Using DNS as a layer of defence

- Swapneel Patnekar
  @pswapneel

About me

- Network engineer & researcher with interests in networking(DNS, DNSSEC, BGP), Unix systems and security.
- Technical trainer - regularly conduct workshops on DNS, DNSSEC, Routing, Unix etc
- APNIC Community Trainer & a RIPE Atlas Ambassador.
- Managing Director of Shreshta IT Technologies Pvt. Ltd, a company based out of Belgaum, building & securing networks of micro, small & medium enterprises & network operators in Tier-II and Tier-III cities.

Key Take-away's

- Adding a layer of defence in a network
- Applicable for network operators
- Applicable for an organisation network - Networks of MSME, large enterprises
- Applicable for home/SOHO networks

Primary attack vectors in a network

1. Websites Accessed
2. Email
3. File/Folder Sharing
4. USB Storage devices

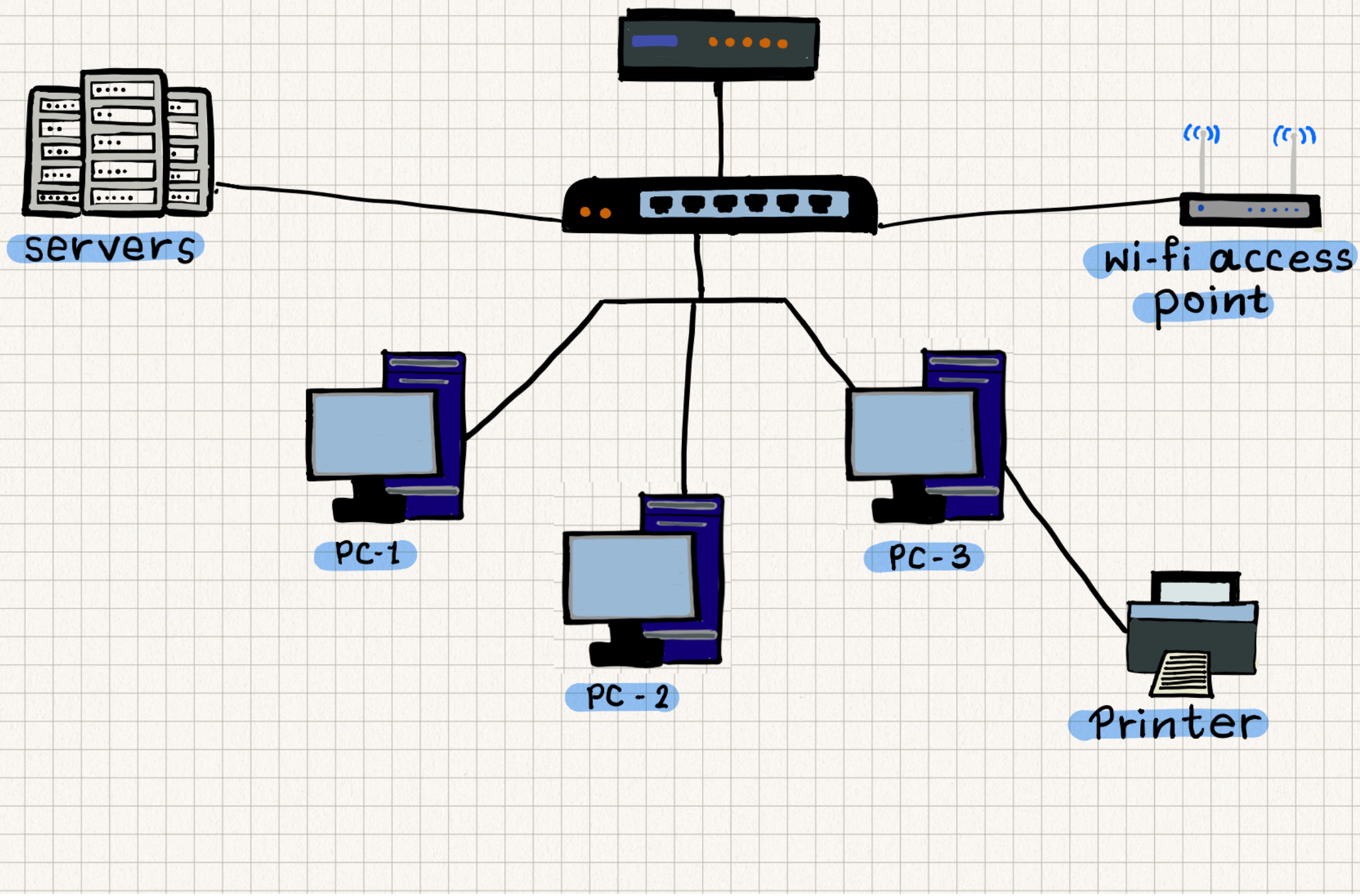
1. Phishing URL's
2. Malicious files
3. Ransomware
4. C2/Bots

