SHRESHTA IT

Threat hunting using DNS

APNIC 52 - 14th September 2021

@pswapneel

TLP:WHITE

$whoami

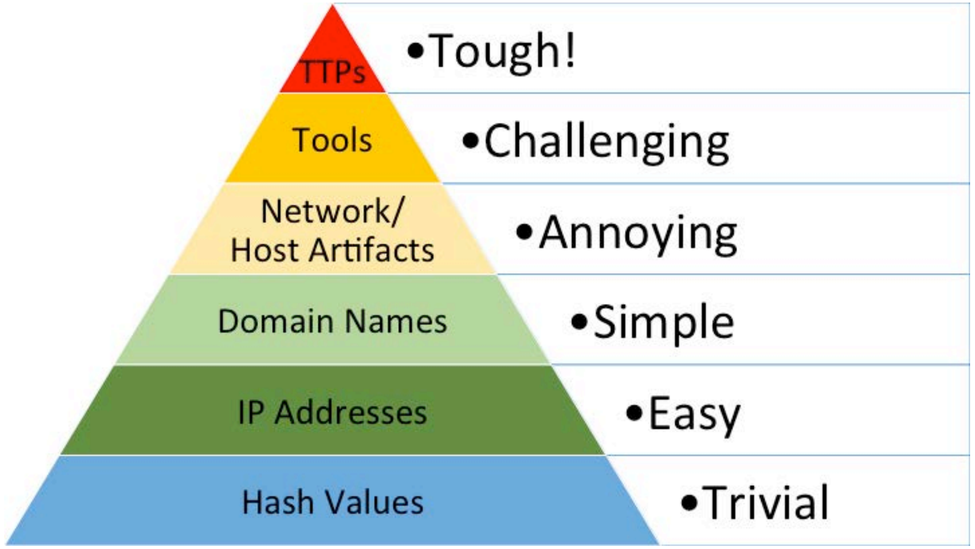
- Chief Network Security engineer and CEO @ Shreshta IT - 15+ years in Information Security
- APNIC Community Trainer
- @pswapneel
- swapneel.patnekar@shreshtait.com

Background

- At $dayjob, we implement Network Security Monitoring(NSM) & DNS Firewalls (Response Policy Zones)
  - 200+ recursive resolvers
- Networks - Network operators, enterprise networks
- Recursive resolver software - BIND9, Unbound

Pyramid of Pain

- Everything on the Internet begins with a DNS query
- Domain names are cheap and used by malware
- Using DNS as layer of defence - Economical layer in a multi-tiered security defense
- Atomic indicators in DNS are a great source for threat hunting!



Source: https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Finding anomalies

Source - Mohan Thomas / https://twitter.com/GetMohanThomas/status/1408309926460477441?s=20

