THREAT HUNTING USING PASSIVE DNS

Investigation & Analysis

Presented by Dr. Paul Vixie with Guest Speaker from Deloitte's Threat Intelligence & Analytics Team
Scott Keoseyan

FARSIGHT SECURITY

INTRODUCTIONS

Dr. Paul Vixie

- Chairman, CEO and Cofounder of Farsight Security Inc
- Former President, Chairman and Founder of Internet Systems Consortium (ISC), President of MAPS, PAIX and MIBH, CTO of Abovenet/MFN, and on the boards of several for-profit and non-profit companies.
- Inducted into the Internet Hall of Fame in 2014 for work related to DNS

Scott Keoseyan

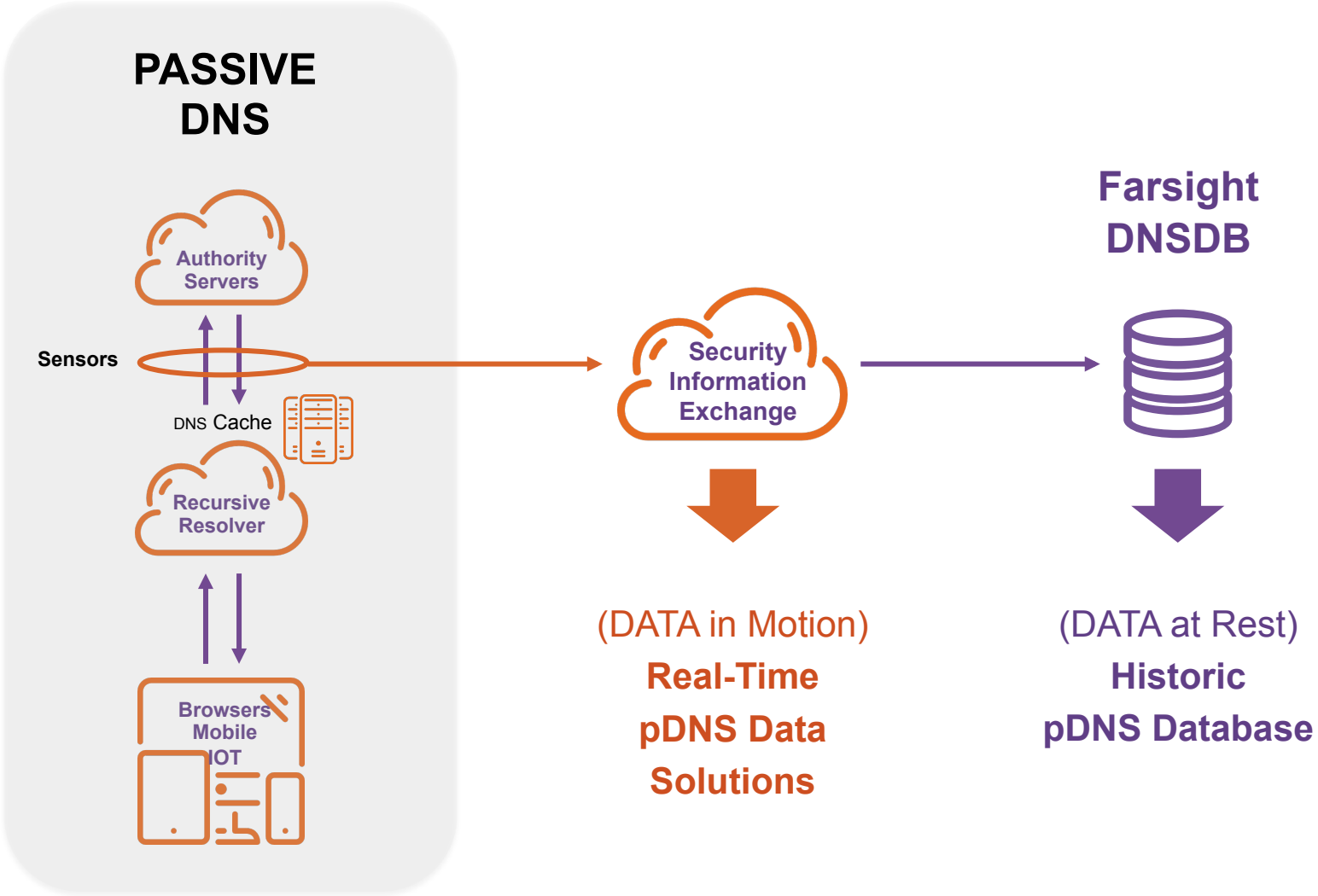
- Chief Technology Officer supporting Deloitte & Touche LLP's Vigilant Services
- Leading multiple cyber-security assessments and breach response engagements.
- Former deputy CISO for Fortune 100 Bank – Capital Markets Group
- One of Fortune 100 Bank's Cyber Security Principal Engineers

VIRTUALLY ALL CYBERCRIMES INVOLVE IPs AND/OR 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 (Command & Control), handoff hosts, spamvertised URLs
- And much more

These IPs or domain names provide a starting point/initial clue...

FARSIGHT SECURITY'S UNIQUE PERSPECTIVE



MOST CYBERCRIMINALS USE MORE THAN JUST ONE IP/DOMAIN

- **The bad guys want to protect themselves against service interruptions due to...**
  -- 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 IPs can also help...**
  -- 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)

- **We* want to find ALL related tentacles of a criminal enterprise to avoid "incomplete takedown" issues**

*We/us in this context (and in this presentation) means a threat analyst, incident responder or a security professional

PASSIVE DNS *EXCELS* AT FOLLOWING CONNECTIONS...

