCS

Show 25 entries

Time Last Seen ▼	Time First Seen	Count	Bailiwick	RRname	RRtype	Rdata
2019-05-06 14:14:04	2017-10-06 17:20:44	1377	pom-pharmacy.com.	pom-pharmacy.com.	A	66.212.148.115
2017-09-26 12:28:46	2017-03-17 12:51:24	390	pom-pharmacy.com.	pom-pharmacy.com.	A	74.81.170.110
2017-03-14 22:42:18	2016-08-18 17:33:38	1414	pom-pharmacy.com.	pom-pharmacy.com.	A	104.28.22.110 104.28.23.110
2016-08-17 22:23:15	2016-02-15 00:10:04	1921	pom-pharmacy.com.	pom-pharmacy.com.	A	185.92.221.211
2016-02-14 21:56:42	2013-07-19 01:33:42	12025	pom-pharmacy.com.	pom-pharmacy.com.	A	50.7.195.186

Showing 1 to 5 of 5 entries

First

Previous

1

Next

Last

Show 25 entries

Time Last Seen ▼	Time First Seen	Count	Bailiwick	RRname	RRtype	Rdata
2019-05-07 00:42:49	2017-03-15 21:21:39	15494	com.	pom-pharmacy.com.	NS	ns1.seizedservers.com. ns2.seizedservers.com.
2019-05-06 14:14:04	2017-10-06 17:20:44	1377	pom-pharmacy.com.	pom-pharmacy.com.	A	66.212.148.115
2018-03-22 16:02:25*	2017-03-16 16:02:32*	372	com.	pom-pharmacy.com.	NS	ns1.seizedservers.com. ns2.seizedservers.com.
2017-09-26 12:28:46	2017-03-17 12:51:24	390	pom-pharmacy.com.	pom-pharmacy.com.	A	74.81.170.110
2017-03-15 16:02:35*	2014-01-24 17:13:12*	1141	com.	pom-pharmacy.com.	NS	duke.ns.cloudflare.com. lily.ns.cloudflare.com.
2017-03-14 22:42:18	2016-08-18 17:33:38	1414	pom-pharmacy.com.	pom-pharmacy.com.	A	104.28.22.110 104.28.23.110
2017-03-14 22:42:18	2014-01-23 22:48:40	7841	com.	pom-pharmacy.com.	NS	duke.ns.cloudflare.com. lily.ns.cloudflare.com.