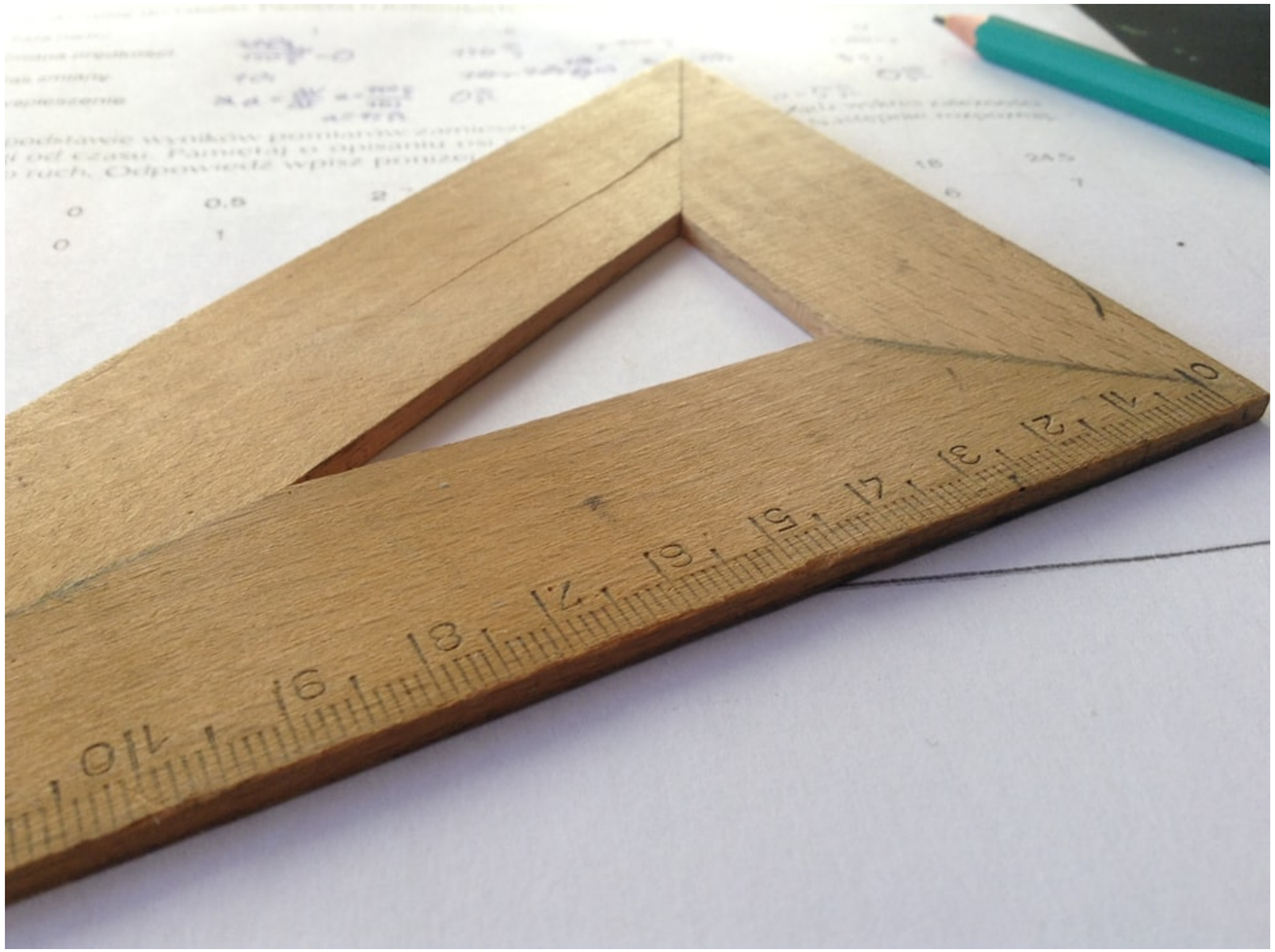
Anomalies

- DGA’s
- Fast flux
- Newly registered domains
- Look alike domains
- Punycode domains

Source: https://www.porterblepeople.com/2015/03/finding-your-material-dropbox-and-devonthink/

Baselining your environment

- On-premise email server in the infrastructure will result in a lot of DNS PTR
- Web browsing will be DNS A, AAAA, CNAME
- What is triggering the NXDOMAIN and NULL responses ?



Source: @djmalecki / Unsplash

Malware 🔗🛸

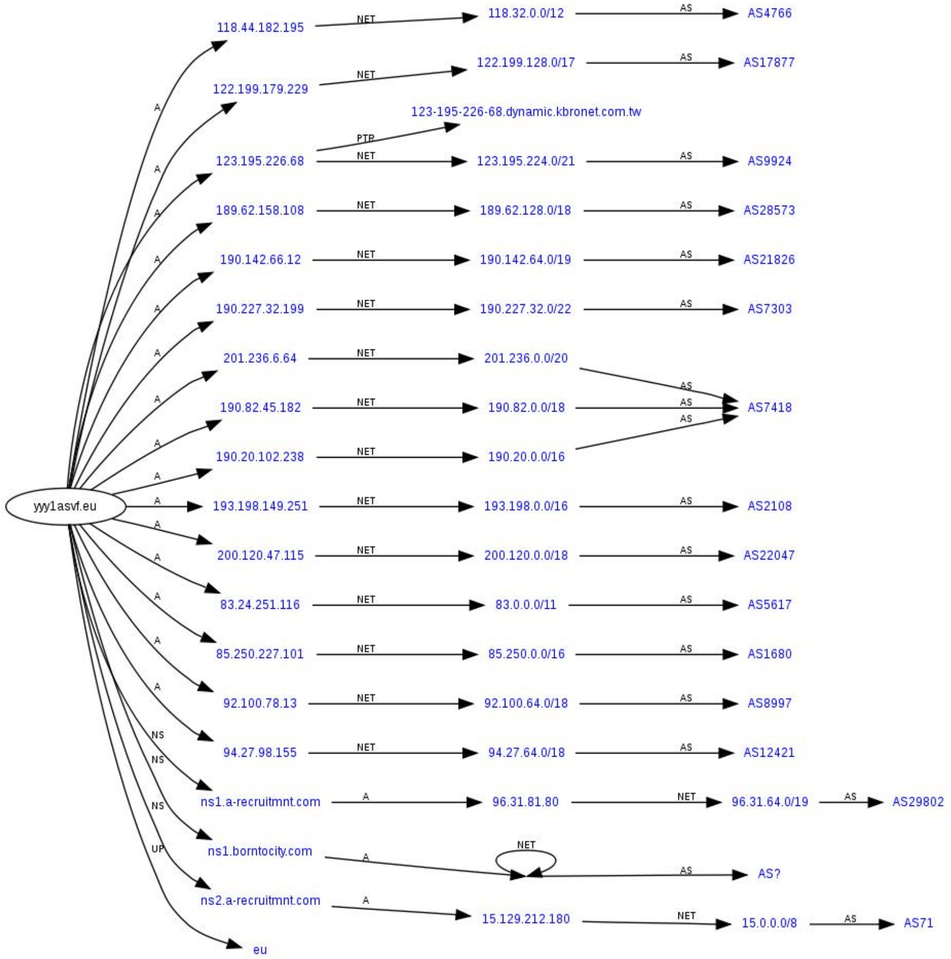
Domain Generation Algorithm (DGA)

