DRAVis

Visualizing Domain Reputation & Attribution

Terry Nelms, Kulsoom Abdullah, & Joshua Kimball

Team 13

Motivation

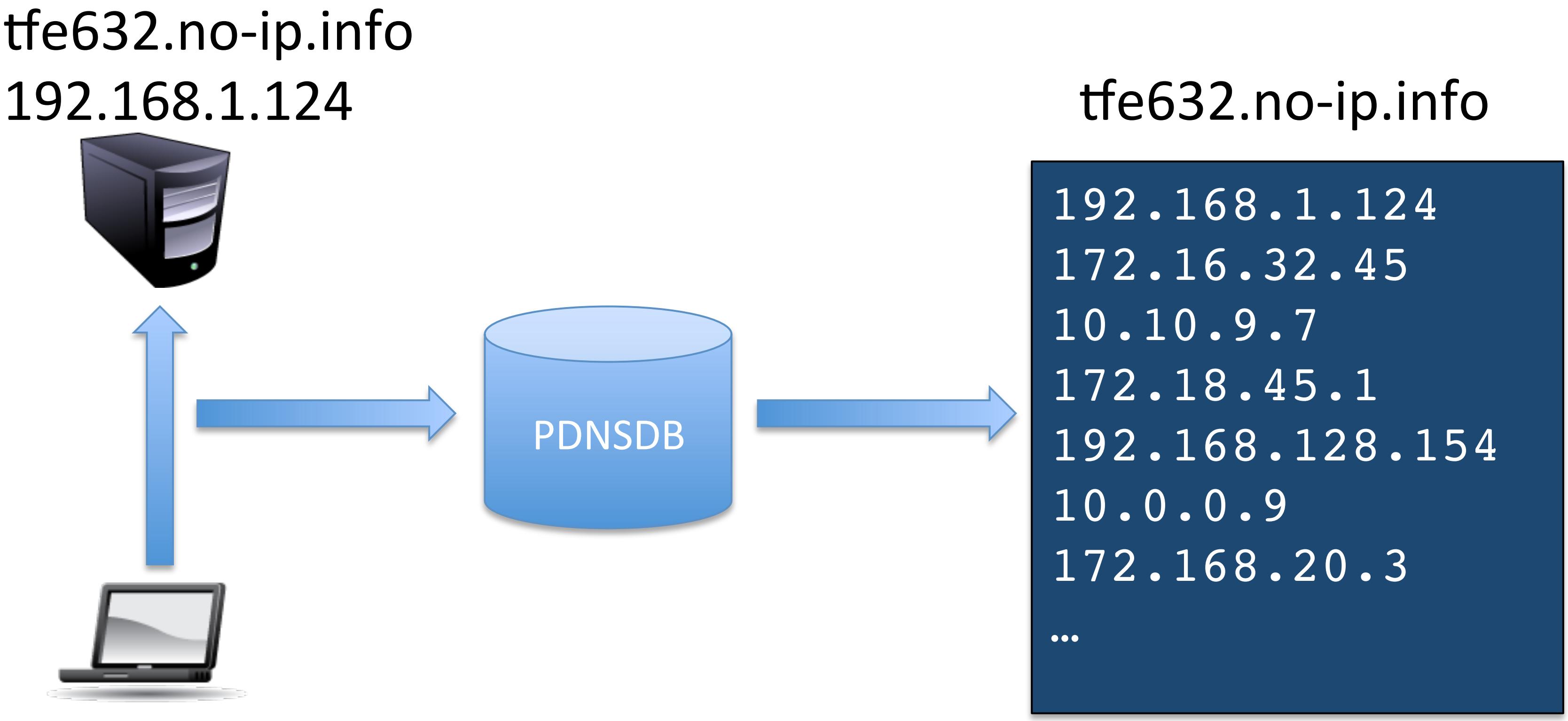
- Malicious domains are agile.
  - Avoid takedown.
  - Avoid blacklisting.
- Leverage DNS agility for reputation & attribution.
  - Cluster domains on their network relationships.
  - Visualize the most important relationships.