What is a flat network ?

- Network is not segmented i.e computers can connect/ access any other computer in the network

- A simple computer network with the goal to reduce cost, maintenance and administration.

FLAT NETWORK



Problems with the flat network

- No segmentation of traffic - Single broadcast domain
- Propagation of malicious traffic within the network spreads rapidly

Examples of a flat network

- Home network
- SOHO

Mix this with

- Ignorance on basic security best practices -
  1. Anti-virus license expired/not updated
  2. After connecting a USB storage device, user clicks cancel on the Anti-virus scan

- Decentralised User management. Everybody logs-in as Administrator because the ERP/Account software doesn’t work !

- Lack of IT processes

From: [mailto:no-reply@accounts.google.com]
Sent: 09 January 2019 05:32
To:
Subject: Security alert

Attention:

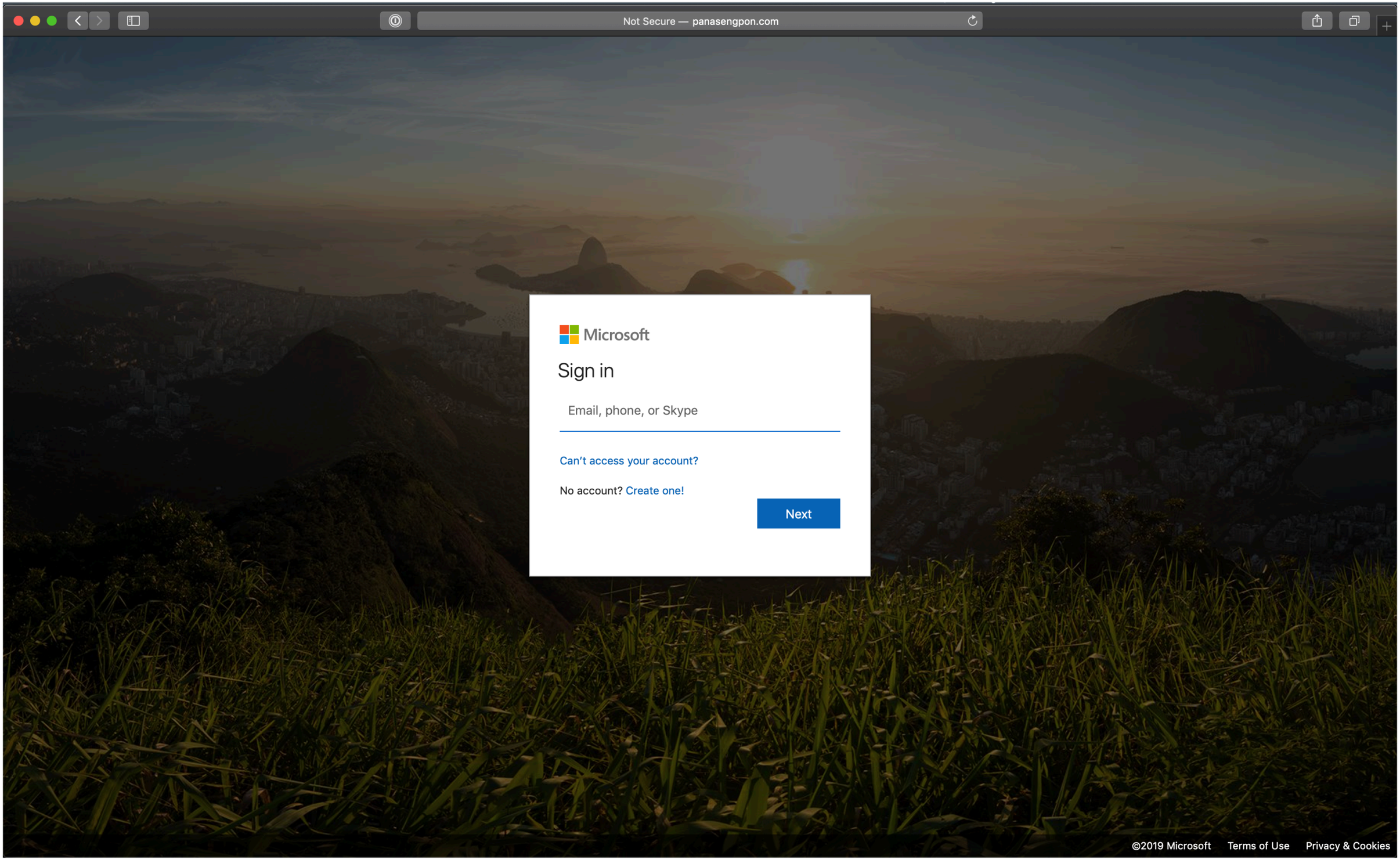
This is to inform you that virus activities have been detected un your email account.
And we demand that you take immediate action to scan and delete all threatst from your email account