- Malware connects to it’s C2C using a single/few domains - Defence implies blocking the malicious domains
- DGA - On the fly generation of new domain names for the malware to connect to (C2C)
- Detection becomes more work for network defenders

PC @nasa / Unsplash

Fast flux

- Domain name points to rapid changing IP address where the IP addresses are swapped in and out with extremely high frequency
- The real attacker network sits behind compromised hosts which are used as proxy
- Mitigation is by blocking the domain but detection is key



Source: https://en.wikipedia.org/wiki/Fast_flux

Punycode domains

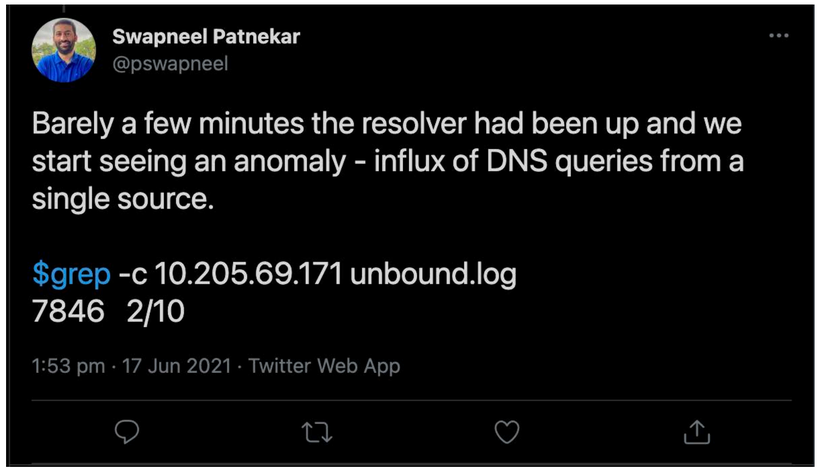
- Punycode is a special encoding used to convert Unicode characters to ASCII

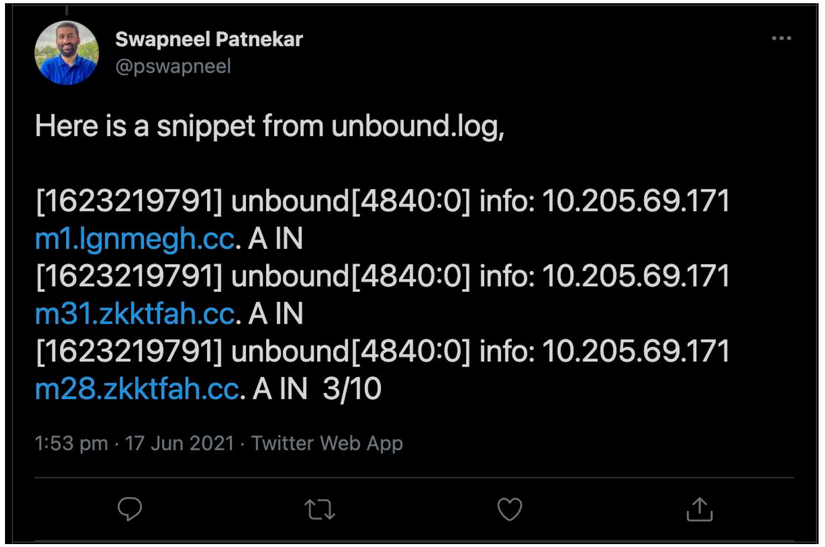
```
[1623322522] unbound[1826:0] info: 10.205.69.155 xn--elan-gebudereinigung-izb.de. A IN
[1624348976] unbound[1826:0] info: 10.205.69.204 xn--kontinentalsngar-6nb.nu. A IN
[1624348978] unbound[1826:0] info: 10.205.69.204 www.xn--kontinentalsngar-6nb.nu. A IN
[1624598024] unbound[1826:0] info: 10.205.69.160 xn--80avc1e.xn--p1acf. A IN
[1624598120] unbound[1826:0] info: 10.205.69.160 xn----8sbkeadqdasb3ajanjhk4b9b.xn----8sbjbwkieldg1bp.xn--p1ai. A IN
[1624598151] unbound[1826:0] info: 10.205.69.160 xn--80aaag8b7af9f.xn--p1ai. A IN
```