- If you find a domain, it can be resolved to an IP
  - **Passive DNS can tell you all the other domains that are also on that IP**
- Every domain has name servers
  - **Passive DNS can tell you all the other domains that use the same nameservers**
- If an evil host hops from IP to IP, you can see the IPs it is using
  - **Checking past IPs can lead to additional connections**

- Sometimes passive DNS may find what seems like an overwhelming number of results. Fortunately, you can also limit passive DNS results by
  - **A cap on max results** (if you know you never want more than N results)
  - **Time boundaries** ("show me just results from the last month")
  - **Record types** ("I only care about 'A' records" perhaps)
  - **Bailiwick** ("What's a bailiwick?" Please see http://homepage.ntlworld.com/jonathan.deboynepollard/FGA/dns-server-bailiwick.html)

pDNS – STARTING POINT FOR INVESTIGATION

Why do we start with Passive DNS for investigation?

- **Looking at an IP** – easily and rapidly distinguish between a web-host, a park-page, versus potential criminal infrastructure
- **Looking at a domain** – rapidly identify key aspects such as fluidity of infrastructure (fluxing on fixed or fluid # of IPs), DNS server stability, domain stability-age (time on infrastructure), and other "reputation" aspects needed to help assess threat and nature

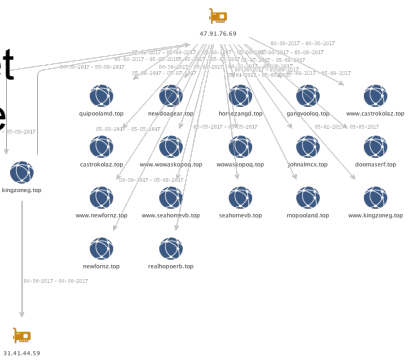
Point is – driving context into what we're looking at helps us understand its nature and enables us to make better decisions faster

You can learn a lot about a person by looking at who they hang around with. You can learn a lot about a domain by looking at it's neighbors, too

INVESTIGATION AND AUTOMATION REQUIREMENTS

Must have command-line access so we can write automation as needed

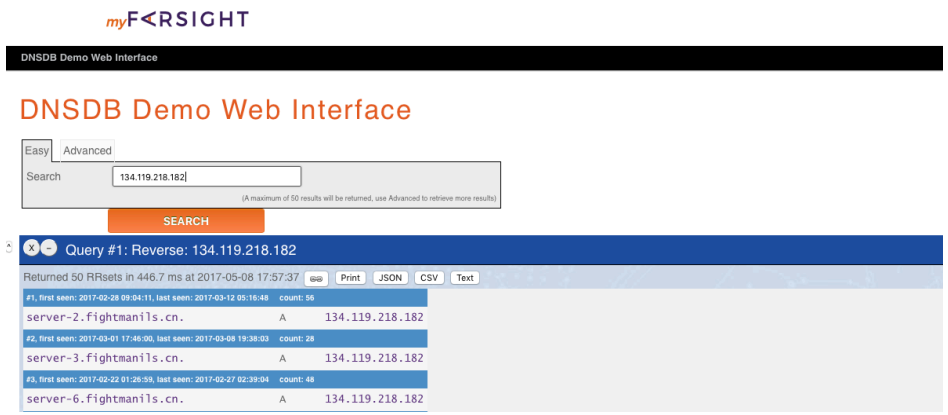
```
1. bash
snarky$ while read line ; do python dnsdb_query.py -c ../../../dnsdb-query.conf  -i $line ; done
 < <(cat suspicious_ip.txt)
server-2.fightmanils.cn. IN A 134.119.218.182
server-3.fightmanils.cn. IN A 134.119.218.182
server-6.fightmanils.cn. IN A 134.119.218.182
server-8.fightmanils.cn. IN A 134.119.218.182
server-9.fightmanils.cn. IN A 134.119.218.182
server-10.fightmanils.cn. IN A 134.119.218.182
server-13.fightmanils.cn. IN A 134.119.218.182
server-1.actionfilms.de. IN A 134.119.218.182
server-2.actionfilms.de. IN A 134.119.218.182
server-3.actionfilms.de. IN A 134.119.218.182
server-4.actionfilms.de. IN A 134.119.218.182
server-5.actionfilms.de. IN A 134.119.218.182
server-6.actionfilms.de. IN A 134.119.218.182
server-7.actionfilms.de. IN A 134.119.218.182
server-8.actionfilms.de. IN A 134.119.218.182
server-9.actionfilms.de. IN A 134.119.218.182
server-10.actionfilms.de. IN A 134.119.218.182
server-13.actionfilms.de. IN A 134.119.218.182
server-2.musicforlove.de. IN A 134.119.218.182
server-3.musicforlove.de. IN A 134.119.218.182
server-5.musicforlove.de. IN A 134.119.218.182
```



We need a way to integrate pDNS into the tools we use to help perform and track investigations

Link analysis toolset (like Maltego is nice to have too!

Lastly, we always need a way to simply “look things up” (AKA a human using a web-browser)



INVESTIGATING BULLETPROOF HOSTING USING PDNS

We (now) know that a **bulletproof hosting** service (BPH) is providing a criminal reverse proxy service is leveraging widely used cloud-providers' infrastructure to deliver his service…

First, the threat – why do we care?