To keep your account safe, please follow the URL below to run a quick email scan.

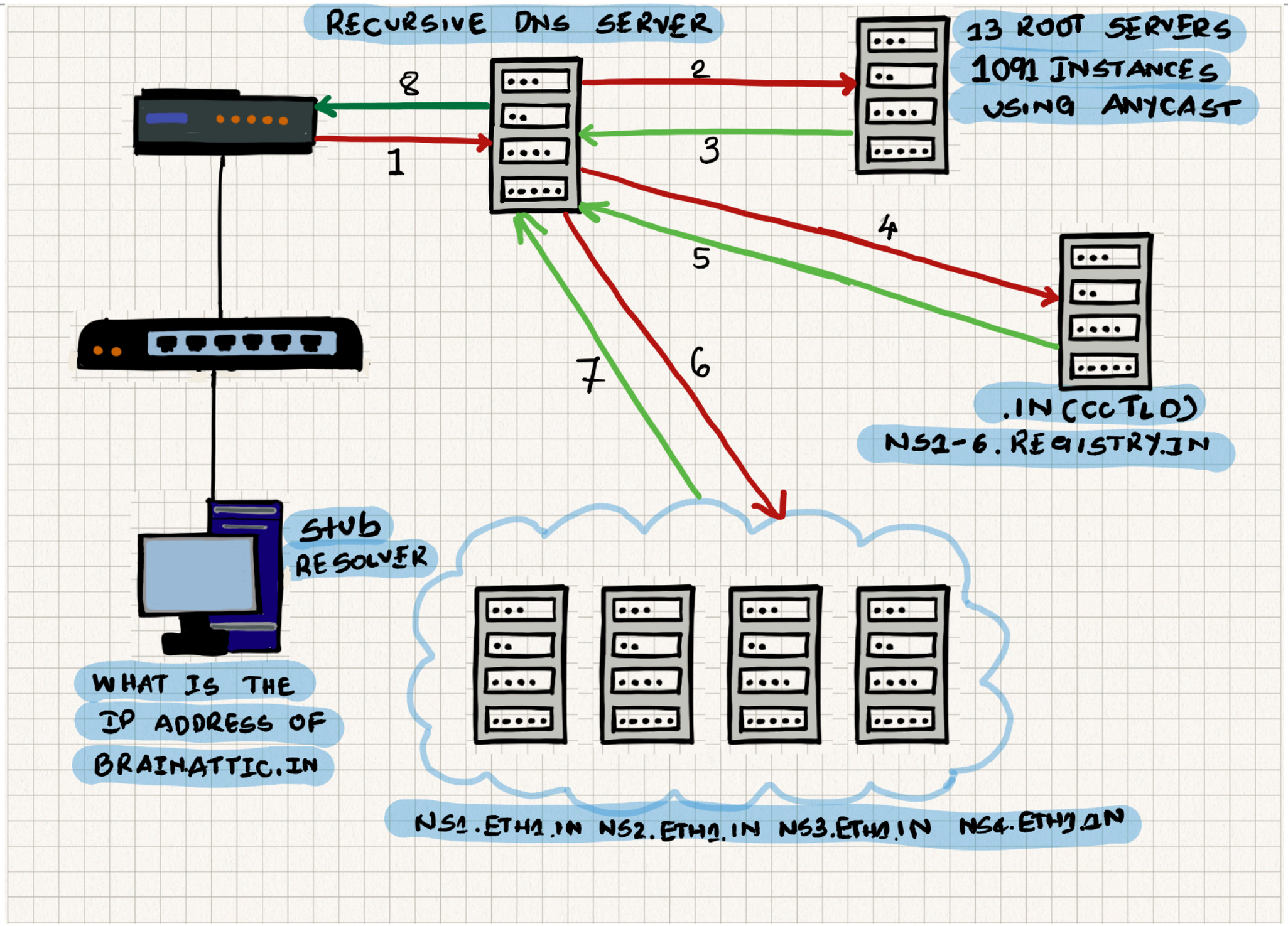
If you ignore this notice, your account will be suspended to protect our server from further damage.

