

# 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




<https://github.com/gorhill/uBlock>

Firefox Add-ons

ExploreExtensionsThemesMore... ▾

Find add-ons

Extension WorkshopDeveloper HubRegister or Log in



# uBlock Origin

by [Raymond Hill](#)

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

Remove

Recommended

5,020,149 Users

9,876 Reviews


4.7 Stars

5	★		8,241
4	★		954
3	★		284
2	★		142
1	★		255

chrome web store

s.m3rrick@gmail.com ▾

Home > Extensions > uBlock Origin



## uBlock Origin

Offered by: Raymond Hill (gorhill)

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

Remove from Chrome

Overview

Reviews

Support

Related

# 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-savvy family members / flatmates



[GITHUB](#)[COMMUNITY](#)[ABOUT](#)[BLOG](#)[DONATE](#)

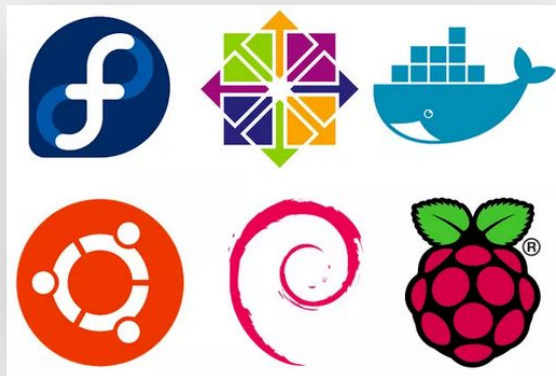
# Pi-hole® Network-wide Ad Blocking

A black hole for Internet advertisements

[INSTALL](#)[DONATE](#)[BECOME A PATRON](#)

## 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.

[DOCKER INSTALL](#)[SUPPORTED OPERATING SYSTEMS](#)

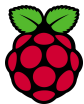
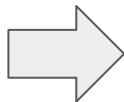


**FTL**  **DNS**<sup>TM</sup>

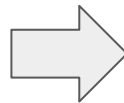




Clients



Pi-hole DNS Proxy



Upstream DNS Server







- 8.8.8.8
- 1.1.1.1



google.co.nz



analytics.evil.com

Time 	Type 	Domain 	Client 	Status 	Action 
2019-10-15 17:13:42	A	t.cfjump.com	122-58-95-74- adsl.sparkbb.co.nz	Blocked (gravity)	<a href="#">Whitelist</a>
2019-10-15 17:13:39	A	sumo.com	122-58-95-74- adsl.sparkbb.co.nz	Blocked (gravity)	<a href="#">Whitelist</a>
2019-10-15 17:13:36	A	mobile.pipe.aria.microsoft.com	122-58-95-74- adsl.sparkbb.co.nz	Blocked (gravity)	<a href="#">Whitelist</a>
2019-10-15 17:13:36	AAAA	mobile.pipe.aria.microsoft.com	122-58-95-74- adsl.sparkbb.co.nz	Blocked (gravity)	<a href="#">Whitelist</a>
2019-10-15 17:13:34	A	t.cfjump.com	122-58-95-74- adsl.sparkbb.co.nz	Blocked (gravity)	<a href="#">Whitelist</a>