EXPORT AS CSV

EXPORT AS JSON

API DOCS

Show

25

▼

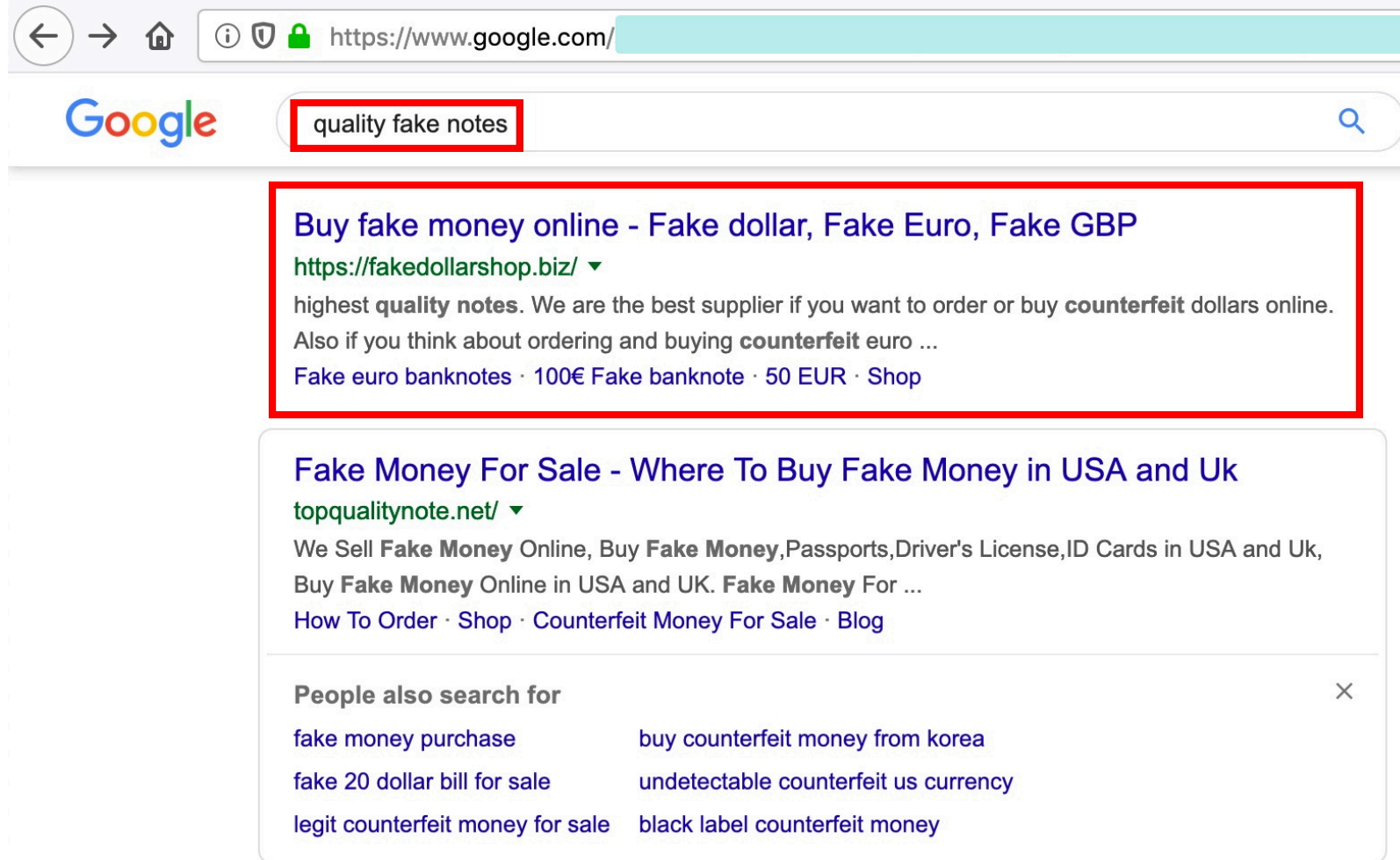
entries

Time Last Seen ▼	Time First Seen	Count	RRname	RRtype	Rdata
2019-05-07 01:28:18	2017-03-16 01:16:29	4130	cialisonlinecl.com.	NS	ns1.seizedservers.com.
2019-05-07 01:28:08	2016-04-25 15:49:20	5949	onlinerx-solutions.com.	NS	ns1.seizedservers.com.
2019-05-07 01:27:57	2017-03-17 19:23:26	3525	eudrg.com.	NS	ns1.seizedservers.com.
2019-05-07 01:27:23	2017-03-17 05:21:50	3925	erowdi.com.	NS	ns1.seizedservers.com.
2019-05-07 01:26:55	2017-03-16 23:21:17	10685	ph-mo.com.	NS	ns1.seizedservers.com.
2019-05-07 01:25:16	2017-03-16 23:04:25	4332	eeepharmacy.com.	NS	ns1.seizedservers.com.
2019-05-07 01:23:48	2017-03-16 14:02:08	12702	alexapharma.com.	NS	ns1.seizedservers.com.
2019-05-07 01:23:35	2019-02-14 21:38:16	2499	srscover.com.	NS	ns1.seizedservers.com.
Copyright 2019 Farsight Security, Inc.					

Threat Hunting Using DNS

Example III. Counterfeit [Currency|Identification|Merchandise|Etc]

Nonetheless, Counterfeit Currency Does Get Advertised Online



Buying High-Quality Counterfeit Money online-Express Documentation

exdocumentation.com/product/buying-high-quality-counterfeit-money-online/

Buying High-Quality Counterfeit Money online. Our fake bank notes are top quality passing the pen



fakedollarshop

HOME SHOP NEWS KNOWLEDGE BASE CONTACT US

LOGIN

CART / \$0.00



SHOP / FAKE DOLLAR BANKNOTES

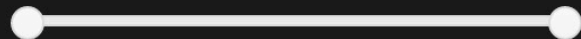
Sort by popularity

BROWSE

Fake dollar banknotes

Fake euro banknotes

Fake pound banknotes



FILTER

Price: \$5 – \$25



FAKE DOLLAR BANKNOTES

10 USD



\$5.00



FAKE DOLLAR BANKNOTES

20 USD

\$9.00



FAKE DOLLAR BANKNOTES

100 USD

\$25.00

What Do We See In DNSDB?