Source:

This message is auto-generated from E-mail security server, and replies sent to this email can not be delivered.
This email is meant for:


Not Secure — panasengpon.com
Microsoft
Sign in
Email, phone, or Skype
Can’t access your account?
No account? Create one!
Next
©2019 Microsoft
Terms of Use
Privacy & Cookies

Fundamentals of DNS



DNS resolver options

- **Hosted(“Outsourced") Recursive DNS resolvers** - Google DNS(8.8.8.8/8.8.4.4) , Quad9(9.9.9.9), Cloudflare(1.1.1.1, 1.0.0.1), ISP's DNS resolvers(Do they even exist now? :-))

- **On-premise recursive DNS resolvers** - Unbound, BIND, PowerDNS, KnotDNS, pi-Hole.

How does a DNS firewall help?

- Everything begins with a DNS query.
- DNS is used(legitimate queries).
- DNS is also used for abuse by malware
- Set a differentiated route for the bad stuff.
- Cheap defence in a flat network.
- Of course - Security is Multi-layered approach. No silver bullet. DNS firewall is just one of the mechanisms.

DNS RPZ(Response Policy Zones) or DNS Firewalls

- DNS RPZ - A vendor-neutral distributed DNS firewall
- IETF Internet Draft by Dr. Paul Vixie & V. Schryver. Not a standardised IETF protocol yet.
- Allows policy to be applied to DNS queries. DNS server will respond with a differentiated answer
- Threat intelligence data feeds ‘zone’ files.
- BIND 9.10 / Unbound 1.10 / PowerDNS

TRIGGER → ACTION

1. QNAME
2. CLIENTIP IP ADDRESS
3. RESPONSE IP ADDRESS
4. NSIP
5. NSDNAME

1. LOCAL DATA
2. NXDOMAIN
3. DROP
4. NODATA
5. TCP-ONLY
6. PASSTHRU

Example of a DNS zone file

```
$ORIGIN .
$TTL 10800      ; 3 hours
instaping.in            IN SOA  ns1.instaping.in. admin.instaping.in. (
                                286446     ; serial
                                10800      ; refresh (3 hours)
                                3600       ; retry (1 hour)
                                604800     ; expire (1 week)
                                3600       ; minimum (1 hour)
                                )
                        NS      ns1.instaping.in.
                        NS      ns2.instaping.in.
$TTL 60 ; 1 minute
                        A       122.171.37.156
                        MX      100 us2.mx3.mailhostbox.com.
                        MX      100 us2.mx1.mailhostbox.com.
                        MX      100 us2.mx2.mailhostbox.com.
$ORIGIN instaping.in.
webmail                 A       106.201.125.76
www                     A       122.252.225.22
staging                 A       203.192.220.112
~
```