- Cloud provider abuse desks trying to play catch-up with an actor who is multiple steps ahead of them and their business processes – the reality is they cannot keep up!
- Popular cloud services cannot be dealt with at the IP level – blocking an IP might not make sense when you're hosting your own infrastructure there
- The criminal activities and the associated responses makes the infrastructure fluid and difficult to deal with and track – oh, and it's not just ransomware!
  - Cerber and other ransomware variants
  - Downloaders, trojans, and mobile malware
  - Cybercrime forums, card-shops, counterfeit goods marketplaces
  - Scanning, DDoS botnet activities, and other recon-based activities

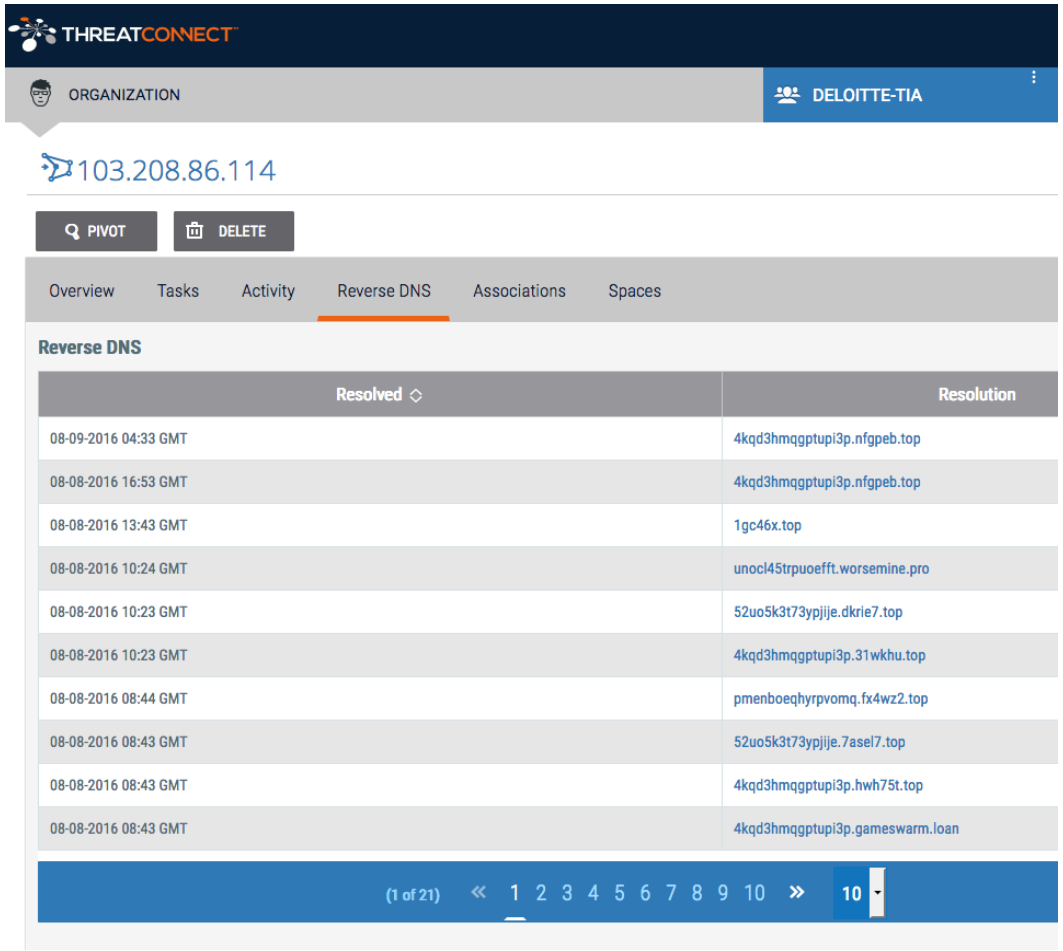
Point is – BPH is a supporting service for multiple threats targeting us that we need to be able to understand and respond to in a tactical manner in order to address

.

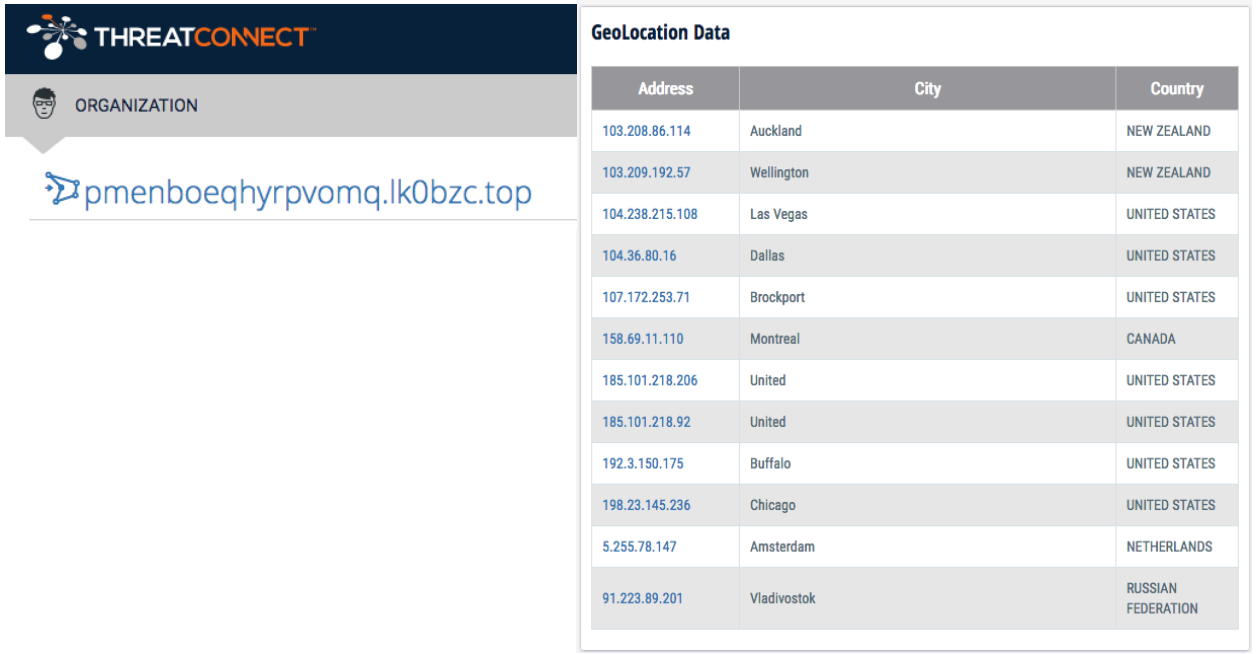
..but how did we get there to begin with?

