Shut your pi-hole

Running a Network-wide ad-blocker

...on the public internet
Adverts :(
Adverts:(

- Malware / Malvertising
- Tracking
- Analytics
- General Security Hygiene
  - Even when there is no malintent, Ads can pose a risk. E.g
    - Insecure content (http) displayed on secure (https) webpages
uBlock Origin
by Raymond Hill

Finally, an efficient blocker. Easy on CPU and memory.

chrome web store

uBlock Origin
Offered by: Raymond Hill (gorhill)

21,628 | Productivity | 10,000,000+ users

Remove from Chrome
Cons

Only works in the browser

Has to be installed in every browser, on every device

Not well supported on mobile

- This is slowly changing as mobile browsers support extensions or have built in Ad blockers

Doesn’t help with Ads / analytics in native apps (mobile or desktop)
Part 1:  
Network wide Ad-blocking...
Blocking ads at the network level rather than the client level.

● Works for blocking Ads/analytics in native apps

● Protects less-savy family members / flatmates
1. Install a supported operating system

You can run Pi-hole in a container, or deploy it directly to a supported operating system via our automated installer.
Upstream DNS Server
- 8.8.8.8
- 1.1.1.1

Clients
- google.co.nz
- anlytics.evil.com
<table>
<thead>
<tr>
<th>Time</th>
<th>Type</th>
<th>Domain</th>
<th>Client</th>
<th>Status</th>
<th>Action</th>
</tr>
</thead>
</table>
Pi-hole DNS Proxy

Network Perimeter
● (Firewall)

Clients
World Wide Web

Network Perimeter
● (Firewall)

Clients

Pi-hole DNS Proxy
World Wide Web

Network Perimeter ● (Firewall)

Pi-hole DNS Proxy

Clients
Features:

- Community block lists
- Regex Filters
- Tool for testing domains see if / why they are blocked
- Logging / Graphing / Reporting
Compute graphical statistics from the Pi-hole query database

Date and time range:

Queries over the selected time period
## Top Blocked Domains

<table>
<thead>
<tr>
<th>Domain</th>
<th>Hits</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>mobile.pipe.aria.microsoft.com</td>
<td>60415</td>
<td></td>
</tr>
<tr>
<td>graph.instagram.com</td>
<td>9337</td>
<td></td>
</tr>
<tr>
<td>settings-win.data.microsoft.com</td>
<td>9174</td>
<td></td>
</tr>
<tr>
<td>v10.events.data.microsoft.com</td>
<td>6757</td>
<td></td>
</tr>
<tr>
<td><a href="http://www.googleadservices.com">www.googleadservices.com</a></td>
<td>4401</td>
<td></td>
</tr>
<tr>
<td>e.crashlytics.com</td>
<td>2855</td>
<td></td>
</tr>
<tr>
<td>browser.pipe.aria.microsoft.com</td>
<td>2749</td>
<td></td>
</tr>
<tr>
<td>app-measurement.com</td>
<td>2418</td>
<td></td>
</tr>
<tr>
<td>metrics.brightcove.com</td>
<td>1968</td>
<td></td>
</tr>
<tr>
<td>app-analytics.snapchat.com</td>
<td>1842</td>
<td></td>
</tr>
</tbody>
</table>
Problems

Privacy

- Admin has log of all DNS requests made by each client
Problems

Does not block youtube Ads

- r3—sn-4g57kn7e.googlevideo.com
- r2—sn-4g5e6n7d.googlevideo.com
- r5—sn-5hne6n7s.googlevideo.com
- r18—sn-4g57knd7.googlevideo.com

Google has millions of these subdomains
“uBlock can block youtube Ads, so why is it so hard for the pihole?”
<table>
<thead>
<tr>
<th>uBlock</th>
<th>Pi-Hole</th>
</tr>
</thead>
<tbody>
<tr>
<td>● domain names</td>
<td>● domain names</td>
</tr>
<tr>
<td>● URL fragments</td>
<td></td>
</tr>
<tr>
<td>● Content on the page</td>
<td></td>
</tr>
<tr>
<td>○ HTML substrings</td>
<td></td>
</tr>
</tbody>
</table>
Problems

