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/](https://paterva.com/) part of the transform hub.

- **Dnsdbq** – [https://github.com/dnsdb/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 It is already outdated.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>
  ...relied 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](http://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

- DNS Key = {QNAME, QCLASS, QTYPE}
- pDNS key = {QNAME, QCLASS, QTYPE, RDATA, bailiwick}
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.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/
Threat Hunting Using DNS

Example I. Phishing
This is "probably" **NOT** PayPal!
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
### DNSDB Scout

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

<table>
<thead>
<tr>
<th>Time Last Seen</th>
<th>Time First Seen</th>
<th>Count</th>
<th>Bailliwick</th>
<th>RRname</th>
<th>RRtype</th>
<th>Rdata</th>
</tr>
</thead>
</table>

Showing 1 to 2 of 2 entries
bapril@rd2:$ dnsdbq -r paypal-care.serveirc.com
;; 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
paypal-care.serveirc.com. A 129.213.120.15
Threat Hunting Using DNS

Example II. Fake-Pharma
Pom-Pharmacy.com

Site Self-Description
POM Pharmacy

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
Visa, Mastercard, American Express, PayPal, Bitcoin

Alexa Popularity
8488791
### Successful Query for: pom-pharmacy.com A (Limit 50000)

<table>
<thead>
<tr>
<th>Time Last Seen</th>
<th>Time First Seen</th>
<th>Count</th>
<th>Bailiwick</th>
<th>RRname</th>
<th>RRtype</th>
<th>Rdata</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-08-17 22:23:15</td>
<td>2016-02-15 00:10:04</td>
<td>1921</td>
<td>pom-pharmacy.com</td>
<td>pom-pharmacy.com</td>
<td>A</td>
<td>185.92.221.211</td>
</tr>
</tbody>
</table>

Showing 1 to 5 of 5 entries
## Successful Query for: pom-pharmacy.com ANY (Limit 50000)

### Table of Data

<table>
<thead>
<tr>
<th>Time Last Seen</th>
<th>Time First Seen</th>
<th>Count</th>
<th>Bailiwick</th>
<th>RRname</th>
<th>RRtype</th>
<th>Rdata</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Last Seen</td>
<td>Time First Seen</td>
<td>Count</td>
<td>RRname</td>
<td>RRtype</td>
<td>Rdata</td>
<td></td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------</td>
<td>-------</td>
<td>-------------------</td>
<td>--------</td>
<td>----------------------------</td>
<td></td>
</tr>
</tbody>
</table>
Threat Hunting Using DNS

Example III. Counterfeit [Currency|Identification|Merchandise|Etc]
Nonetheless, Counterfeit Currency **Does Get Advertised Online**
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 webservers.

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

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

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

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

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

```bash
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
```
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 3\(^{rd}\) party domains

- **Many related domains use the same set of dedicated name servers**, with no innocent 3\(^{rd}\) 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