WE STARTED WITH WRIST-WATCHES…

Last summer, Deloitte identified a nexus between a significant number of domains being registered in the [.]top and .bid TLD that were being specifically used to support Cerber ransomware campaigns. The nexus started off with dozens of email addresses being used to register these domains – and these were hosted across dozens of common IP addresses and shifted rapidly

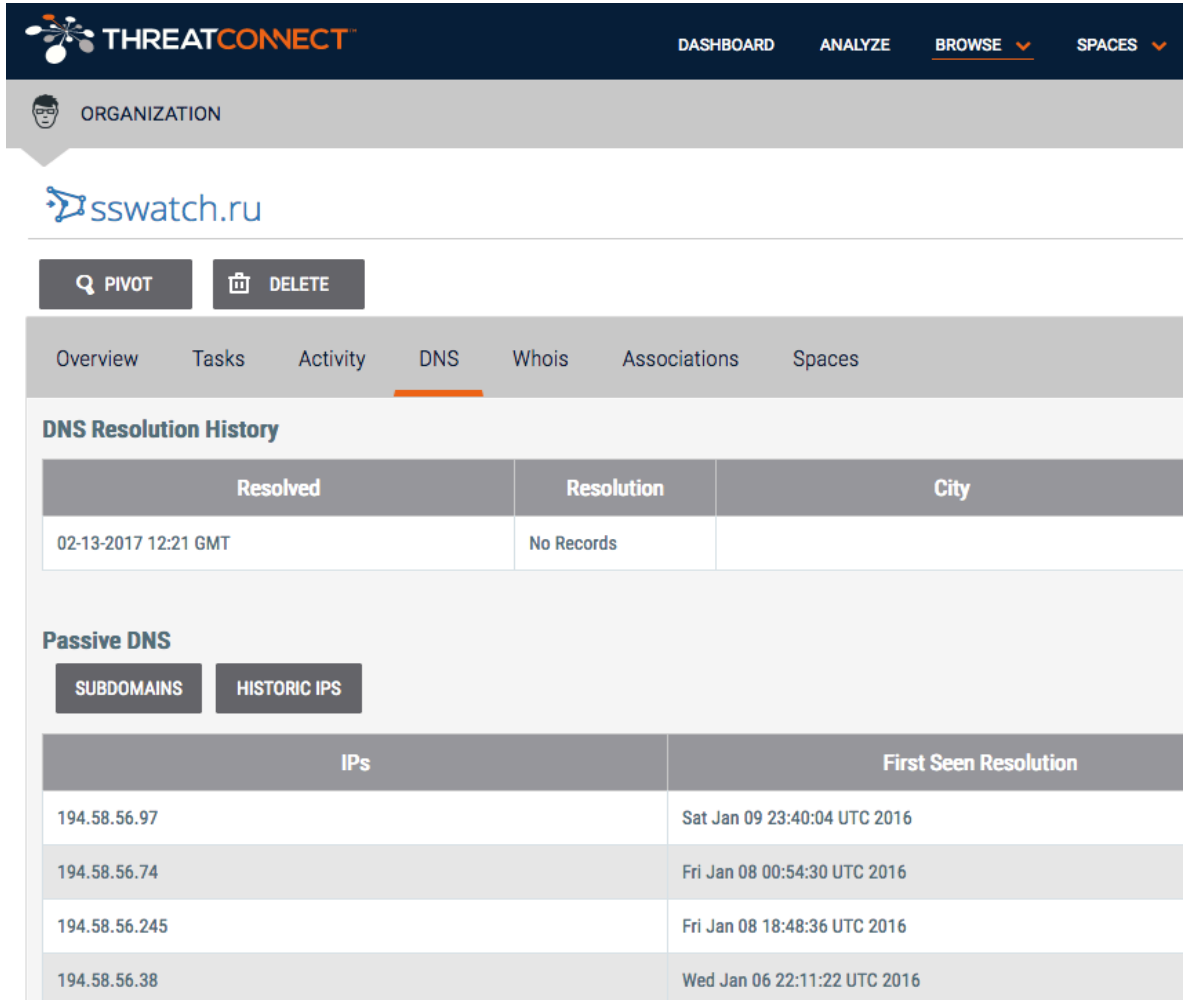


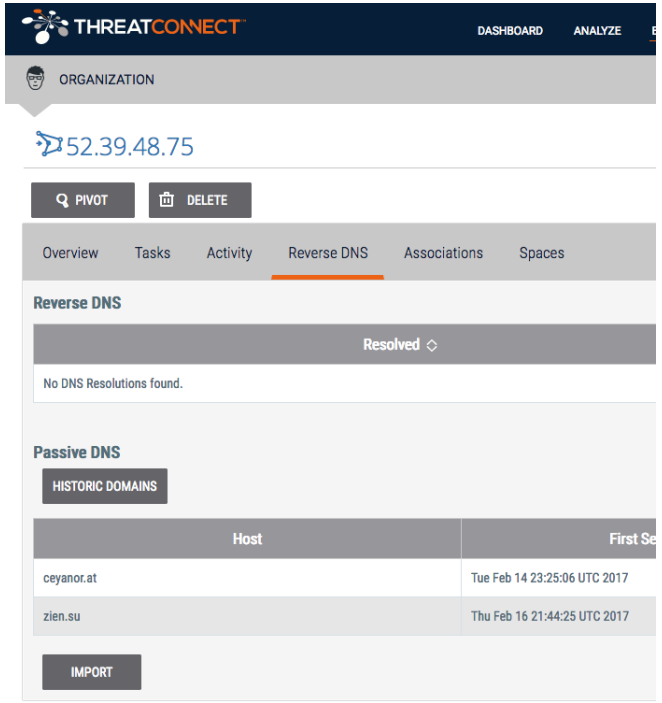
Using passive DNS at first, to pivot off of and identify infrastructure being leveraged, then moving to active DNS tracking on the domains in question, we were able to identify both infection and payment domains that had been, were being, and going to be used in these campaigns



BUT YOU SAID WRIST WATCHES!

One of the domain registrants that kept popping up (we'll call him Alex for now) seemed to be going beyond simply registering Cerber domains, and moved towards some other activities – look-alike/typo-squatting domains for banks, and then in December 2016, typo-squatting domains for some very popular wrist-watch brands as well…





