Mapping Adversary Infrastructure Using DNS

Merike Kaeo, CTO
merike@fsi.io

FARSIGHT SECURITY
DISCUSSION POINTS

• Introduction to Passive DNS
• Using pDNS for Fighting Fraud
• Protecting Against Phishing / SPAM
• Key Takeaways
PASSIVE DNS HISTORY

• 2004: Florian Weimer reconstructs DE zone through passive monitoring
  – Presents at FIRST meeting
  – BFK.de
• 2008: Security Information Exchange created
  – ncapptool
  – nmsgttool
• 2010: Create DNSDB to also track historical information
DNS FUNDAMENTALS

- root
  - com
    - infinera
  - org
    - ciena
    - icann
    - geant
  - eu
    - europa
      - codeweek
    - ... etc ...
  - gTLD
    - ... etc ...
  - enisa
DNS RECURSION (CACHE MISS)

“I want to visit tnc17.geant.org”
DNS RECURSION

“I want to visit tnc17.geant.org”

Caching Recursive DNS Server

tnc17.geant.org A?
A 145.0.2.31

f.root-servers.net

a0.org.afilias-nst.info

lon-ns0.geant.net
PASSIVE DNS – WHAT IS COLLECTED

Collecting responses “above” the recursive nameserver

Reconstruct current state of DNS passively

Passive DNS and Privacy:
https://www.farsightsecurity.com/assets/media/download/passive-dns-privacy.pdf
WATERFALL PROCESSING

“Loosely-coupled multi-processor”
SOME DNS STATISTICS

- **278 Million** Current Domain Names
- **100+ Million** ccTLD Domains
- **10+ Billion** Current Hostnames

Questions That Can Be Answered Using Passive DNS

- Where did this domain name point to in the past?
- What domain names are hosted by a given nameserver?
- What domain names point into a given IP network?
- What subdomains exist below a certain domain name?
- What new names are hosted in ccTLDs?
Most cybercrime involves IP addresses and domain names

- **Controlled Substance Sales**: web sites (or email addresses) used to sell narcotics and other dangerous drugs
- **Hacking/Cracking**: sites used to scan for vulnerable hosts, stepping stone hosts used to login to unpatched hosts, etc.
- **Knock-off Merchandise**: online stores selling replica merchandise
- **Malware**: check in hosts, C&C hosts, 2nd stage downloaders
- **Online Child Abuse Materials**: email accounts, file sharing sites
- **Phishing**: look-alike web sites, phishing email reply-to addresses
- **Spam**: spambot C&Cs, handoff hosts, spamvertised URLs
CORRELATING INFORMATION

• Criminals want to protect against service interruptions
  – systems being seized/hosting services getting disabled
  – domain names being seized/put on hold
  – network connectivity getting cut
  – affiliates proving themselves untrustworthy, etc

• Using multiple domains and multiple IP addresses
  – efforts to "fly under the radar"/avoid looking "too prominent"
  – load balancing (some of these guys operate at *scale*)
  – SEO (bad guys compete for search engine rankings just like legitimate businesses)
CRIMINALS SHARE INFRASTRUCTURE

• Reasons for sharing
  – Limited number of evil infrastructure providers to choose from
  – Bad guys tend to "trade notes" on the providers that work well for them
  – Evil infrastructure may be premium-priced; incent cost sharing

• Benefits to good guys
  – When you're chasing one bad guy, you may bump into others
  – If you focus is on one type of badness, you may run into other unrelated illegal content, which can require jurisdictional coordination/deconfliction
FIGHTING FRAUD

Dolce & Gabbana
Sicily Medium Floral Cameo Textured Leather Top-Handle Satchel

0400087343914

Write a Review
Q & A: Ask a Question

Color: White-Black

$2995.00

ADD TO BAG

Details

Dolce & Gabbana’s signature Sicily satchel is beautifully updated with an array of contrasting floral appliqués, each dotted with shimmering crystals or cameo studs for a look that's vintage inspired yet modern and fresh.

