DNS SINKHOLING

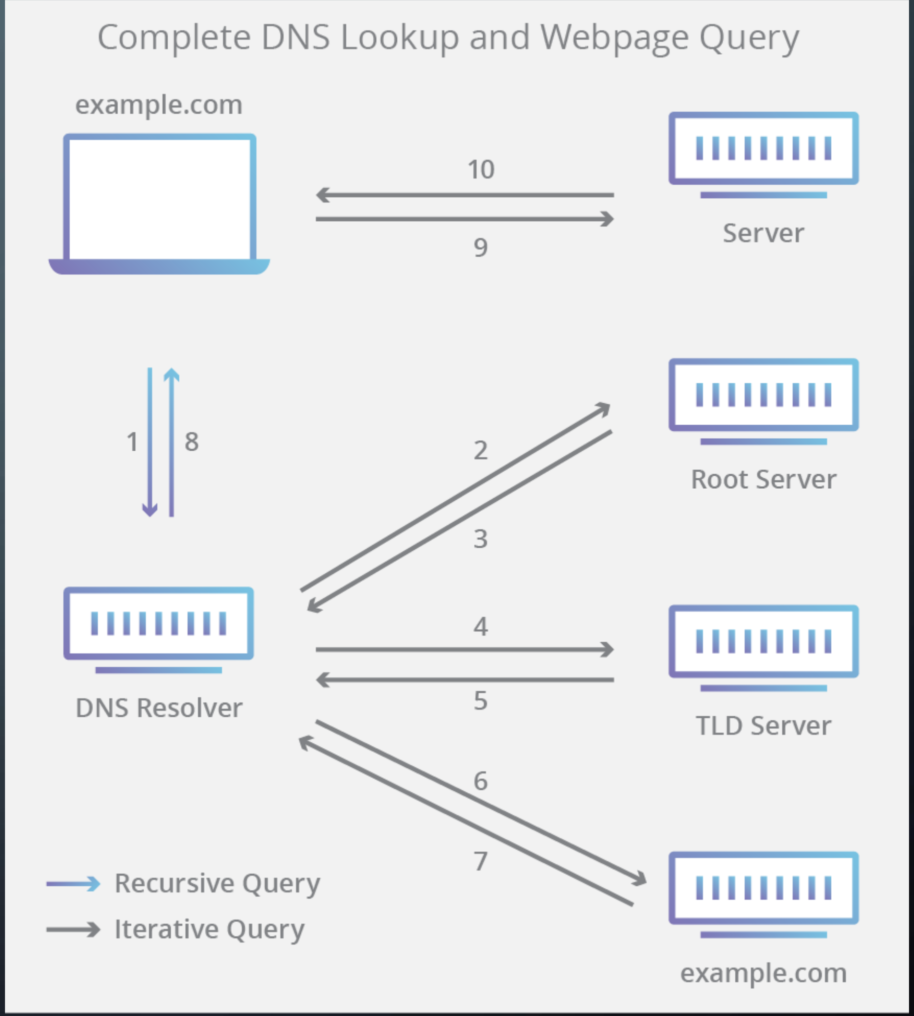
JONATHAN ALTER

OVERVIEW

1. A Quick Review of DNS
2. What is DNS Sinkholing?
3. Use cases
4. Solutions available
   - Enterprise Solutions
   - Consumer Solutions
5. Weaknesses, Threats, and Limitations to DNS Sinkholing
6. Food for thought – Discussion

1) A QUICK REVIEW OF DNS

- DNS = Domain Name Service
- AKA: “Phonebook of the internet”
- What is “www.google.com”?
  - 172.217.10.46
- Bottom line: FQDN → IP Address
- Technical Details:
  - Runs over UDP port 53
  - Request, Response
  - Hierarchical structure:
    - Root → TLD → …etc.