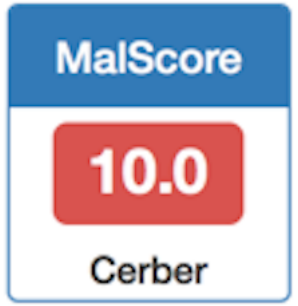
Suddenly, the domains we were tracking for Cerber, and the techniques used for hosting them, shifted toward registering all the domains under a handful of emails, and the IP infrastructure away from widely-distributed VPS providers in dozens of data-centers, to one or two large cloud infrastructure providers

SO TODAY… AN EXAMPLE OF HOW WE WORK

Step 1. Identifying new campaigns via malware or spam analysis

Inbound spam leads us to a downloadable binary. Submit this binary to a sandbox and see where this leads…

Uh oh… the domain “kingzoneg[.]top” is being used to support Cerber ransomware as a recovered sample makes DNS queries and a URL request for this domain



47.91.76.69:80 (kingzoneg.top)	GET	/admin.php?f=404	GET /admin.php?f=404 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: kingzoneg.top Connection: Keep-Alive ⇄ 200 OK

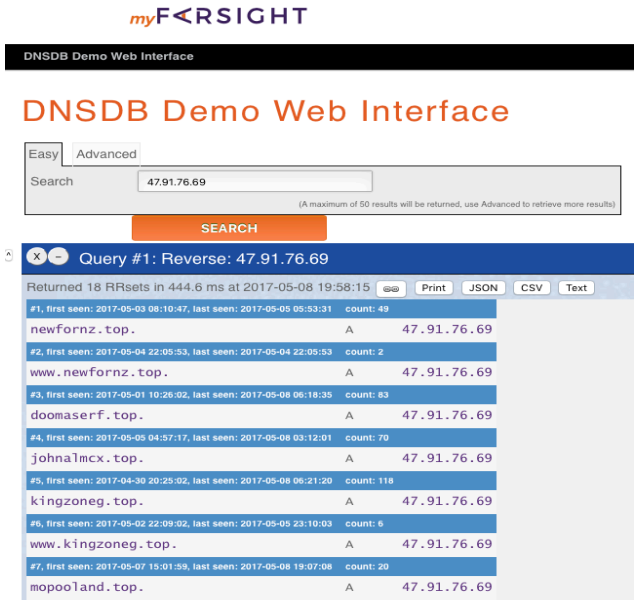
So knowing that kingzoneg[.]top is resolving to **47.91.76[.]69** is interesting, but where has it resolved to and is it linked to anything else we can pivot or track off of?