World Wide Web

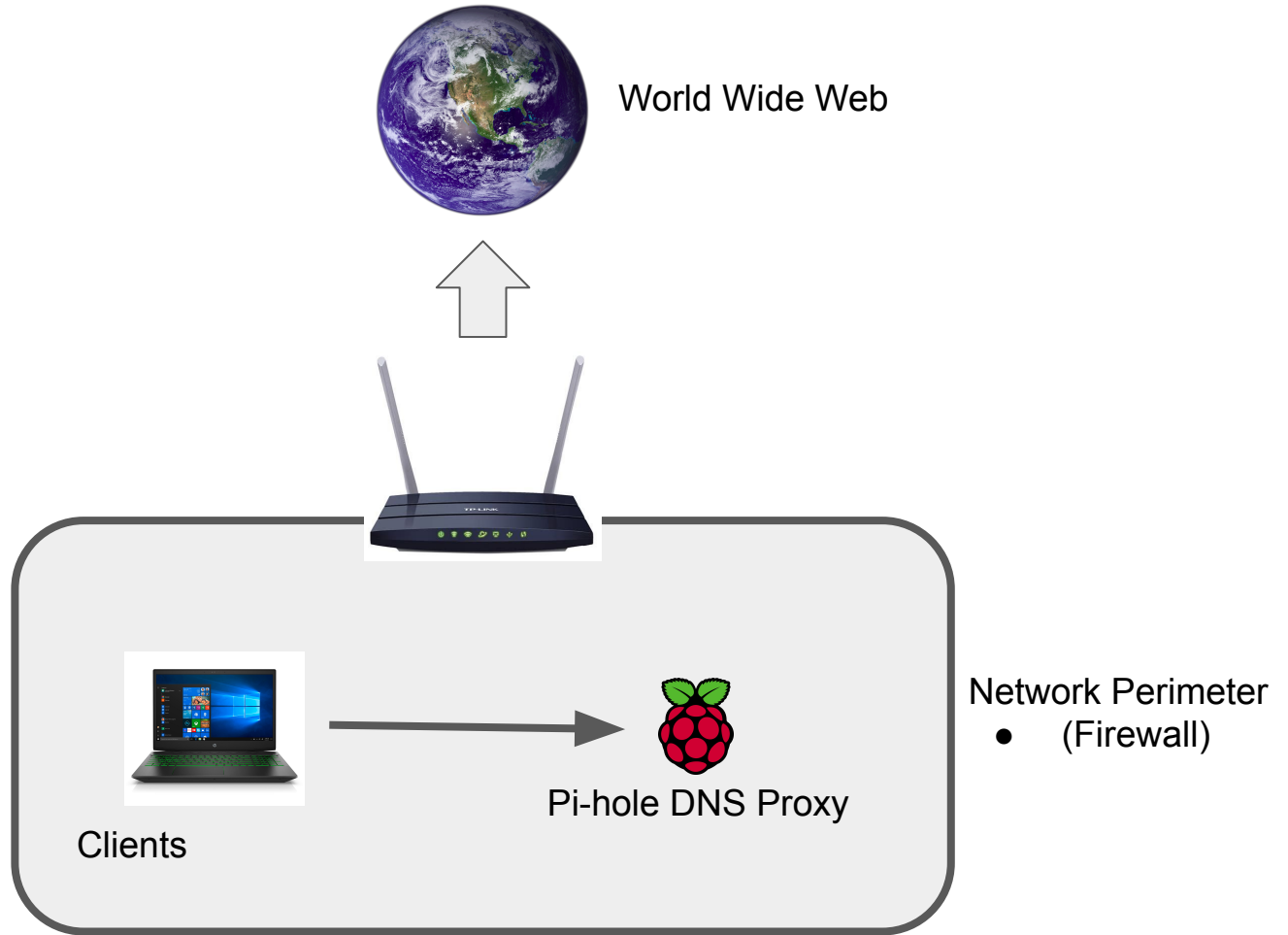


Clients



Pi-hole DNS Proxy

Network Perimeter  
• (Firewall)