Example of a DNS RPZ zone file

```
$TTL 30
@ SOA rpz.brainattic.in. hostmaster.brainattic.in. 1908220633 300 1800 604800 30
 NS localhost.
;
; StevenBlack/(adware + malware) unified hosts Response Policy Zones (RPZ)
; For the raw hosts file : https://raw.githubusercontent.com/StevenBlack/hosts/master/hosts
; Last updated: 2019-08-22 06:33:01 (UTC)
;
; For questions please contact swapneel [at] brainattic.in
;
adservice.google.com.vn CNAME .
1493361689.rsc.cdn77.org CNAME .
30-day-change.com CNAME .
www.30-day-change.com CNAME .
2468.go2cloud.org CNAME .
www.2468.go2cloud.org CNAME .
adservice.google.nl CNAME .
analytics.ff.avast.com CNAME .
androidads23.adcolony.com CNAME .
analytics.publitas.com CNAME .
www.analytics.publitas.com CNAME .
annualconsumersurvey.com CNAME .
www.annualconsumersurvey.com CNAME .
amarktflow.com CNAME .
www.amarktflow.com CNAME .
```

```
zone "adware-malware.zone" {
        type master;
        file "/etc/bind/adware-malware.rpz";
        allow-query { any; };
        allow-update { none; };
        allow-transfer { none; };
};
```

```
response-policy { zone "adware-malware.zone"; };
```

Demo

Reputation Feeds

- URLhaus
- SURBL
- Spamhaus
- Farsight Security
- Switch
- Create your own feed/zone data

Lessons Learned

- Lookout for false positives - especially if you are curating your own feeds
- Monitoring & analysis is a must(log file is your friend)
- ELK(Elasticsearch, Logstash, Kibana) for realtime analysis

Spamhaus DNS RPZ free feeds

- Do Not Route or Peer (DROP)
- Coinblocker
- Torblocker

- Identify & stop unwanted/malicious outbound abuse by IoT devices

- Run your own recursive DNS resolver for the entire network - Unix/Linux box, pi-Hole

- Run your own recursive DNS resolver on a computer/ laptop - BIND, unbound

Pi-hole

pihole

Pi-hole

Status

- DNS service not running
- Load: 0 0 0
- Memory usage: 17.9 %

MAIN NAVIGATION

- Dashboard
- Query Log
- Long term data
  - Graphics
  - Query Log
  - Top Lists
- Whitelist
- Blacklist
- Disable
- Enable
- Tools
- Settings
- Logout
- Donate
- Help

Total queries (3 clients)