Data – Passive DNS

```
qrl89y666z.tang.la
p5ctnvqyd3.myftp.org
5opskttv3y.serveblog.net
tzeh62imx.informatix.com.ru
0zd2bwqqyu.no-ip.info
2ndk2swdma.madhacker.biz
pe4d0t35bs.no-ip.info
5c0x3re4vr.zapto.org
seqkhgd4pj.logout.us
zkycgbn8es.serveblog.net
a4669k3.spacetechnology.net
s45223a.tang.la
0098.no-ip.info
Sbdat.servevlog.net
0few3kd4yv.mooo.info
…
```

- Numbers
  - **22 Billion** per day.
  - **8 Trillion** per year.
- DNS Records
  - ISPs
  - Telcos
  - Enterprises

pDNSDB - Related Historic IP Addresses



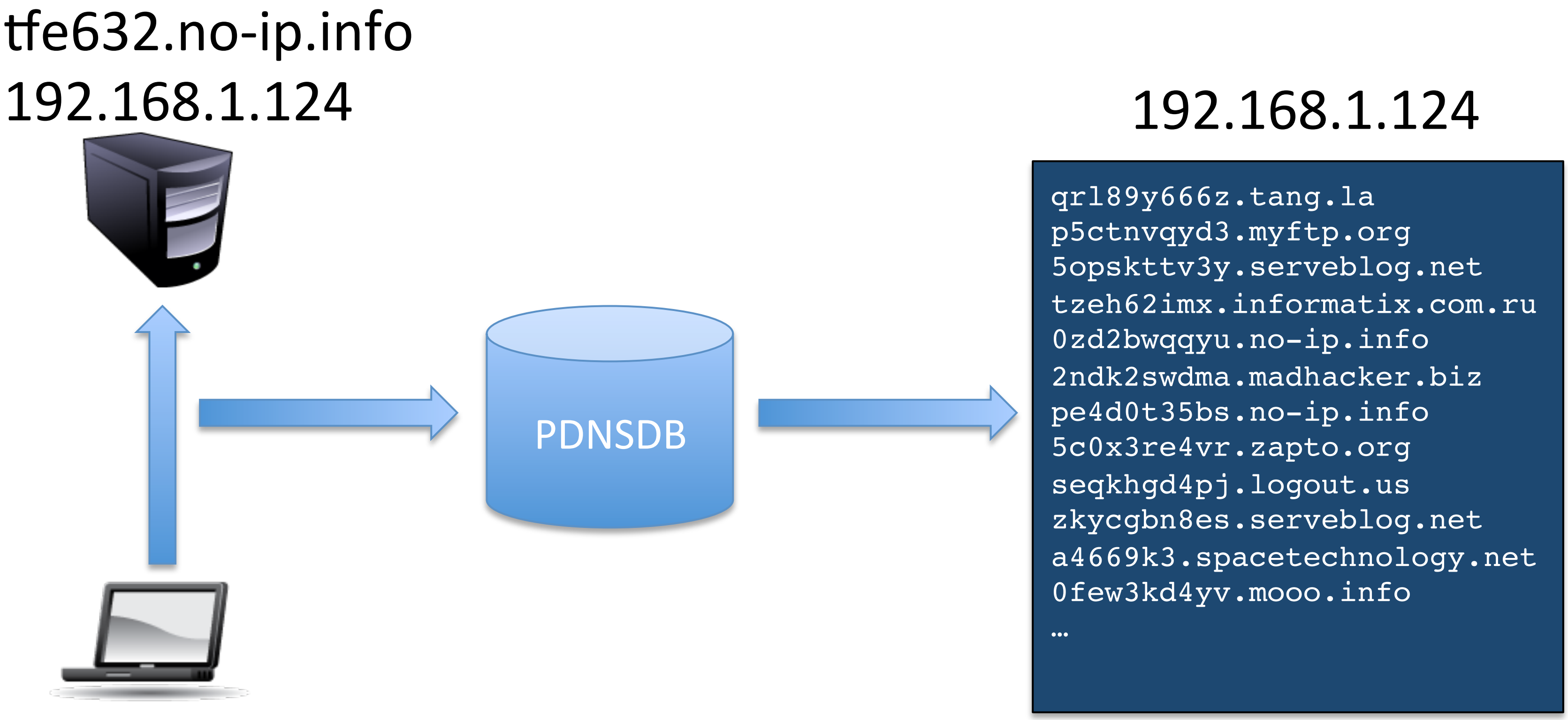
tfe632.no-ip.info
192.168.1.124

PDNSDB

tfe632.no-ip.info

192.168.1.124
172.16.32.45
10.10.9.7
172.18.45.1
192.168.128.154
10.0.0.9
172.168.20.3
…