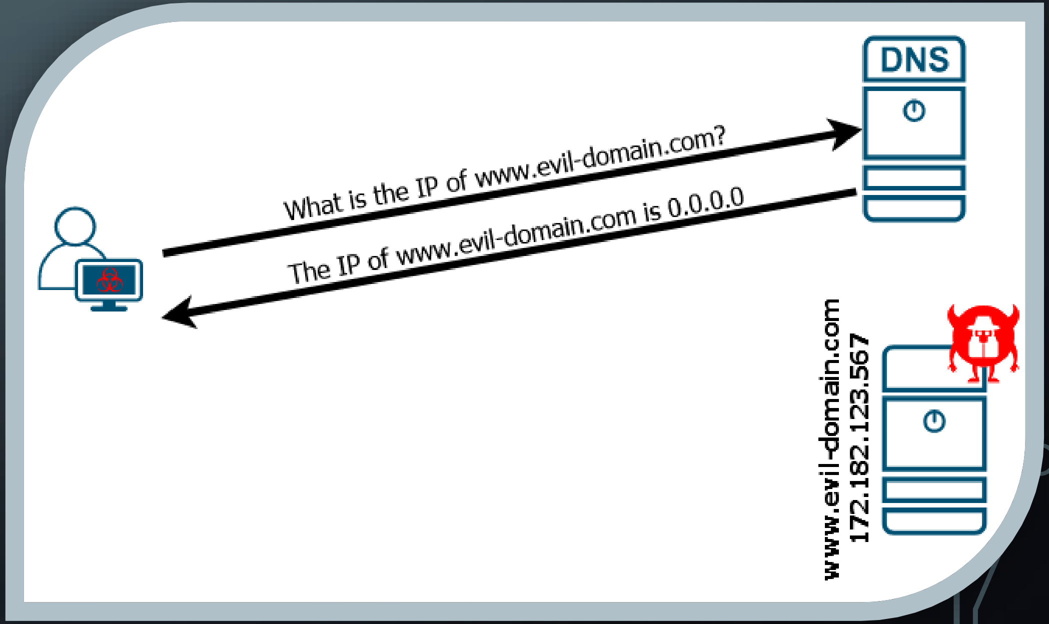


2.1) WHAT IS DNS SINKHOLING?

Definition (Wikipedia): A DNS sinkhole, also known as a sinkhole server, Internet sinkhole, or Blackhole DNS is a DNS server that gives out a false result for a domain name.

Approaches to returned IP address:

- NXDOMAIN – *DNS Response saying that the domain requested is non-existent **
- 0.0.0.0 – *Non-routable, results in instant failure*
- 127.0.0.1 – *Loopback address for localhost. Results in failure, after a bit.*
- Bogus IP outside of the host's zone – *Allows firewalls to log all attempts to reach malicious hosts (Palo Alto)*


DNS
What is the IP of www.evil-domain.com?
The IP of www.evil-domain.com is 0.0.0.0
www.evil-domain.com
172.182.123.567

2.2) DNS SINKHOLING

- Host-Level
  - Hosts file
  - Local client / application
  - Remote DNS Sinkhole resolver
- Network-Level
  - DHCP lease sets DNS Server on client to be a DNS Resolver that performs sinkholing

Operating System	Location of Hosts file
Windows (NT - 10)	%SystemRoot%\System32\drivers\etc\hosts
Mac OS X (10.2+)	/etc/hosts
Linux (most distros)	/etc/hosts

3.1) USE CASES – Malware/ Botnets

- We can stymie the operations of botnets by keeping track of known C2 (Command & Control) servers and malicious domains.
  - When an infected bot attempts to reach out to its C2 server for updates/ instructions, it is given a sinkholed IP address and is then unable to communicate
- Similarly, domains used to traffic malware can be added to a similar “blacklist” and sinkholed.
- In commercial settings, its preferable to use a bogus IP address as opposed to a non-routable one (127.0.0.1 & 0.0.0.0).
  - Allows system administrators to quickly see which hosts are attempting to communicate with malicious domains.