Time Last Seen ▼	Time First Seen	Count	Bailiwick	RRname	RRtype	Rdata
2019-04-11 07:55:35	2018-03-03 16:06:39	2195	fakedollarshop.biz.	fakedollarshop.biz.	A	104.27.170.199 104.27.171.199

Showing 1 to 1 of 1 entries

First	Previous	1	Next	Last
-------	----------	---	------	------

Whois confirms that **those IP addresses are associated with Cloudflare**, a "reverse proxy" provider that acts to conceal the actual location of a web site's web servers.

Cloudflare also intermingles domains from various customers on the same IPs, thereby making it more difficult to identify closely-related domains

Cloudflare is an example of a site that complicates passive DNS-based approaches.

Get a list of Cloudflare nameservers

```
bapril@rd2:~$ dnsdbq -r *.ns.cloudflare.com/A -j | jq -r '.rrname' | sort | uniq | head
abby.ns.cloudflare.com.
adam.ns.cloudflare.com.
ada.ns.cloudflare.com.
adel.ns.cloudflare.com.
adi.ns.cloudflare.com.
adrian.ns.cloudflare.com.
aida.ns.cloudflare.com.
aiden.ns.cloudflare.com.
ajay.ns.cloudflare.com.
alan.ns.cloudflare.com.
bapril@rd2:~$ dnsdbq -r *.ns.cloudflare.com/A -j | jq -r '.rrname' | sort | uniq > cloudflare_ns.txt
bapril@rd2:~$ wc -l cloudflare_ns.txt
401 cloudflare_ns.txt
```

Get domains associated with the NS list

```
bapril@rd2:~$ cat cloudflare_ns.txt | sed -e "s/^/rdata\/name\/" | sed -e "s/$/\/NS/" | dnsdbq -f -l 1000000 -j > cf_domains.json
```

```
bapril@rd2:~$ wc -l cf_domains.json
77911620 cf_domains.json
```

```
bapril@rd2:~$ cat cf_domains.json | sed -e "/^--$/d" | jq -r '.rrname' > cf_domains.txt
```

```
bapril@rd2:~$ wc -l cf_domains.txt
77911219 cf_domains.txt
```

```
bapril@rd2:~$ ls -lha |grep cf_
-rw-r--r--  1 bapril bapril  11G May  8 04:07 cf_domains.json
-rw-r--r--  1 bapril bapril 1.3G May  8 04:20 cf_domains.txt
```



```
bapril@rd2:~$ grep counterfit cf_domains.txt
encounterfit.com.
counterfitsucks.pw.
counterfittersssav.com.
philjohnsonscounterfitters.com.
encounterfit.com.
buycounterfitmoney.online.
buycounterfitmoney.online.
counterfittin.com.
counterfittin.com.
counterfitllc.com.
counterfitllc.com.
counterfittin.com.
counterfittin.com.
counterfitllc.com.
counterfitllc.com.
counterfit.net.
counterfit.net.
counterfit.io.
counterfitsucks.pw.
counterfittersssav.com.
philjohnsonscounterfitters.com.
counterfit.io.
counterfit.net.
counterfit.net.
bapril@rd2:~$
```

```
bestwatchestoyoucenter.com.
bestwatchestoyoureview.com.
cheapwatches2youcenter.com.
cheapwatches2youreview.com.
cheapwatches4mencenter.com.
cheapwatches4menreview.com.
cheapwatches4youcenter.com.
cheapwatches4youreview.com.
shopwatchestoyoucenter.com.
shopwatchestoyoureview.com.
bestwatches4womencenter.com.
bestwatches4womenreview.com.
bestwatchesformencenter.com.
bestwatchesformenreview.com.
cheapwatchestoyoucenter.com.
cheapwatchestoyoureview.com.
mywatchesforwomencenter.com.
mywatchesforwomenreview.com.
shopwatches4womencenter.com.
shopwatches4womenreview.com.
cheapwatches4womencenter.com.
cheapwatches4womenreview.com.
bestwatchesforwomencenter.com.
bestwatchesforwomenreview.com.
finejewelrywatchesandmore.com.
modernwatchesonlinemarket.com.
cheapsmartwatches.net.
replicaswisswatches.net.
rosegoldwatches.xyz.
watchescoupon.info.
dealsondesignerwristwatches.info.
clothingshoesmenswatchesorigin.info.
watchestoday.site.
```

```
canadian-pharmacy.tech.
canadian-trustpharmacy.party.
online-pharmacy.website.
onlineuspharmacy.accountant.
wceappharmacy.com.
shopko-pharmacy.com.
thefacepharmacy.com.
canadianonlinepharmacys.com.
pharmacytechniciansinfo.com.
pharmacytechnicianschoolsusa.com.
gibsonpharmacy.net.
capsulepharmacy.in.
uppharmacypdf.ml.
hotcanadianpharmacy.us.
wceappharmacy.com.
shopko-pharmacy.com.
www.shopko-pharmacy.com.
thefacepharmacy.com.
safe-pharmacy-24.com.
canadianonlinepharmacys.com.
pharmacytechniciansinfo.com.
pharmacytechnicianschoolsusa.com.
gibsonpharmacy.net.
canadianpharmacyonline.top.
bachelorofscienceinpharmacy.xyz.
pharmacytechnicianschoolspa.xyz.
howtobecomeappharmacytechnician.xyz.
onlineschoolsforpharmacytechnician.xyz.
pharmacyplus.date.
```