www.xn--kontinentalsngar-6nb.nu — — — —-> www.kontinentalsängar.nu.

The Hunt

- Network operator - 5000 systems Internal network





Source: https://twitter.com/pswapneel/status/1405441027746324482?s=20

DNS logging

- DNS query logging doesn’t log responses by default
- Logging responses impacts the operational performance of the DNS resolver
- DNS query logging - bare minimum - something is better than nothing!

Tooling

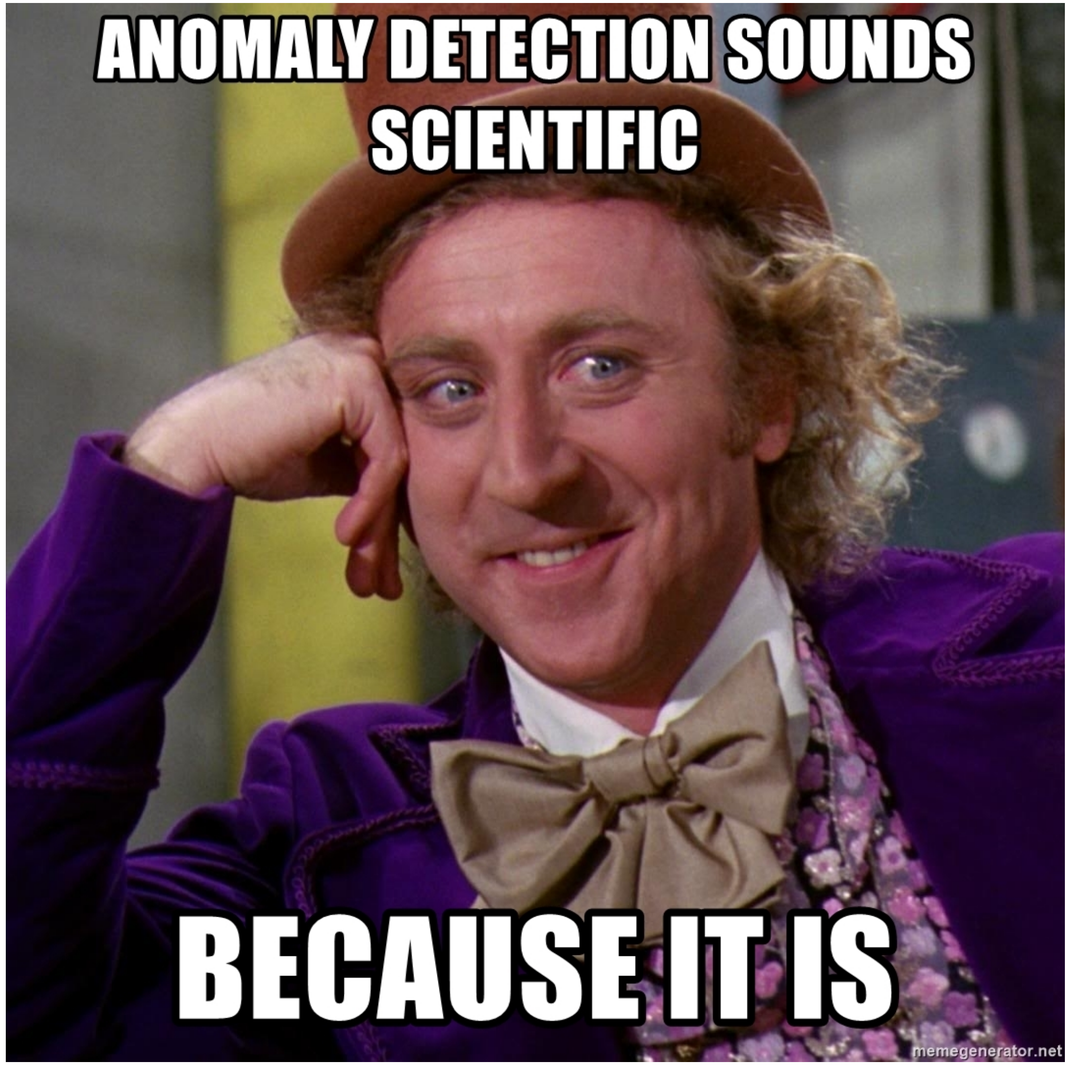
https://securityonionsolutions.com/

https://zeek.org/

Source: https://memegenerator.net/img/instances/61457871/open-source-open-source-open-source-open-source.jpg