3.2) USE CASES – Ads/ Trackers

DNS Sinkholing can also be used to defend against advertisements and trackers.

- Many sites and Github projects dedicated to amassing lists of tracking domains and ad sites
  - Sinkhole lists syntax can be:
    - Regular expressions
      - ^ads\.google\.com$
    - ABNF (Augmented Backus-Naur Form)
      - ||ads.google.com^
    - Simply IP-Hostname maps
      - 0.0.0.0   ads.google.com
- These are usually non-routable addresses (0.0.0.0) or DNS errors (NXDOMAIN)

4.1) SOLUTIONS AVAILABLE - Enterprise

Some notable DNS security solutions are available:

- Palo Alto (sinkhole.paloaltonetworks.com)
- Cisco Umbrella
  - Allows for sinkhole configuration
- InfoBlox
  - BloxOne Threat Defense
- SonicWall
- Shadowserver
  - “Operates a vast sinkhole infrastructure”
  - Provides support for dozens of Law Enforcement operations

4.2) SOLUTIONS AVAILABLE – Consumer (Network-Level)

Pi-hole®

- Runs on Linux, and in a Docker container
- Lots of available extensions that can be installed
- Long-time, well respected
- Written in Bash, PHP, C, and CSS

ADGUARD

- Can natively run on Windows, Linux, Mac OS, FreeBSD
- Can run in a Docker or Snapcraft container
- Supports DoH, DoT
- Supports HTTPS for web-app
- Can enforce *Safe Search*
- *Written in Go and JavaScript*

<u>Both:</u>

- Can run on a Raspberry Pi
- Great solutions for DNS Sinkholing on a network level
- Provides admin with a nice dashboard
- Can perform DHCP
- Open Source (AdGuard-Home only)
- Allow the addition of custom block lists

4.3) SOLUTIONS AVAILABLE – Host-level: Hosts File

- No need to “trust” a dev-team and run code
- Lists are constantly being updated
- Hosts file is usually first place checked during the Name Resolution Process

Some notable ones are:

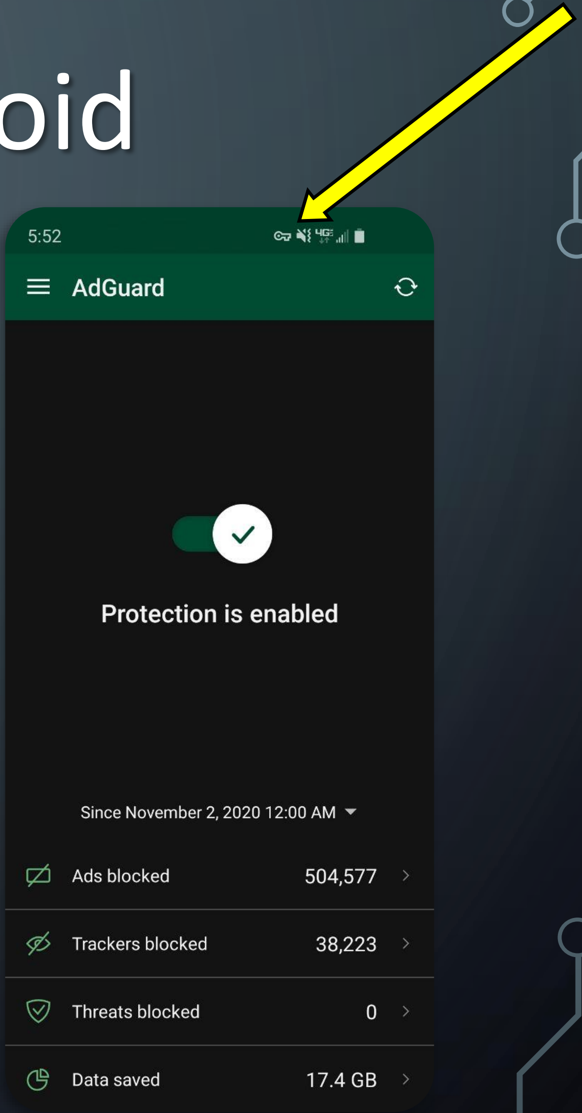
- Steven Black’s Host File: https://github.com/StevenBlack/hosts
- AdAway: https://raw.githubusercontent.com/AdAway/adaway.github.io/master/hosts.txt