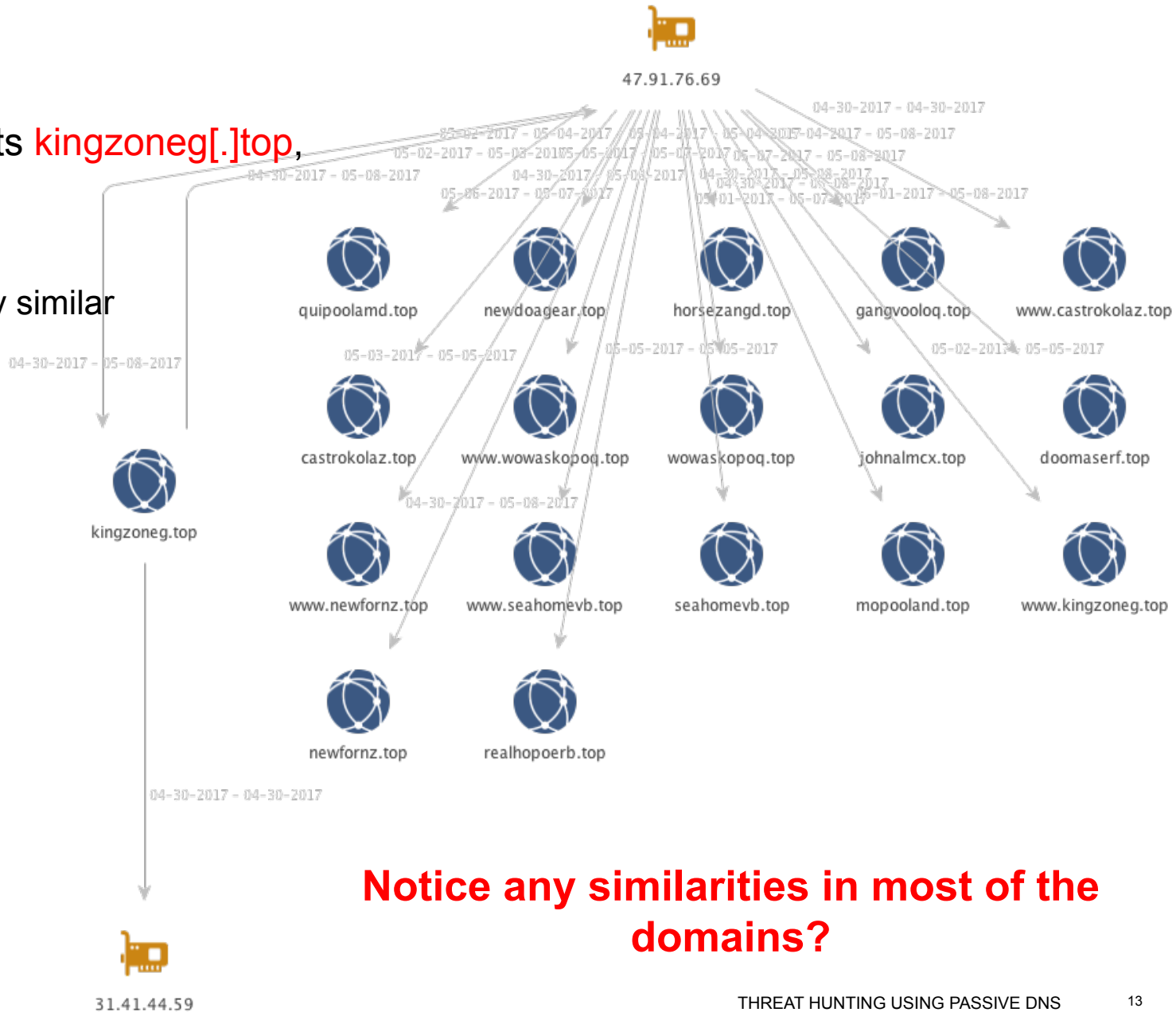
PIVOT INTO PDNS

Step 2. Pivot further out

We've established that 47.91.76[.]69 hosts kingzoneg[.]top, a known Cerber ransomware domain:

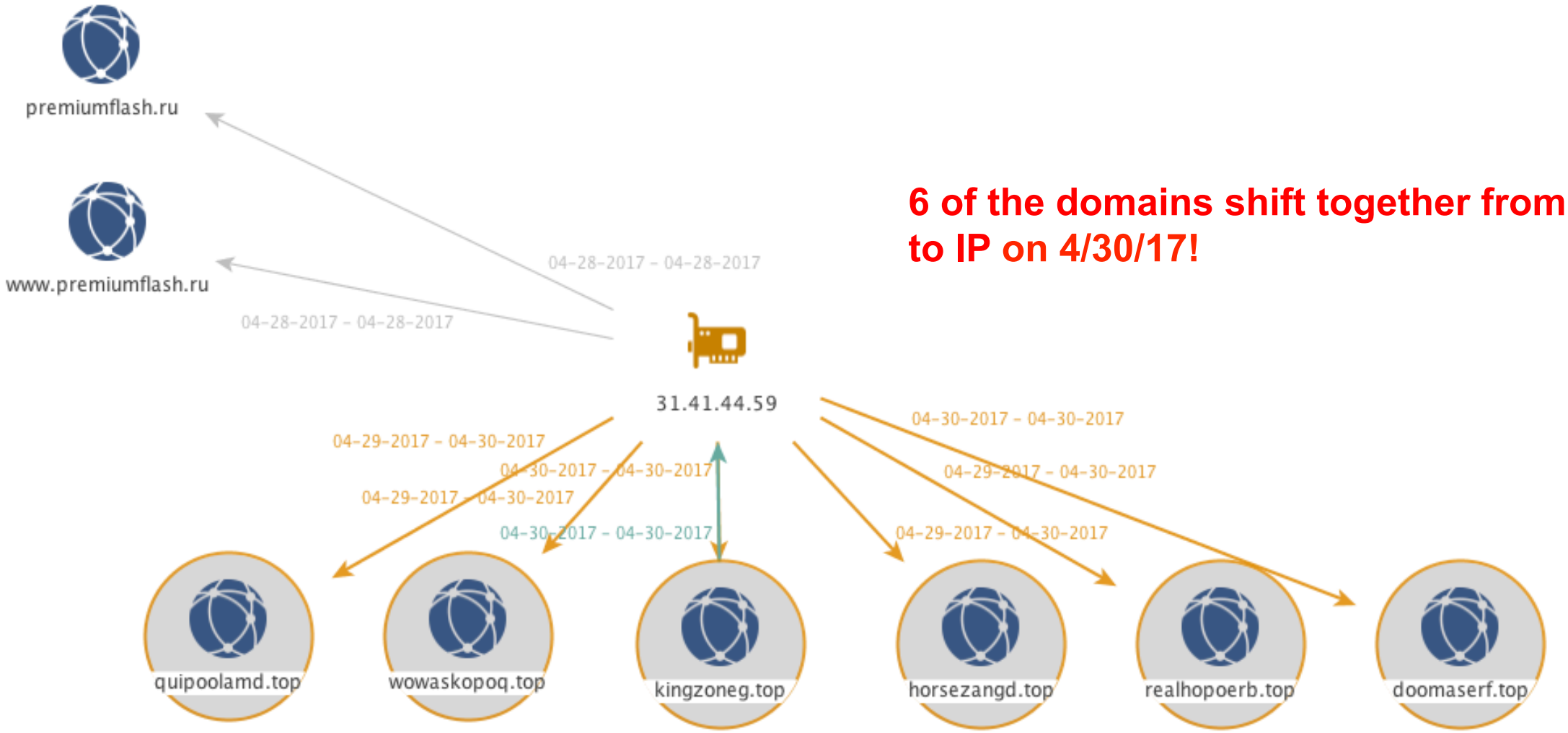
- What else does it host?:
  - a lot of other domains that look very similar
- Where else has it been hosted?:
  - Recently seen on 31.41.44[.]59
  - What was hosted there?