domain_stats2

- A log enrichment utility written by Mark Baggett
- Domains that were recently registered
- Domains that no one in your organization has ever visited before
- Domains with hostnames that appear to be random characters



Source : https://memegenerator.net/instance/60078448/willy-wonka-anomaly-detection-sounds-scientific-because-it-is

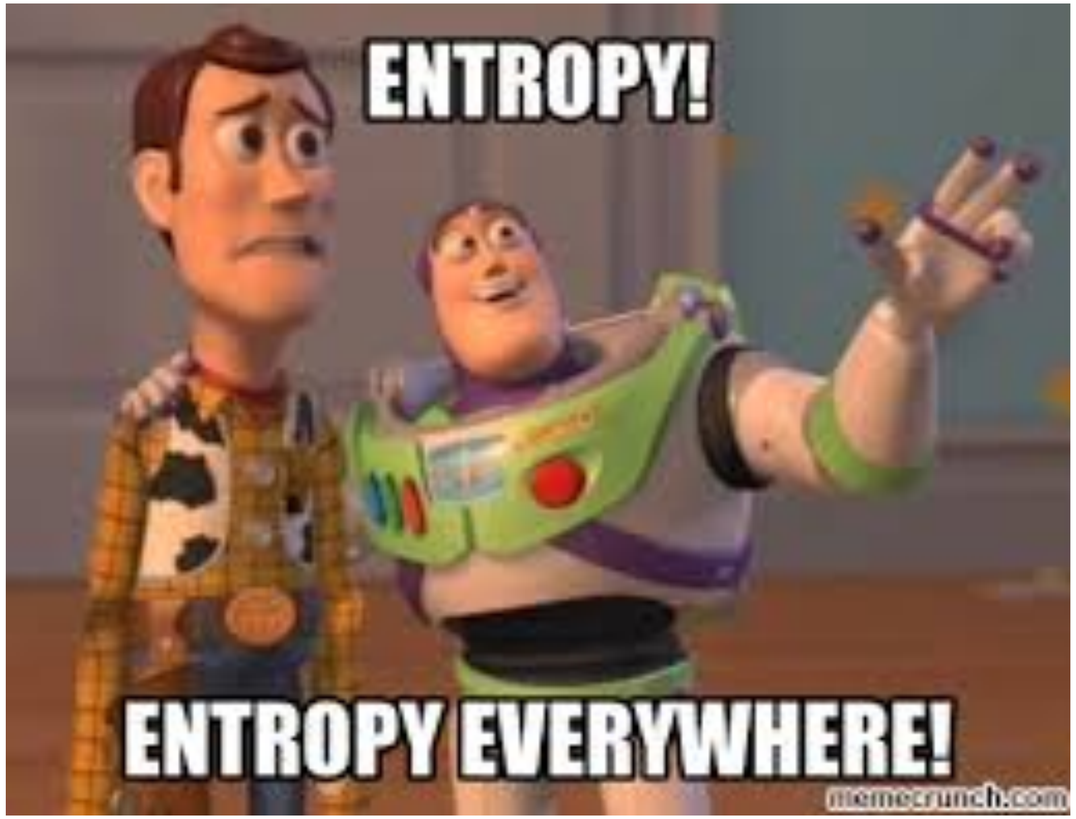
{"alerts":["YOUR-FIRST-CONTACT"],"category":"ESTABLISHED","freq_score":[8.0248,6.1107],"seen_by_isc":"RDAP","seen_by_web":"Tue, 01 Nov 1994 05:00:00 GMT","seen_by_you":"Thu, 15 Jul 2021 13:59:17 GMT"}