15,189

Queries Blocked

1,721

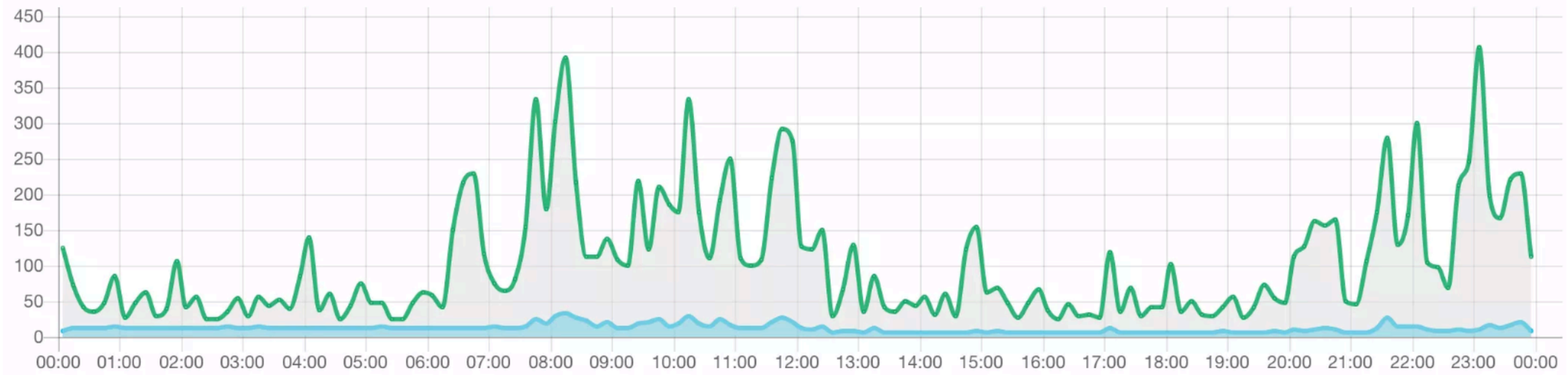
Percent Blocked

11.3%

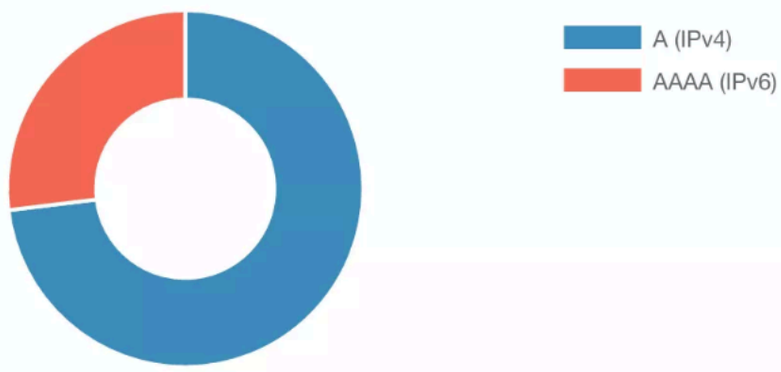
Domains on Blocklist

111,175

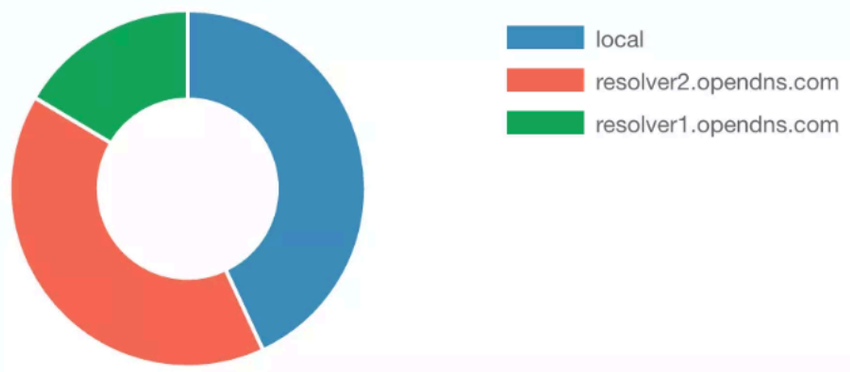
Queries over last 24 hours



Query Types (integrated)



Forward Destinations (integrated)



Current challenges

- DOH(DNS over HTTPS), RFC 8484

- Browser will send DNS queries over HTTPS thereby bypassing local network/system DNS resolver
  1. Firefox - Opt-out -Enabled for everyone in United States
  2. Google Chrome - Opt-in -
  3. Brave - Opt-in - Won’t upgrade to DOH unless OS is using a resolver that supports DOH (Google / Cloudflare)

- Windows 10 - Opt-in

- Apple - iOS 14 and macOS 11

References

1. Flat Network
   https://en.wikipedia.org/wiki/Flat_network

2. Google Public DNS
   https://developers.google.com/speed/public-dns/docs/using

3. Cloudflare Recursive DNS
   https://www.cloudflare.com/learning/dns/what-is-1.1.1.1/

4. Quad9 - https://www.quad9.net/

5. DNS RPZ - https://dnsrpz.info/

6. DNS Response Policy Zones (RPZ) draft-vixie-dns-rpz-04
   https://tools.ietf.org/html/draft-vixie-dns-rpz-04

7. Root DNS Servers list - https://root-servers.org/

8. URLhaus - https://urlhaus.abuse.ch/

9. SURBL - http://www.surbl.org/

10. Spamhaus - https://www.spamhaustech.com/

11. Farsight Security - https://farsightsecurity.com

12. Switch - https://www.switch.ch/

13. Godlua Malware using DNS-over-HTTPS
    https://www.bleepingcomputer.com/news/security/new-godlua-malware-evades-traffic-monitoring-via-dns-over-https/

References

1. RFCsWeLove - Current state of DNS and DoH - https://www.iiesoc.in/post/virtual-rfcs-we-love-may-2020

2. DOH in Brave - https://github.com/brave/brave-core/pull/4314

3. DOH in Windows 10 - https://techcommunity.microsoft.com/t5/networking-blog/windows-will-improve-user-privacy-with-dns-over-https/ba-p/1014229#

4. Pi-hole 5.0 - Per client blocking
https://pi-hole.net/2020/05/10/pi-hole-v5-0-is-here/#page-content

5. My blog post @ APNIC
https://blog.apnic.net/2020/07/02/dns-rpz-using-the-dns-as-a-layer-of-defence/

Questions/Comments ?

Contact -

Swapneel Patnekar

swapneel@brainattic.in

Twitter: @pswapneel