- Top handle, 3.5” drop
- Removable, adjustable crossbody strap, 19”-26” drop
- Snap flap closure
- Protective metal feet
- Goldtone hardware
- One inside zip pocket
FIGHTING FRAUD: FAKE?
voguebags.cn Whois Info

Domain Name: voguebags.cn
ROID: 20151118s10001s78437261-cn
Domain Status: ok
Registrant ID: hc7296611749622
Registrant: 梁龙锦
Registrant Contact Email: 1607897117@qq.com
Sponsoring Registrar: 阿里云计算有限公司（万网）
Name Server: dns10.hichina.com
Name Server: dns9.hichina.com
Registration Time: 2015-11-18 08:30:29
Expiration Time: 2016-11-18 08:30:29
DNSSEC: unsigned
**WHERE IS SITE LOCATED?**

-- If we dig for www.voguebags.cn ➔ 46.17.100.18

-- Following that IP's whois:

<table>
<thead>
<tr>
<th>inetnum:</th>
<th>46.17.100.0 - 46.17.103.255</th>
</tr>
</thead>
<tbody>
<tr>
<td>netname:</td>
<td>HOSTKEY-NET</td>
</tr>
<tr>
<td>person:</td>
<td>Shevchenko Andrey</td>
</tr>
<tr>
<td>address:</td>
<td>Tussen de Bogen 6, 1013 JB Amsterdam, The Netherlands</td>
</tr>
<tr>
<td>phone:</td>
<td>+31 20 820 3777</td>
</tr>
<tr>
<td>nic-hdl:</td>
<td>ANSH31-RIPE</td>
</tr>
<tr>
<td>abuse-mailbox:</td>
<td><a href="mailto:abuse@hostkey.nl">abuse@hostkey.nl</a></td>
</tr>
</tbody>
</table>
OTHER DOMAINS ON 46.17.100.18

abercrombieskleppolska.com.  
billigaabercrombiefitch.com.  
billigmonclergermany.com.  
cheapdiedelnuewjeans.com.  
cheapnewbalancebuy.com.  
classicbirkenstocksale.com.  
famosasgfasrayban.com.  
giubbottimonclerroma.com.  
hermesbrandbags.com.  
magasinnmulberrysac.com.  
marcjacobscomprar.com.  
monclergermanyoutlet.com.  
monclermagyar.com.  
northfacenegozi.com.  
oakleyssolbrilleronline.com.  
poloralphlaurenkaufen.net.  
replicabagsgood.cn.  
scarpeairmaxdonna.com.  
scarpejordanbasket.net.  
soldeskarenmillen.com.  
timberlandprecios.net.  
ugglesbottes.com.  
verkaufmanoloblahnik.com.  
[etc]
$ dnsdb_query.py -l 1000000 -i 46.17.100.0/24 > 46.17.100.0.txt

$ wc -l 46.17.100.0.txt
   34384 46.17.100.0.txt
$ more 46.17.100.0.txt
ns1.wsmp.biz. IN A 46.17.100.21
ns2.wsmp.biz. IN A 46.17.100.21
ns1.warezmarket.biz. IN A 46.17.100.21
ns2.warezmarket.biz. IN A 46.17.100.21
[etc]

$ awk '{print $1}' < 46.17.100.0.txt | 2nd-level-dom | reverse-domain-names | sort -u > output.txt

$ wc -l output.txt
   14779 output.txt
$ more output.txt
ar.com.1stmadly
ar.com.3mligatures
[etc]
pDNS FINDS OTHER DOMAINS ON THAT IP