{"alerts":[],"category":"ESTABLISHED","freq_score":[8.0248,6.1107],"seen_by_isc":"RDAP","seen_by_web":"Tue, 01 Nov 1994 05:00:00 GMT”, "seen_by_you":"Thu, 15 Jul 2021 13:59:17 GMT"}

{"alerts":[],"category":"ESTABLISHED","freq_score":[8.0248,6.1107],"seen_by_isc":"top1m","seen_by_web":"Tue, 01 Nov 1994 05:00:00 GMT","seen_by_you":"Fri, 16 Jul 2021 03:58:01 GMT"}

freq.py

- freq.py and freq_server.py - Tool for detecting DGA written by Mark Baggett
- Web interface which can integrate with a SIEM
- It’s available in Security Onion



Source - https://memecrunch.com/meme/364YE/entropy-everywhere

Passive DNS Monitoring

- Talk I gave ‘Uncovering badness using Passive DNS’ - APNIC 50 FIRST Security 1
- Free and Commercial providers - CIRCL, Farsight Security, Spamhaus Technology
- But they don’t provide the context and correlation within my baseline
- passivedns tool by Edward Bjarte Fjellskål
- Incident handling, Network Security Monitoring, network forensics
- Uses libpcap and parses DNS traffic over TCP and UDP