pDNSDB - Related Historic Domain Names



tfe632.no-ip.info
192.168.1.124

192.168.1.124

```
qrl89y666z.tang.la
p5ctnvqyd3.myftp.org
5opskttv3y.serveblog.net
tzeh62imx.informatix.com.ru
0zd2bwqqyu.no-ip.info
2ndk2swdma.madhacker.biz
pe4d0t35bs.no-ip.info
5c0x3re4vr.zapto.org
seqkhgd4pj.logout.us
zkycgbn8es.serveblog.net
a4669k3.spacetechnology.net
0few3kd4yv.mooo.info
…
```

Clustering

- Features.
  - Total IPs & networks.
  - IP address, BGP prefix, ASN, country code.
- Algorithm.
  - K-means.
  - sparse matrix.
- Domain annotation.
  - Identify cluster with domain of interest.
  - Label blacklist domains.
  - Euclidean distance from domains in cluster.

Visualization Demo

Evaluation

- Pulled 9 “unlabeled” domains to investigate
- Using clustering and statistics about clusters to make a decision about “unlabeled” domain
- Looked up these domains in 5+ reference sources: hpHosts, Damballa, Google, Sucuri and Honeypot
- Compared decisions of analyst to these reference sources to determine accuracy
- Results: 1 False Negative and 1 False Positive, All others matched correctly

Conclusion

- Initial evaluation led analyst to correctly classify approximately 80% of the “unlabeled” domains
- Generally, clustering and visualization is a good approach for this problem:
  - Only mechanism to communicate & analyze inordinately large, complex structures, i.e. IP networks
    - More levels of indirection exponentially increases the number of nodes in the graph
  - Helps to improve accuracy, reliability of blacklists. [Blacklists are created for different purposes; seeing blacklisted firms in or near one cluster is helpful.]
  - Reveal new, potentially interesting features: hyphenated names, # of total blacklist / # of domains in combined cluster