com.2012chanelbag
com.2012chanelbagsforsale
com.2013guccibagsoutlet
com.bagslongchampoutlet
com.bagslongchampuk
com.bagsmulberryoutletuk
com.bagsmulberrysaleuk
com.bestcoachbagjapan
com.bestpradabagjp
com.buymulberrybag
com.celinebaggujp
com.celinebaggusale
com.chanelbagonlinejapan
com.chanelbagoutletjapan
com.chanelbags-onlineeshop
com.chanelbagsshop
com.chanelbagtojp
com.chanelbagyo
com.chanelhandbags-2012outlet
com.cheapchanelbagjapan
com.coachbagjp2012
com.coachbagonsalejapan
com.coachbagpop
com.coachbagshopjapan
com.coachbagsja
com.coachhandbags-onsale
com.coachhandbagsoutletsx
com.guccibagsjan
com.gucci bagsoutletnl
com.handbagsmulberryuk
com.hermesbrandbags
com.longchambagsaleuk
com.longchampbagsinusale
com.longchampbaggssaleaustralia
com.louisvuittonhandbag-eshop
com.lvbagonsalejapan
com.mulberrybagsaleukonline
com.mulberrybagstore
com.nbagamesstore
com.nbagamestore
com.nbagoodstore
com.nbagoodstore
com.newlouisvuittonhandbagsoutlet
com.popmulberrybag
com.pradabagguoutlet
com.pradabaggusale
com.pradabagonsalejapan
com.pradaoutletbagsjp
com.replicabags-1
com.replicahandbags-1
com.russibags
com.selllvbag
com.topchanelbagoutlet
info.louisvuittonbagsonlinesale
net.brand Chanelhandbags
org.bagslongchampuk
org.lcbags
org.longchampaustraliabagsonline
org.longchampbagoutlet
org.longchampbagnolinesaleaustralia
org.longchampbagsaleaustralia
org.longchampbagsuksale
org.longchampoutletbag
org.longchampoutletbagsale
org.longchampoutletbagsale
uk.co.bagslongchampuk
uk.co.bagsmulberryuk
uk.co.longchampbagnolinesale
uk.co.louisvuittonhandbagsoutlet
USING pDNS TO COMBAT FRAUD

- An easily identified starting point can be developed into a large number of related and apparently infringing domains
- By resolving those domains, we can then find additional IP addresses involved with the apparently infringing behavior, and those IP will often yield additional domains of interest
  - Find an initial lead
  - Resolve that domain to an IP
  - Find additional domains on that IP using passive DNS
  - Resolve those additional domains to IPs
  - Find additional domains on those new IPs using passive DNS
DETECTING PHISHING SCAMS

- Many domain names are long established
- Newly observed domains and hostnames are worthy of careful scrutiny

```bash
$ nmsgtool -C ch213 -o - | grep -f phishing-strings.txt | grep -v -f whitelist.txt
```

- The `phishing-strings.txt` file might contain frequently phished terms, such as: account, login, patch, update, etc
- The `whitelist.txt` file might contain strings matching domains we believe to be unlikely to be associated with phishing, such as: .akadns.net., .edgekey.net., .fbcdn.net., etc
EMAIL – CHECK SPAM SENDER DOMAIN

DNSDB Demo Web Interface

- Record Type: ANY
- Result Limit: 50
- IDN/Punycode: Encode
- Search Mode: RRSet
- Search: hzjw11.hzw.com
- Bailiwick: example.com

SEARCH
## INITIAL RESULTS

**Query #1: RRset: hzjw11.hzjw.com ANY [Adv]**

Returned 4 RRsets in 1599 ms at 2017-05-31 01:12:22

<table>
<thead>
<tr>
<th>RRset ID</th>
<th>First Seen</th>
<th>Last Seen</th>
<th>Count</th>
<th>Bailiwick</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>#1</td>
<td>2017-03-25</td>
<td>2017-03-25</td>
<td>2</td>
<td>hzjw.com</td>
<td>50.117.113.222</td>
</tr>
<tr>
<td>#2</td>
<td>2016-07-28</td>
<td>2016-08-02</td>
<td>35</td>
<td>hzjw.com</td>
<td>103.51.144.81</td>
</tr>
<tr>
<td>#3</td>
<td>2016-07-28</td>
<td>2017-02-23</td>
<td>91</td>
<td>hzjw.com</td>
<td>1 mail.skrimple.com</td>
</tr>
</tbody>
</table>
### IPs ASSOCIATED WITH mail.skrimple.com

<table>
<thead>
<tr>
<th>#</th>
<th>First Seen</th>
<th>Last Seen</th>
<th>Count</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2016-03-14 15:50:16</td>
<td>2016-03-27 22:18:10</td>
<td>3807</td>
<td>23.21.54.75</td>
</tr>
<tr>
<td>2</td>
<td>2015-01-03 16:47:12</td>
<td>2015-01-20 08:07:23</td>
<td>15203</td>
<td>23.21.60.79</td>
</tr>
<tr>
<td>3</td>
<td>2016-03-02 16:38:51</td>
<td>2016-03-09 18:40:22</td>
<td>2383</td>
<td>23.21.60.140</td>
</tr>
<tr>
<td>4</td>
<td>2014-12-29 11:32:59</td>
<td>2015-01-06 02:04:43</td>
<td>8350</td>
<td>23.21.60.194</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>23.21.245.63</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>23.23.104.175</td>
</tr>
</tbody>
</table>
### Query #3: mail.skrimple.com (Reverse)