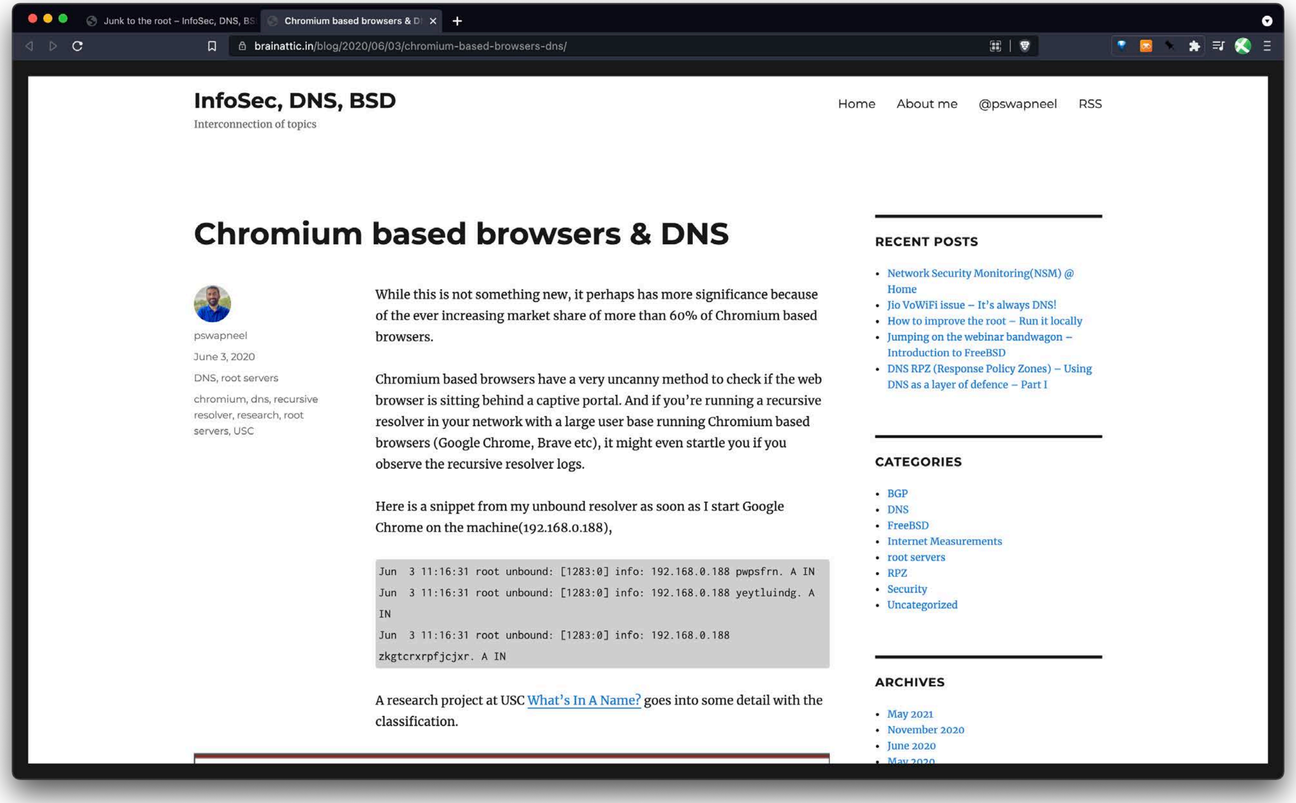
```
1626411461.194161||192.168.0.250||205.251.192.29||IN||ns-225.awsdns-28.com.||A||205.251.192.225||172800||1
1626411461.197736||192.168.0.250||205.251.198.122||IN||ns-1492.awsdns-58.org.||A||205.251.197.212||172800||1
1626411461.225267||192.168.0.250||205.251.195.27||IN||ns-713.awsdns-25.net.||A||205.251.194.201||172800||1
1626411461.241111||192.168.0.250||205.251.196.156||IN||ns-225.awsdns-28.com.||AAAA||2600:9000:5300:e100::1||172800||1
1626411461.250961||192.168.0.250||205.251.194.252||IN||ns-1492.awsdns-58.org.||AAAA||2600:9000:5305:d400::1||172800||1
1626411461.275363||192.168.0.250||205.251.197.89||IN||ns-713.awsdns-25.net.||AAAA||2600:9000:5302:c900::1||172800||1
1626411461.298799||192.168.0.250||205.251.197.212||IN||sin.t100.prod.ter.amazonvideo.com.||A||3.0.120.41||60||1
1626411461.298799||192.168.0.250||205.251.197.212||IN||sin.t100.prod.ter.amazonvideo.com.||A||18.141.80.109||60||1
1626411461.298799||192.168.0.250||205.251.197.212||IN||sin.t100.prod.ter.amazonvideo.com.||A||18.136.60.74||60||1
1626411461.471808||192.168.0.250||205.251.193.106||IN||ns-1877.awsdns-42.co.uk.||A||205.251.199.85||172800||1
1626411461.524977||192.168.0.250||205.251.199.46||IN||ns-1877.awsdns-42.co.uk.||AAAA||2600:9000:5307:5500::1||172800||1
1626411476.799938||192.168.0.250||205.251.196.113||IN||us06web.zoom.us.||A||3.235.71.227||60||1
1626411476.817611||192.168.0.250||205.251.193.131||IN||us06web.zoom.us.||A||3.235.71.220||60||1
1626411480.703805||192.168.0.250||205.251.195.153||IN||unagi-eu.amazon.com.||A||52.94.223.32||60||1
1626411532.262796||192.168.0.250||17.253.200.1||IN||3-courier.push.apple.com.||CNAME||3.courier-push-apple.com.akadns.net.||28800||1
1626411532.709847||192.168.0.250||193.108.88.128||IN||3.courier-push-apple.com.akadns.net.||CNAME||apac-in-courier-4.push-apple.com.akadns.net.||60||1
```

Use cases

- Anomalies based on domain creation dates
- Anomalies based on entropy
- Baseline - whitelisted domains instead of the Cisco top 1 million
- Historical context of a domain name in the network

False Positives

- Chromium browsers - junk queries to the root. Fixed in Chromium 87
- Certain applications send DNS queries which appear to be DGA



Source: https://brainattic.in/blog/2020/06/03/chromium-based-browsers-dns/

Challenges

Do53

- Plain text query response protocol - It *is* an ideal friend of the network defender
- Visibility - getting insight into a threat hunt starts with DNS

Test	Sysmon DNS Events	Zeek DNS Queries	Zeek HTTP Logs	Zeek SSL Logs
DoH Disabled	5142	5560	325	2154 (449 TLS 1.3)
DoH Enabled	0	848	530	2747 (499 TLS 1.3)