World Wide Web



Clients



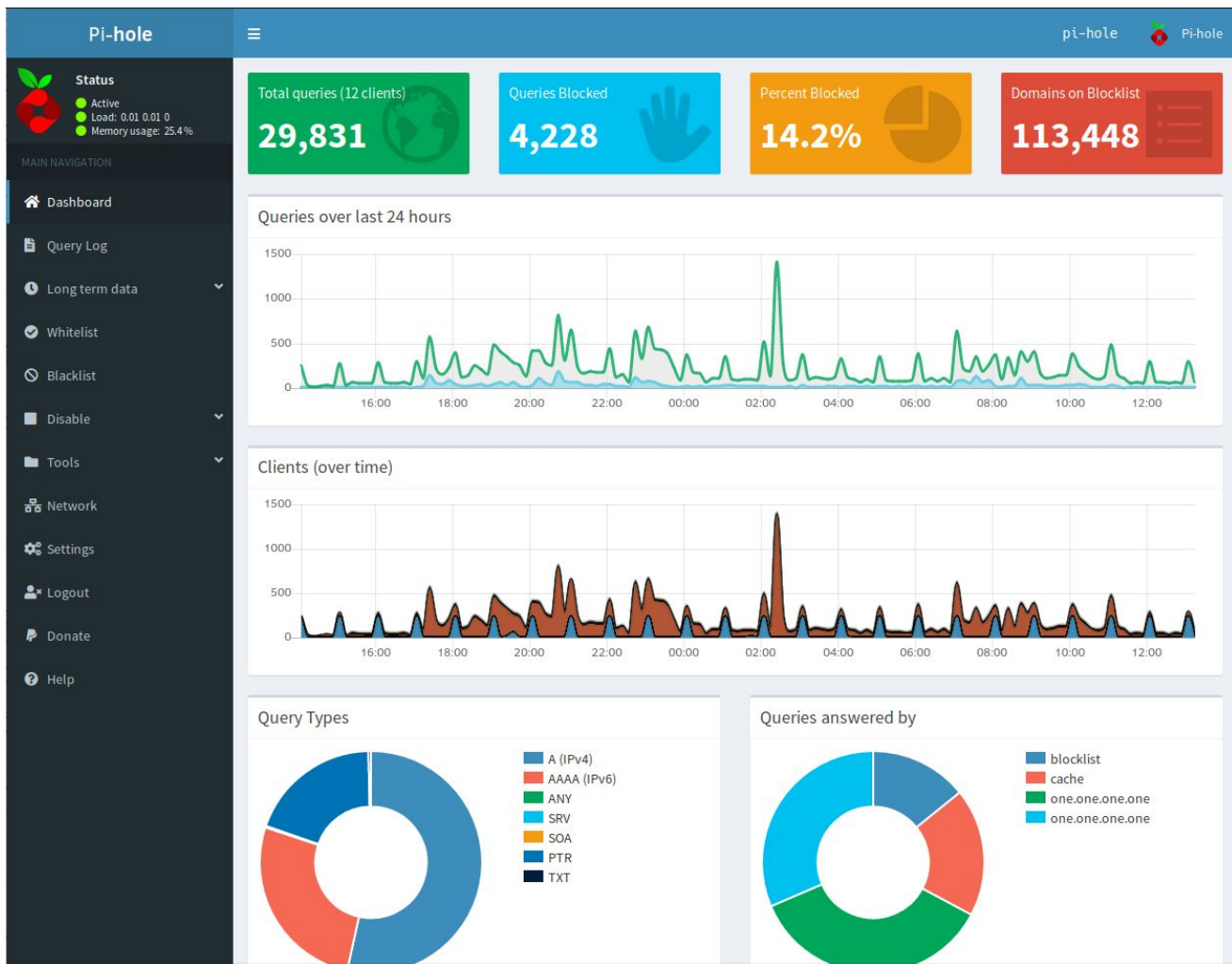
Pi-hole DNS Proxy

Network Perimeter  
• (Firewall)



# Features:

- Community block lists
- Regex Filters
- Tool for testing domains see if / why they are blocked
- Logging / Graphing / Reporting

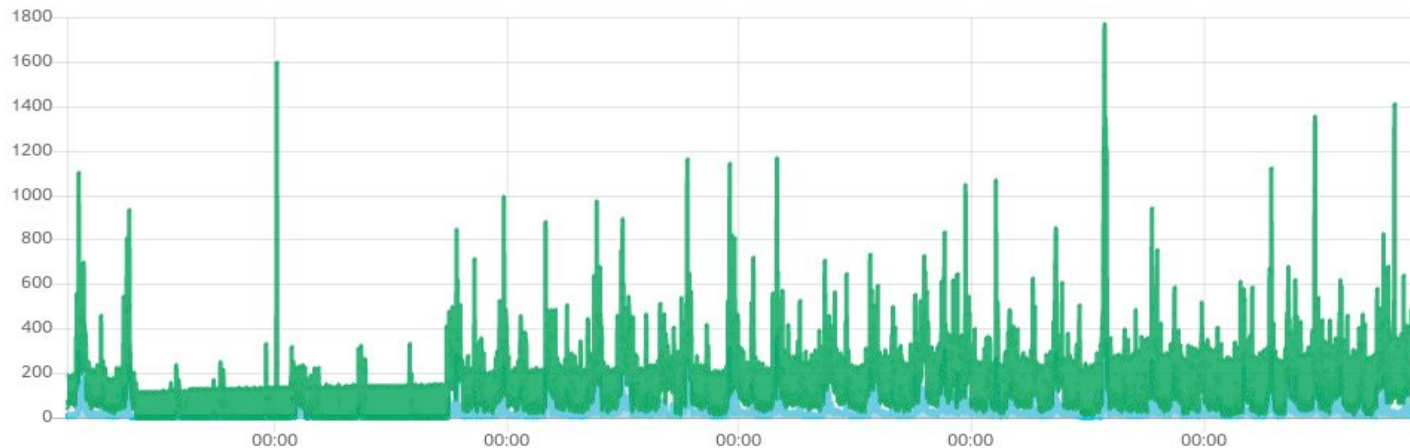


# Compute graphical statistics from the Pi-hole query database

Date and time range:

September 16th 2019, 13:32 to October 15th 2019, 13:32


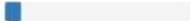
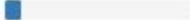
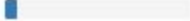
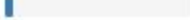





Queries over the selected time period



Last 30 Days

Last 30 Days

### Top Blocked Domains

Domain	Hits	Frequency
mobile.pipe.aria.microsoft.com	60415	
graph.instagram.com	9337	
settings-win.data.microsoft.com	9174	
v10.events.data.microsoft.com	6757	
www.googleadservices.com	4401	
e.crashlytics.com	2855	
browser.pipe.aria.microsoft.com	2749	
app-measurement.com	2418	
metrics.brightcove.com	1968	
app-analytics.snapchat.com	1842	

# 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?”

uBlock	Pi-Hole
<ul style="list-style-type: none"><li>● domain names</li><li>● URL fragments</li><li>● Content on the page<ul style="list-style-type: none"><li>○ HTML substrings</li></ul></li></ul>	<ul style="list-style-type: none"><li>● domain names</li></ul>



https://yt3.ggpht.com/a-/AAUE/mD6XJ6bc/p4Qrq-vcXdc

https://www.youtube.com/api/stats/qoe?event=streamin

https://www.youtube.com/get\_video\_info?html5=1&videoc

https://www.google.com/pagead/lvz?req\_ts=157111355

https://www.google.co.nz/pagead/lvz?req\_ts=157111355

https://lh3.googleusercontent.com/4VxFnOf3nduhdiRl8e

# 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*

### The Author



Hi, I'm Scott Helme, a Security Researcher, international speaker and author of this blog.

I'm also the founder of the popular [securityheaders.com](https://securityheaders.com) and [report-uri.com](https://report-uri.com), free tools to help you deploy better security!

<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

<b>uBlock / Browser Based</b>	<b>Pi-Hole</b>
Whitelist / disable filter on a per site basis	Whitelist / disable filter for all applications for all clients

# 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)





World Wide Web



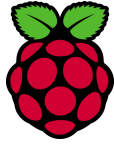
Clients



Pi-hole DNS Proxy

Network Perimeter  
• (Firewall)