Notice any similarities in most of the domains?

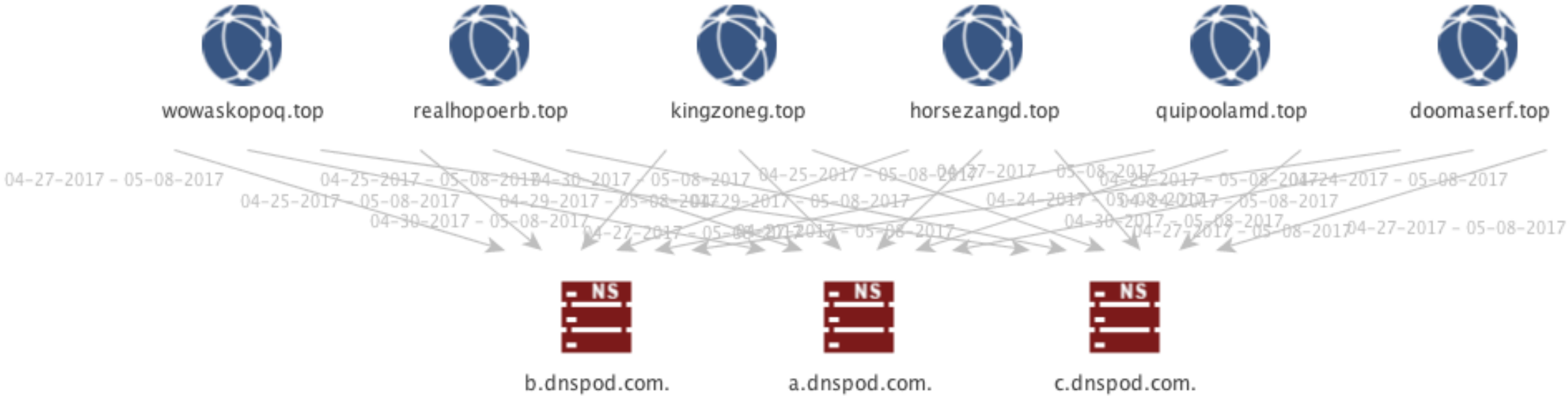
Shifting IP Addresses



6 of the domains shift together from IP to IP on 4/30/17!

WHAT ELSE CAN PDNS TELL US?

All 6 domains share the same DNS infrastructure!

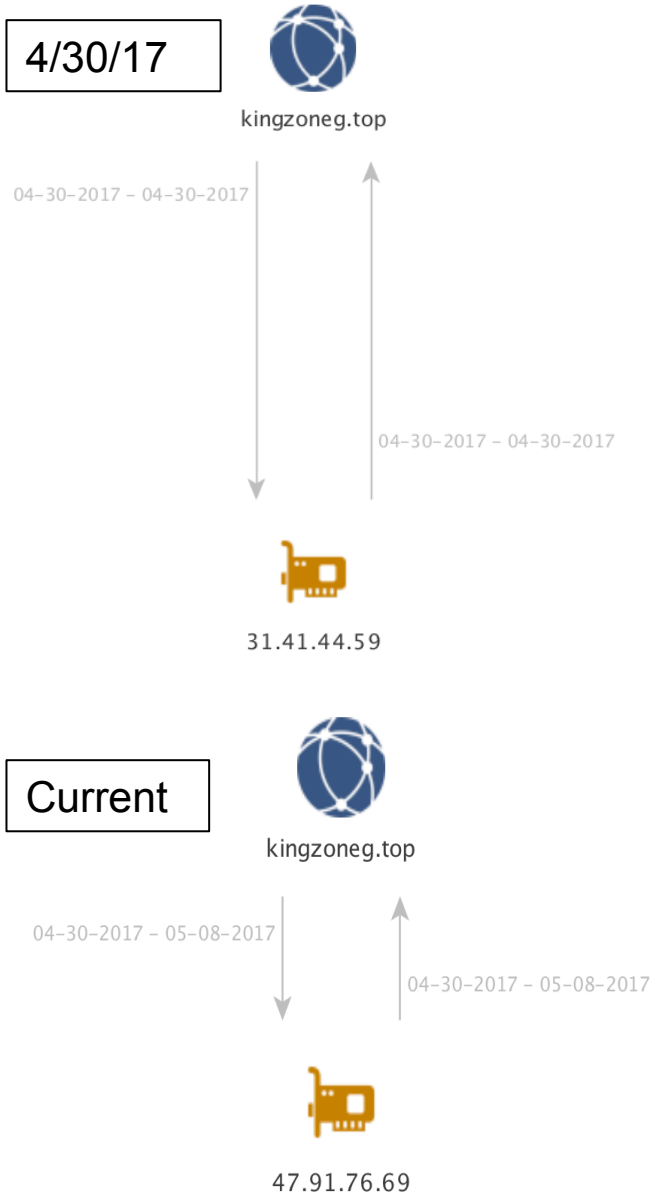


This is not a trivial observation – the facts are adding up quickly that these domains are all connected to one another, and the only data source we've explored is passive DNS!