4.4) AVAILABLE SOLUTIONS – Host-level: Static DNS

1. OpenDNS: (208.67.222.222)
   - Both enterprise and consumer options (Family Shield, Home, Home VIP, Umbrella Prosumer)
     - Can leverage a DDNS-like method to allow for customizations. (Although, you must run a client to update them about your IP address)
     - This is not required for standard DNS
2. Quad9 (9.9.9.9) - Protection from phishing and spyware
3. Cloudflare – Malware Blocking (1.1.1.2)
4. AdGuard DNS – Blocks ads and trackers (94.140.14.14)

4.5) SOLUTIONS AVAILABLE - Android

- AdGuard for Android (Closed Source) ☹
  - Utilizes a “VPN” to filter DNS queries on all apps
  - Allows for filtering HTTPS traffic by installing a CA
  - Allows for flexible rules based on app and WiFi/Data use
  - Supports DoH, DoT
  - Free and paid options
- NetGuard (Open Source)
  - Uses “VPN” technique too
  - Many similar features to AdGuard
  - Does not utilize CA or support DoH, DoT
- AdAway (Open Source)



Protection is enabled

Since November 2, 2020 12:00 AM

Ads blocked	504,577
Trackers blocked	38,223
Threats blocked	0
Data saved	17.4 GB

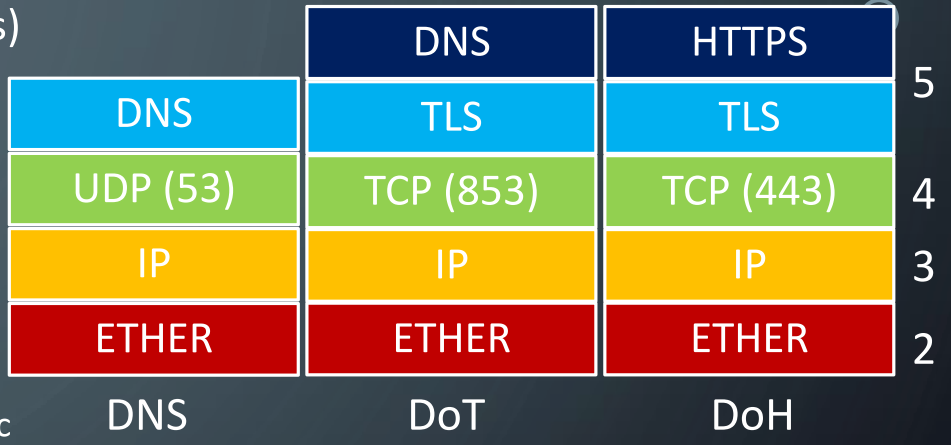
4.6) SOLUTIONS AVAILABLE - iOS

You *can* technically block *some* ads and trackers on iOS. However, because of restrictions with regard to VPN apps and Safari browser, there are no ways (to my knowledge) to block ads on a system-wide level.