Pi-hole DNS Proxy



World Wide Web

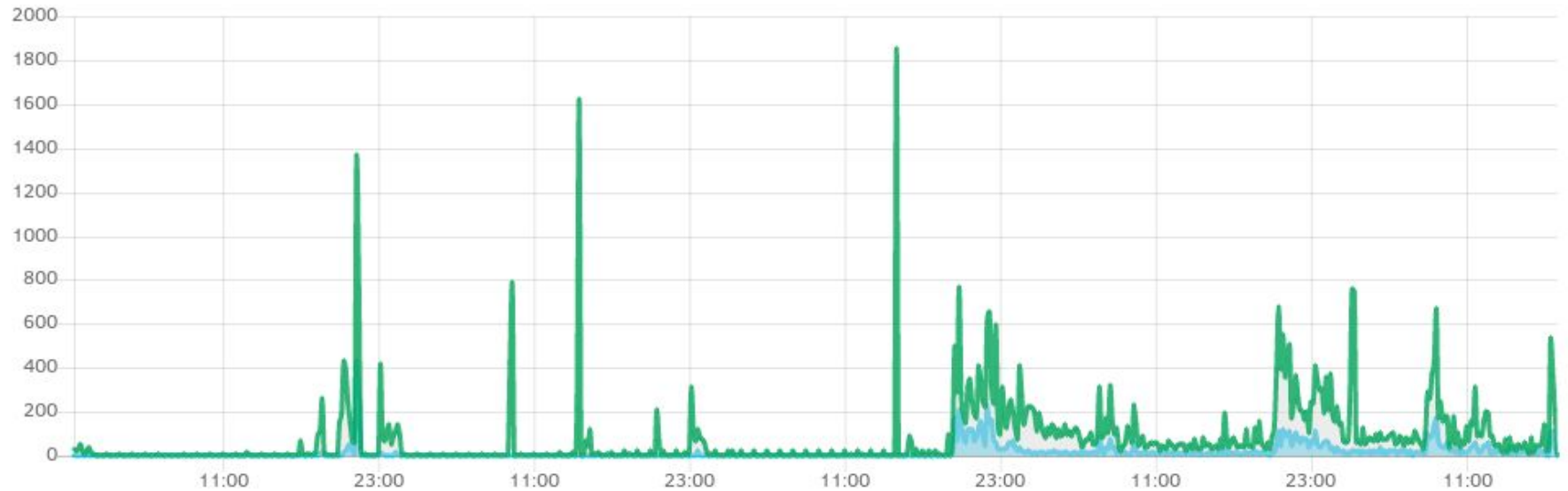


















Clients

Network Perimeter  
• (Firewall)

## First week on the Public Internet

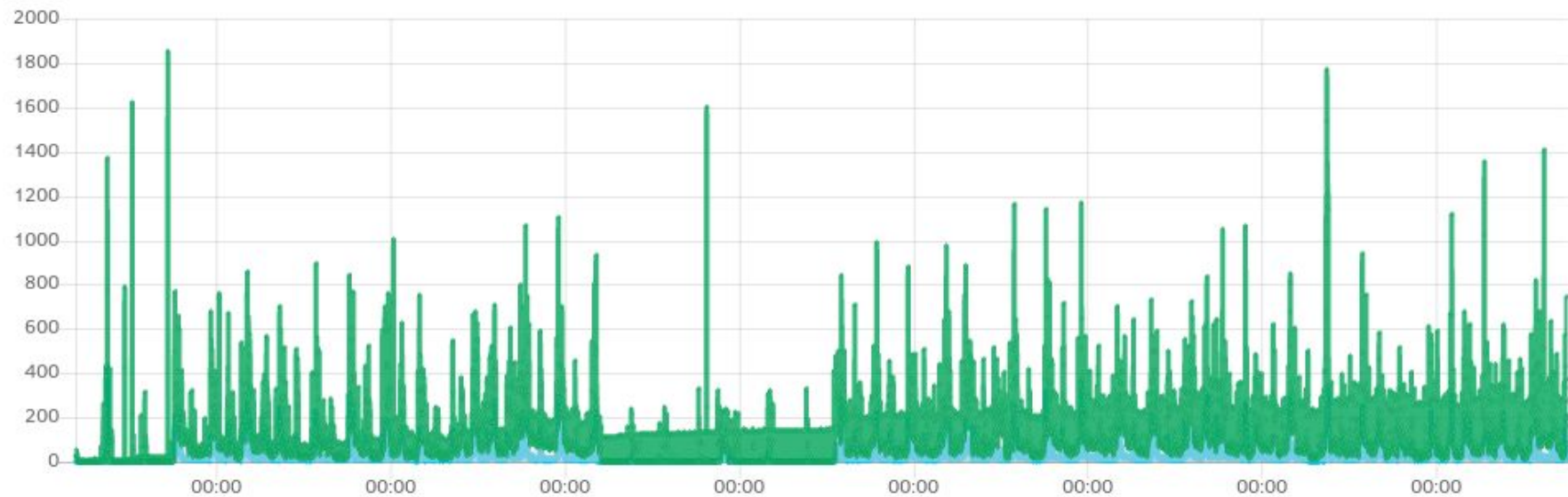
Queries over the selected time period



Time 	Type 	Domain 	Client 	Status 	Action 
2019-09-05 15:08:46	PTR	1.58.0.10.in-addr.arpa	195.37.190.69	OK (cached)	 Blacklist
2019-09-05 15:08:46	PTR	254.65.168.192.in-addr.arpa	195.37.190.69	OK (cached)	 Blacklist
2019-09-05 15:08:46	PTR	254.246.0.10.in-addr.arpa	195.37.190.69	OK (cached)	 Blacklist
2019-09-05 15:08:45	PTR	254.0.101.10.in-addr.arpa	195.37.190.69	OK (cached)	 Blacklist
2019-09-05 15:08:45	PTR	254.164.168.192.in-addr.arpa	195.37.190.69	OK (cached)	 Blacklist
2019-09-05 15:08:45	PTR	254.142.1.10.in-addr.arpa	195.37.190.69	OK (cached)	 Blacklist
2019-09-05 15:08:45	PTR	1.175.5.10.in-addr.arpa	195.37.190.69	OK (cached)	 Blacklist
2019-09-05 15:08:44	PTR	1.159.27.172.in-addr.arpa	195.37.190.69	OK (cached)	 Blacklist
2019-09-05 15:08:44	PTR	254.38.0.10.in-addr.arpa	195.37.190.69	OK (cached)	 Blacklist
2019-09-05 15:08:44	PTR	254.125.22.172.in-addr.arpa	195.37.190.69	OK (cached)	 Blacklist
Time	Type	Domain	Client	Status	Action