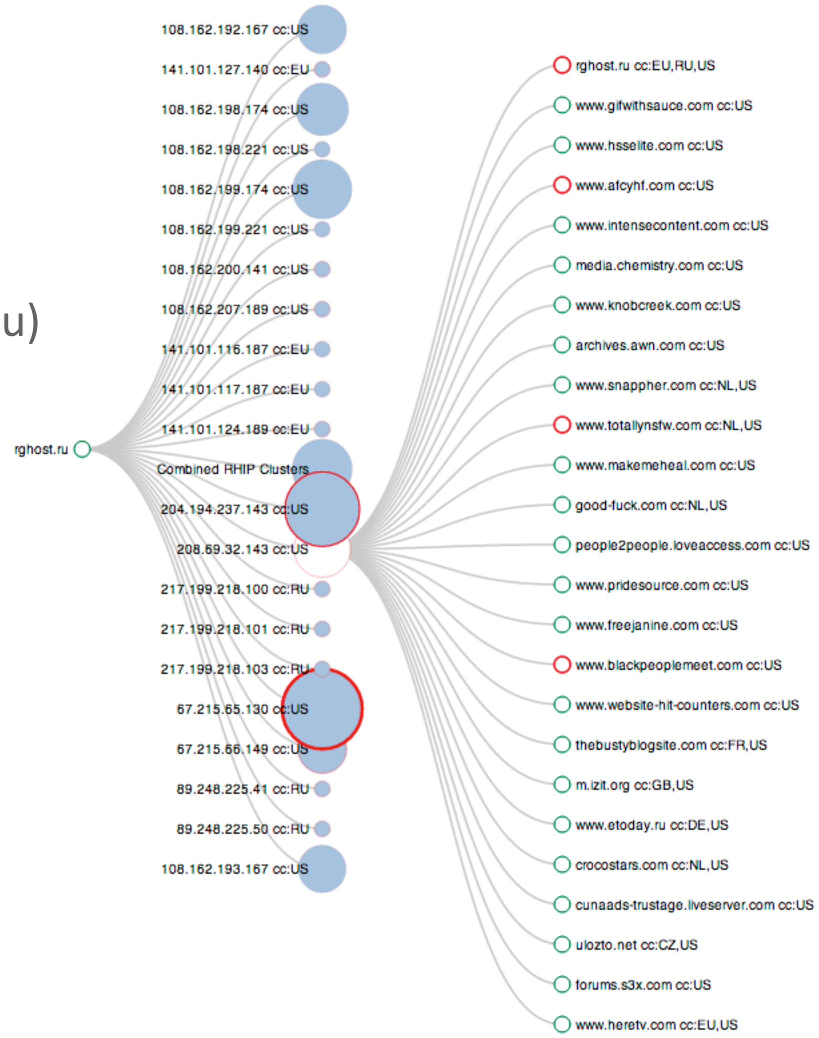
Future Work

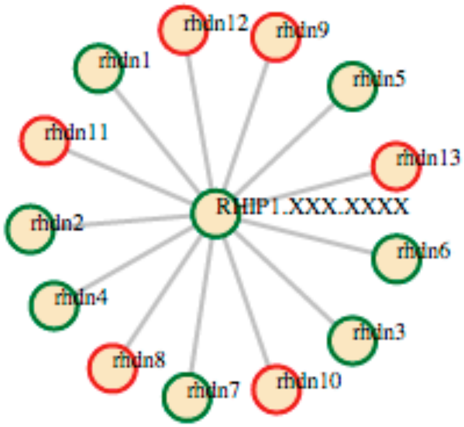
- More evaluation!
  - Needs to encompass larger evaluation data set
- Build infrastructure to handle 2 additional levels of indirection for a given domain of interest
  - This adds MM of nodes to the graph
- More features based on network structure needed like different measures of centrality
  - Agility of attacks lends itself to examining network-based features

Thank You!

Team 13

Terry Nelms (tnelms@gatech.edu)
Kulsoom Abdullah (kulsoom@gatech.edu)
Joshua Kimball (jmkimball@gatech.edu)


rghost.ru
108.162.192.167 cc:US
141.101.127.140 cc:EU
108.162.198.174 cc:US
108.162.198.221 cc:US
108.162.199.174 cc:US
108.162.199.221 cc:US
108.162.200.141 cc:US
108.162.207.189 cc:US
141.101.116.187 cc:EU
141.101.117.187 cc:EU
141.101.124.189 cc:EU
Combined RHIP Clusters
204.194.237.143 cc:US
208.69.32.143 cc:US
217.199.218.100 cc:RU
217.199.218.101 cc:RU
217.199.218.103 cc:RU
67.215.65.130 cc:US
67.215.66.149 cc:US
89.248.225.41 cc:RU
89.248.225.50 cc:RU
108.162.193.167 cc:US
rghost.ru cc:EU,RU,US
www.gifwithsauce.com cc:US
www.hsselite.com cc:US
www.afcyhf.com cc:US
www.intensecontent.com cc:US
media.chemistry.com cc:US
www.knobcreek.com cc:US
archives.awn.com cc:US
www.snappher.com cc:NL,US
www.totallynsfw.com cc:NL,US
www.makemeheal.com cc:US
good-fuck.com cc:NL,US
people2people.loveaccess.com cc:US
www.pridesource.com cc:US
www.freejanine.com cc:US
www.blackpeoplemeet.com cc:US
www.website-hit-counters.com cc:US
thebustyblogsite.com cc:FR,US
m.izit.org cc:GB,US
www.etoday.ru cc:DE,US
crocostars.com cc:NL,US
cunaads-trustage.liveserver.com cc:US
ulozto.net cc:CZ,US
forums.s3x.com cc:US
www.heretv.com cc:EU,US


rhdn12
rhdn9
rhdn1
rhdn5
rhdn11
rhdn13
RHIP1.XXX.XXXX
rhdn2
rhdn6
rhdn4
rhdn3
rhdn8
rhdn7
rhdn10