ANALYSIS

Step 3. Analysis and Inference

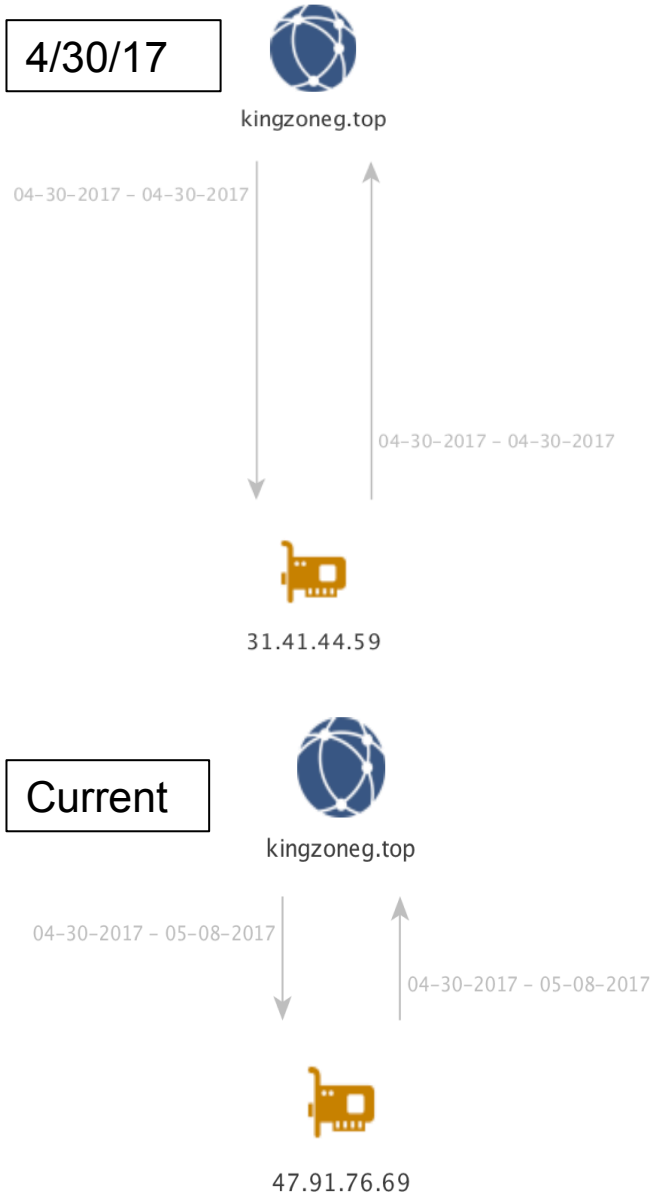
- Thanks to pDNS we are able to immediately see the following similar-looking domains that we can investigate and tie back to the threat:
  - realhopoerb[.]top, horsezangd[.]top, quipoolamd[.]top, doomaserf[.]top. wowaskopoq[.]top and (our original) kingzoneg[.]top
- We can see that when kingzoneg[.]top shifted addresses on 4/30, the others shifted too
- They all share the same DNS infrastructure
- We haven't looked – but can we assume they're all registered by the same person?
- These domains are all likely tied to Cerber (confirmed)
- The BPH provider possibly lost control of the original address (31.41.44[.]59) and simply shifted everything over to a new address they already controlled – no loss of service for the criminals
- These addresses are used for little else, so this is not a CDN, a webhost, or other similar situation – ***traffic to these IPs is highly suspicious***!



ANALYSIS - CONT

Step 4. Action

- Perform a look-back analysis in our SIEM (Security Information Event Management System) to determine communications to 31.41.44[.]59 for the week of 4/30/17
- Consider blocking access to these domains from our enterprise
- Consider alerting on communications to the associated IP
- Track where these domains go next to ensure we're blocking and monitoring on a continual basis
- Evaluate newly discovered domains hosted on 47.91.76[.]69 for additional threats (premiumflash[.]ru also looks dodgy)



CONCLUSIONS (WHAT DID WE LEARN TODAY?)

- Passive DNS allows us to rapidly distinguish between a web hosting IP and dedicated/subverted infrastructure…
  - ***Result – better/faster time to respond and identify the context of an indicator***
  - ***Result – faster response means better security outcomes in the long-run***
- Passive DNS allows us to find additional things we need to watch out for.
  - ***Result – we can now alert/block on a broader set of indicators with confidence!***
- Using a pDNS source (like Farsight) with flexible and open integration options helps us go ***faster!***
  - ***Lots of options for integration and automation!***

Q&A

Thank you for your attention.

QUESTIONS?

Resources:

Response Policy Zone(RPZ)

https://dnsrpz.info/

https://www.farsightsecurity.com/2016/07/06/molloy-nodrpz/

https://www.farsightsecurity.com

Response Rate Limiting in DNS (DNS RRL)

http://www.redbarn.org/dns/ratelimits

FARSIGHT SECURITY

This presentation contains general information only and Deloitte is not, by means of this presentation , rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation .

As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.