Limits to Passive DNS

Simple Passive DNS Works GREAT...

- **Lots of related domains coexist on a single IP** (or small CIDR block), with no innocent 3rd party domains
- **Many related domains use the same set of dedicated name servers**, with no innocent 3rd party domains
- **The bad guy is apparently stubbornly fond of a favorite domain**, despite being kicked off provider after provider after provider

Passive DNS has a harder time with:

- **ZERO interrelated data points** – e.g., "lone wolf" or domain names, IP addresses, name servers, etc.
- **TOO many related resources** – CDNs etc.
- Related bad guy resources are comingled inextricably with innocent 3rd party resources.

Limits Inherent to Passive DNS Results

- **Passive DNS is based on observed DNS queries.** While our sensors see most popular DNS names (and many unpopular ones!) no passive DNS service can guarantee that they'll "always" see "everything." ("Absence of evidence is not evidence of absence.")
- Some content may be intentionally filtered from DNSDB for a variety of reasons. Some traffic may be of low value (example: randomized subdomain attack traffic), other traffic may be reveal proprietary information (such as DNS blocklist content), etc.
- Don't put too much weight on reported counts. In particular, be careful of making comparisons between different domains based on counts. Because we collect passive DNS from above large caching recursive resolvers, those counts will be strongly influenced by the time-to-live values used by each domain.
- Domains can "lie" about where they live (if they do lie, the IPs they *claim* to use may not respond, but we don't check that)

Key Takeaways

- Almost everything we do online uses DNS
 - People can use the Internet to lie, but the Internet itself does not.
- Bad guys often will reuse DNS assets for their malicious infrastructures
- Passive DNS reveals subtle relationships among DNS datasets, from domain names to IP addresses to name or mail or web or file servers
- Uncovering shared Internet infrastructure connections can advance investigations, from e-crime to nation-state attacks
- DNSDB API Trial Key is available for commercial use, however LEO and other non-profits can apply for a grant. Farsight is committed to making the Internet safer for all users.
- Running a sensor and contribute data.
- Additional resources: DNSDB® Get Started Guide (<https://www.farsightsecurity.com/get-started-guide>)
- Have questions? Contact vixie@fsi.io or bapril@fsi.io

Questions

@bapril

bapril@fsi.io