Returned 10000 RRsets in 4013.5 ms at 2017-05-31 01:13:02

<table>
<thead>
<tr>
<th>#1, first seen: 2016-07-29 09:56:44, last seen: 2016-07-29 09:56:44</th>
<th>count: 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>london.ac.</td>
<td>MX 1 mail.skrimple.com</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>#2, first seen: 2014-12-30 03:12:33, last seen: 2014-12-30 03:12:33</th>
<th>count: 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>ku.ac.ac.</td>
<td>MX 1 mail.skrimple.com</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>#3, first seen: 2014-12-27 02:34:36, last seen: 2014-12-28 06:00:00</th>
<th>count: 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>pi.ac.ac.</td>
<td>MX 1 mail.skrimple.com</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>#4, first seen: 2014-12-28 15:21:23, last seen: 2014-12-30 01:00:00</th>
<th>count: 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>zu.ac.ac.</td>
<td>MX 1 mail.skrimple.com</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>#5, first seen: 2014-12-28 02:49:35, last seen: 2014-12-30 01:00:00</th>
<th>count: 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>adu.ac.ac.</td>
<td>MX 1 mail.skrimple.com</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>#6, first seen: 2014-12-30 01:00:11, last seen: 2014-12-30 01:00:11</th>
<th>count: 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>students.adu.ac.ac.</td>
<td>MX 1 mail.skrimple.com</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>agu.ac.ac.</td>
<td>MX 1 mail.skrimple.com</td>
</tr>
</tbody>
</table>
INTERESTING DOMAIN

Query #6: 176zaohuadajipinchuanqi.bgj.cc. (Reverse)
Returned 0 RRsets in 4647.6 ms at 2017-05-31 01:17:31

Query #5: 176zaohuadajipinchuanqi.bgj.cc. (Forward)
Returned 3 RRsets in 28210.5 ms at 2017-05-31 01:17:54

176zaohuadajipinchuanqi.bgj.cc. A 103.51.144.81

176zaohuadajipinchuanqi.bgj.cc. MX 1 mail.skrimple.com.

176zaohuadajipinchuanqi.bgj.cc. TXT "v=spf1 ip6:fd0d:d741:e183::/48 -all"
### Query #8: gaoerfuduboxianjinqipailm0.9gg.cc. (Forward)

| #1, first seen: 2016-08-28 16:25:05, last seen: 2016-08-28 16:25:05 | count: 2 | balliwick: 9gg.cc. | gaoerfuduboxianjinqipailm0.9gg.cc. | A | 69.46.84.52 |
| #2, first seen: 2016-12-20 18:04:21, last seen: 2016-12-20 18:04:21 | count: 2 | balliwick: 9gg.cc. | gaoerfuduboxianjinqipailm0.9gg.cc. | CNAME | num9.dcoin.co. |
| #3, first seen: 2016-08-28 16:25:05, last seen: 2016-08-28 16:25:05 | count: 2 | balliwick: 9gg.cc. | gaoerfuduboxianjinqipailm0.9gg.cc. | MX | 1 mail.skrimple.com. |
| #4, first seen: 2016-08-28 16:25:05, last seen: 2016-08-28 16:25:05 | count: 2 | balliwick: 9gg.cc. | gaoerfuduboxianjinqipailm0.9gg.cc. | TXT | "v=spf1 ip6:fd0:d741:e183::/48 -all" |
USING pDNS TO LOOK AT SPAM/PHISHING

• A starting point can be developed into a large number of related and apparently suspicious looking domains
• By resolving those domains, we can then find additional IP addresses, MX records, etc that could yield additional domains of interest
• It is useful to correlate suspicious domains and/or IP addresses with known blacklist information to ascertain additional information that could lead to more conclusive information.
CONCLUDING THOUGHTS

- Real time pDNS data can be useful for immediate issues needing timely response
  - Domain hijacks
  - Reputation for newly observed domains
- Historical pDNS database is often used for criminal investigations and determining the full extent of a malicious campaign
QUESTIONS ?