## 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

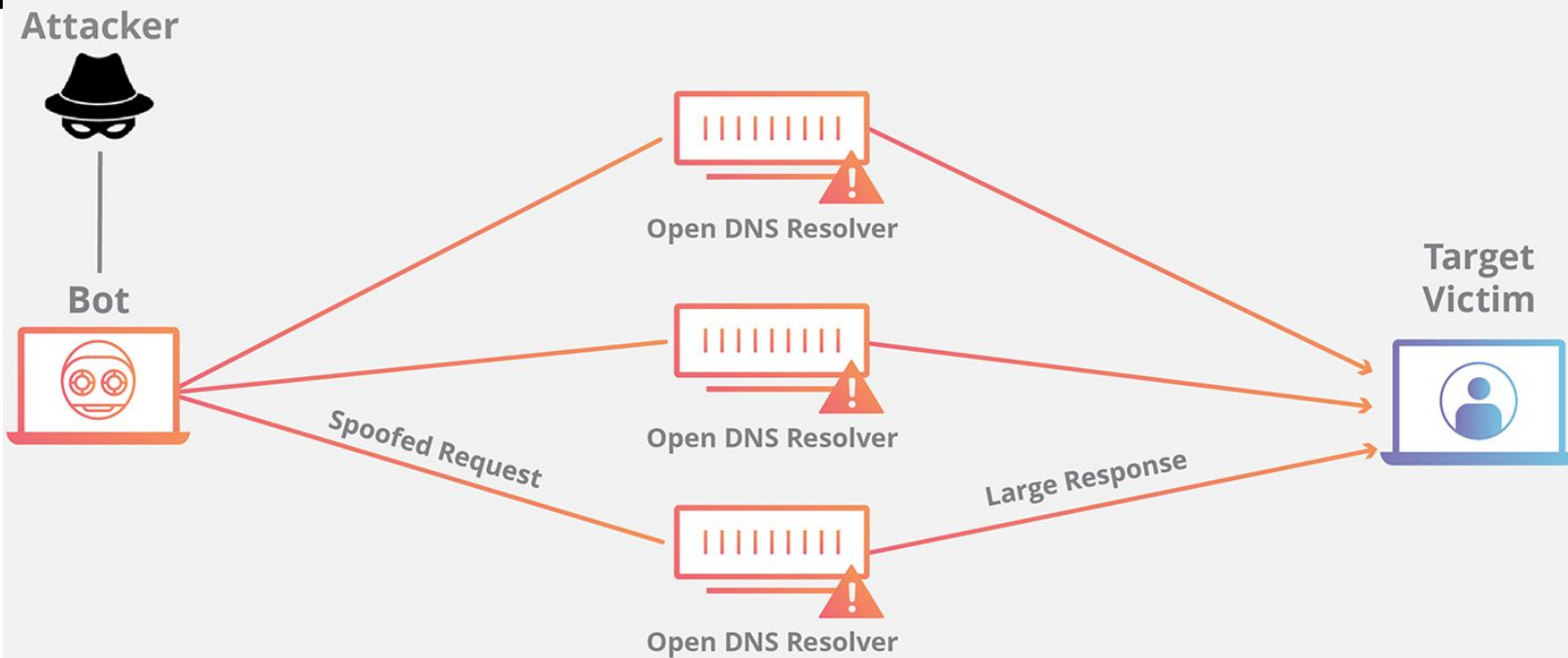
# DNS Amplification

[Products](#)[Solutions](#)[Resources](#)[For Developers](#)[For Enterprise](#)[Pricing](#)

## DNS Amplification Attack

DNS amplification is a DDoS attack that leverages DNS resolvers to overwhelm a victim with traffic.

DI





# The Right Way To Do It / Next Steps

Pi-Hole + VPN

- OpenVPN / Pi-VPN
- Wireguard