Pesky clients on your network may not use the DNS server provided by your router’s DHCP

- Problem if you are trying to prevent IOT devices phoning home
Problems

Catching and dealing with naughty devices on my home network

April 18, 2018

https://scotthelme.co.uk/catching-naughty-devices-on-my-home-network/

TL;DR: Pi-Hole + PF Sense
Problems

- **Granularity**
  - Sometimes there is a genuine need for exceptions to filters
  - DNS filtering is a blunt tool
## Problems

- **Granularity**

<table>
<thead>
<tr>
<th>uBlock / Browser Based</th>
<th>Pi-Hole</th>
</tr>
</thead>
<tbody>
<tr>
<td>Whitelist / disable filter on a per site basis</td>
<td>Whitelist / disable filter for all applications for all clients</td>
</tr>
</tbody>
</table>
Part 2:
...on the public internet
Ad-Blocking on the go

- Save mobile data

* DNS is plain text so privacy is always limited
  - DoH (DNS over HTTPS)
The wrong way to do it

(the way I did it)
Pi-hole DNS Proxy

World Wide Web

Network Perimeter
  ● (Firewall)

Clients
First week on the Public Internet
<table>
<thead>
<tr>
<th>Time</th>
<th>Type</th>
<th>Domain</th>
<th>Client</th>
<th>Status</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019-09-05 15:08:46</td>
<td>PTR</td>
<td>1.58.0.10.in-addr.arpa</td>
<td>195.37.190.69</td>
<td>OK (cached)</td>
<td></td>
</tr>
<tr>
<td>2019-09-05 15:08:46</td>
<td>PTR</td>
<td>254.65.168.192.in-addr.arpa</td>
<td>195.37.190.69</td>
<td>OK (cached)</td>
<td></td>
</tr>
<tr>
<td>2019-09-05 15:08:46</td>
<td>PTR</td>
<td>254.246.0.10.in-addr.arpa</td>
<td>195.37.190.69</td>
<td>OK (cached)</td>
<td></td>
</tr>
<tr>
<td>2019-09-05 15:08:45</td>
<td>PTR</td>
<td>254.0.101.10.in-addr.arpa</td>
<td>195.37.190.69</td>
<td>OK (cached)</td>
<td></td>
</tr>
<tr>
<td>2019-09-05 15:08:45</td>
<td>PTR</td>
<td>254.164.168.192.in-addr.arpa</td>
<td>195.37.190.69</td>
<td>OK (cached)</td>
<td></td>
</tr>
<tr>
<td>2019-09-05 15:08:45</td>
<td>PTR</td>
<td>254.142.1.10.in-addr.arpa</td>
<td>195.37.190.69</td>
<td>OK (cached)</td>
<td></td>
</tr>
<tr>
<td>2019-09-05 15:08:45</td>
<td>PTR</td>
<td>1.175.5.10.in-addr.arpa</td>
<td>195.37.190.69</td>
<td>OK (cached)</td>
<td></td>
</tr>
<tr>
<td>2019-09-05 15:08:44</td>
<td>PTR</td>
<td>1.159.27.172.in-addr.arpa</td>
<td>195.37.190.69</td>
<td>OK (cached)</td>
<td></td>
</tr>
<tr>
<td>2019-09-05 15:08:44</td>
<td>PTR</td>
<td>254.38.0.10.in-addr.arpa</td>
<td>195.37.190.69</td>
<td>OK (cached)</td>
<td></td>
</tr>
<tr>
<td>2019-09-05 15:08:44</td>
<td>PTR</td>
<td>254.125.22.172.in-addr.arpa</td>
<td>195.37.190.69</td>
<td>OK (cached)</td>
<td></td>
</tr>
</tbody>
</table>
All Time Data

Queries over the selected time period
Mobile Data:

- Mobile carrier forces their own DNS servers on you.

Wifi:

- Mobile phones have bad native UX for advanced network configuration
DNS Amplification is a DDoS attack that leverages DNS resolvers to overwhelm a victim with traffic.
The Right Way To Do It / Next Steps

Pi-Hole + VPN

- OpenVPN / Pi-VPN
- Wireguard