Table 1: DNS over HTTPS Baseline Test

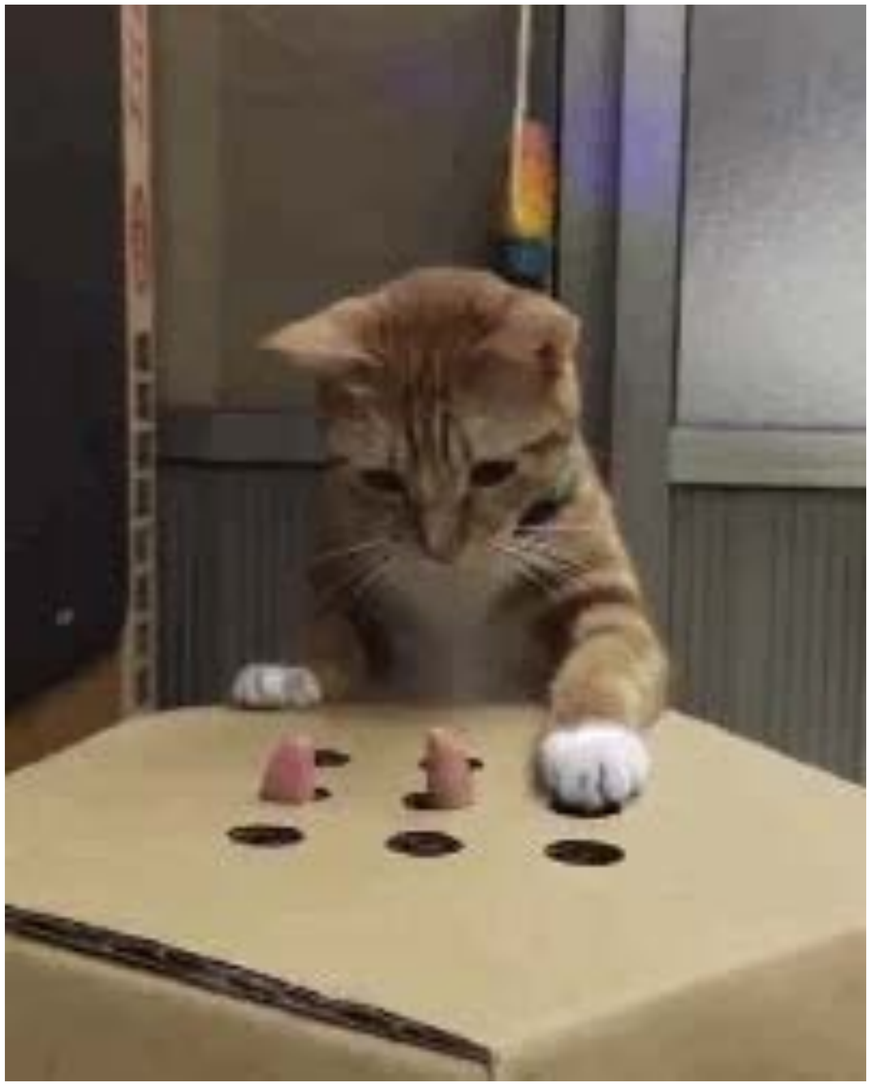
Source: https://www.sans.org/reading-room/whitepapers/dns/paper/39160

DNS over HTTPS (DoH)

- RFC 8484
- Control plane and data plane is the same
- Hides the existence of DNS traffic !
- Identification is a problem - Which session contains DNS traffic and which contains web browsing activity ?

Detecting DoH

- No magic bullets
- TLS Inspection - TLS 1.3 / Certificate Pinning ?
- TLS Fingerprinting - JA3 and JA3S
- Manual heuristics



Source: https://giphy.com/gifs/gifporn-MVUyVpyjakkRW

Community resources

- DNS RPZ zone file - We publish a DNS zone file

```
rpz:
    name: shreshtait-rpz
    url: https://shreshtait.com/dnsrpz/shreshtait-rpz.zone
    rpz-log: yes
    rpz-log-name: shreshtait-rpz
```

- MISP - Currently running a private instance, plan is to share with other MISP communities we are already part of CIRCL etc

Hat tip

Resources

- Pyramid of Pain
  https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html
- Using DNS as a layer of defence
  https://blog.apnic.net/2020/07/02/dns-rpz-using-the-dns-as-a-layer-of-defence/
- Chromium based browsers and DNS
  https://brainattic.in/blog/2020/06/03/chromium-based-browsers-dns/
- domain_stats2
  https://github.com/MarkBaggett/domain_stats
- APNIC 50 - Uncovering badness using Passive DNS
  https://youtu.be/WKJzVOkMbc0?t=2462
- passivedns - https://github.com/gamelinux/passivedns
- A New Needle and Haystack: Detecting DNS over HTTPS Usage
  https://www.sans.org/reading-room/whitepapers/dns/needle-haystack-detecting-dns-https-usage-39160

Contact

- @pswapneel
- swapneel.patnekar@shreshtait.com