5) WEAKNESSES, THREATS, & LIMITATIONS

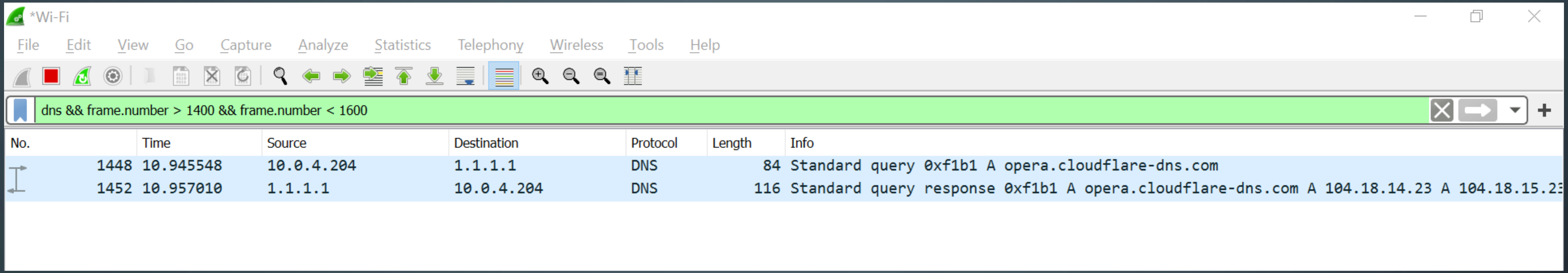
Basic DNS Threats: Eavesdropping & spoofing (MITM – on-path attackers)

- DNS over TLS (like dns.google – yes google is TLD!)
  - Uses TCP port 853
  - Encrypted query
  - Basically DNS stacked on top of TLS instead of UDP
- DNS over HTTPS (DoH) – TCP port 443
  - Privacy & Security Benefits of DoT, but is also disguised as regular HTTPS traffic
  - Firefox – default since 02/2020
  - Chrome, Edge, & Opera – Available feature in settings
- NAT – Hard estimations for how many devices are really compromised - could be 1, could 1,000
- Static DNS assignment
  - Devices not getting their DNS server address from DHCP are potentially vulnerable
  - Malware that makes use of hardcoded DNS server can bypass protections
- Does not solve existing infections



DNS	DoT	DoH	
	DNS	HTTPS	
DNS	TLS	TLS	5
UDP (53)	TCP (853)	TCP (443)	4
IP	IP	IP	3
ETHER	ETHER	ETHER	2

WHAT HAPPENS WHEN WE CAN'T USE DOH?



```
dns && frame.number > 1400 && frame.number < 1600
```

```
No.       Time       Source      Destination  Protocol  Length  Info
   1448  10.945548  10.0.4.204  1.1.1.1      DNS           84  Standard query 0xf1b1 A opera.cloudflare-dns.com
   1452  10.957010  1.1.1.1     10.0.4.204   DNS          116  Standard query response 0xf1b1 A opera.cloudflare-dns.com A 104.18.14.23 A 104.18.15.23
```

If you were really trying to lock down a network, it could be helpful to drop/block all traffic going to UDP port 53 not coming from the DNS server on the network.

- Still, this would only help IFF the IP of the DoH provider was not yet cached.

FOOD FOR THOUGHT:

- What are some legal issues that may relate to DNS Sinkholing?
- Although mostly used for good, DNS Sinkholing can be used for malicious purposes and censorship.
- https://www.shadowserver.org/news/has-the-sun-set-on-the-necurs-botnet/
  - Necurs botnet and territoriality (estimated 9,000,000 compromised devices)
    - https://noticeofpleadings.com/NECURS/files/Application%20for%20TRO/Proposed%20Order.pdf
- Do DNS over HTTPS and TLS even help with privacy?
  - Server Name Indication (SNI) – part of TLS handshake which says which server it is attempting to connect to

SOURCES / RESOURCES:

- https://www.cloudflare.com/learning/dns/what-is-dns/
- https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/use-dns-queries-to-identify-infected-hosts-on-the-network/dns-sinkholing.html
- https://www.shadowserver.org/
- https://www.wired.com/story/microsoft-necurs-botnet-takedown/
- https://resources.infosecinstitute.com/topic/dns-sinkhole/
- https://blog.cloudflare.com/encrypted-sni/