Bloqueando contido prexudicial con Pi-Hole

Quen son?

- Nome:
  - Guzmán Cernadas Pérez
- Redes sociais:
  - @DonCaralludo@defcon.social
  - @DonCaralludo
- Github:
  - https://github.com/Caralludo
- Membro de Hackliza

Introducción

- En internet existen moitas ameazas:
  - Estafas
  - Malware
  - Adware
  - Fake news
- O obxectivo destas ameazas é roubarche os cartos, infectar o teu ordenador, condicionar unha opinión...

Estafa

CNMV
COMISIÓN NACIONAL DEL MERCADO DE VALORES

27 de noviembre de 2023

La Comisión Nacional del Mercado de Valores (CNMV) advierte sobre las siguientes entidades:

Entidad advertida
immediate-momentum.com/es immediate-momentum.io/es IMMEDIATE MOMENTUM
FXNC FINANCIAL fxncfinancial.com/
BITECX BITECX.COM/
GAINGROUND gainground.live
EL MERCADO EFNX elmercado-efnx.com/
ACAPITAL GROUP acapitalgroup.co
QUANTUMAI / QUANTUM AI the-quantum-ai.com quantumai.investing-kapitals.com qai-uk.fin-bestplan.com quantumsai-sp.revepiy.com quantumaielonmusk.com quantumasist.com es.quantum-ai-official.com elonmuskquantumai.com quantums-ai.com quantumsai-sp.muzinoi.com quantum-ai.ca quantum-ai.com.au thequantumai.uk thequantum-ai.com/es quantumaitrading.net/es

La CNMV pone de manifiesto que dichas sociedades no figuran inscritas en el correspondiente registro de esta Comisión y, por tanto, no están autorizadas para prestar servicios de inversión u otras actividades sujetas a la supervisión de la CNMV.

Las advertencias de la CNMV sobre chiringuitos financieros pueden ser consultadas en la página web: Advertencias de la CNMV.

Malware

PurpleFox - Malware Domain Feed V2

CREATED 6 MONTHS AGO | MODIFIED 8 HOURS AGO by otxrobottwo_testing | Public | TLP: White

Command and Control domains for PurpleFox. These domains are extracted from a number of sources, and are suspicious.

Indicators of Compromise (13) | Related Pulses (9) | Comments (0) | History (0)

TYPES OF INDICATORS

Show 10 entries

TYPE	INDICATOR	ROLE	TITLE	ADDED	ACTIVE	RELATED PULSES
domain	ying.mom		Command and Control	Sep 15, 2023, 9:29:19 PM		1
domain	lqwljs.cn		PurpleFox Command and Control	Sep 24, 2023, 2:24:39 AM		7
hostname	4q663223f5.imdo.co		PurpleFox Command and Control	Sep 26, 2023, 3:34:53 AM		0
hostname	7002.aadaa1.cc		PurpleFox Command and Control	Oct 2, 2023, 6:36:04 AM		1
hostname	qlo.amqw.ir		PurpleFox Command and Control	Oct 4, 2023, 7:55:35 PM		1
hostname	oip.xioerabn.site		PurpleFox Command and Control	Oct 25, 2023, 9:07:14 PM		1
hostname	t1492261251.e1.luyouxia.net		PurpleFox Command and Control	Nov 4, 2023, 5:31:18 AM		0
domain	diupo249.top		PurpleFox Command and Control	Dec 5, 2023, 5:25:26 PM		3
hostname	xiaoyuwudi.e3.luyouxia.net		PurpleFox Command and Control	Feb 23, 2024, 4:21:29 AM		1
hostname	www.nsa.bet		PurpleFox Command and Control	Feb 23, 2024, 4:21:29 AM		1

Fake news

https://chemtrailsnews.com/2024-02-26-projects-block-sunlight-depopulation-bill-gates.html

CHEMTRAILSNEWS

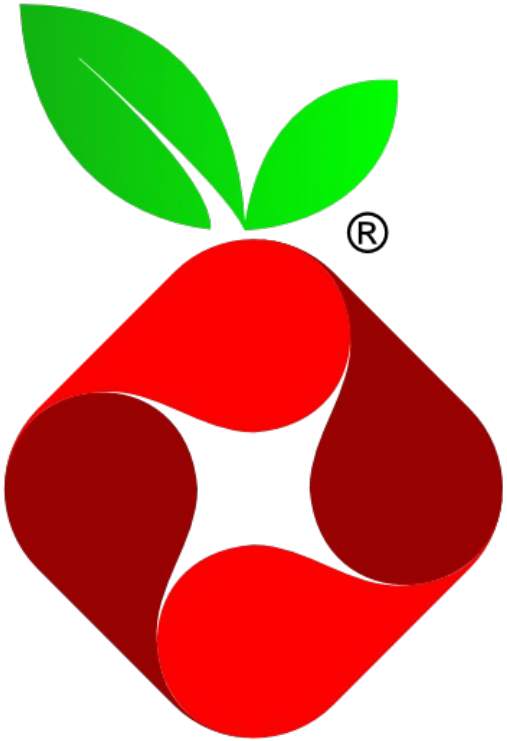
TAPWATER | WATERPURIFIERS | FRACKINGWATCH | FUKUSHIMAWATCH | METALS | CHEMTRAILSNEWS | Searc

Untested projects to block sunlight from reaching surface of the Earth touted by depopulation proponent Bill Gates

02/26/2024 / By Cassie B.

Que é Pi-Hole?

- Software para bloquear URLs
- Funciona a nivel de rede
- Pode executarse nunha Raspberry Pi

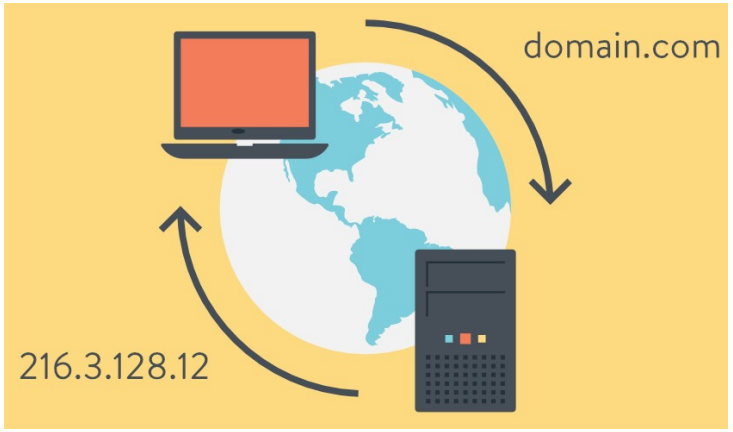


Por que utilizar isto?

- Mellorar a seguridade dos dispositivos dunha rede
  - Bloqueo de páxinas con malware ou phishing
  - Bloqueo de comunicacións de malware
- Quitar anuncios
  - Lixeira mellora no tempo á hora de cargar páxinas web
- Controlar acceso a determinadas páxinas
  - Apostas
  - Pornografía
  - Fake news

Como funciona?

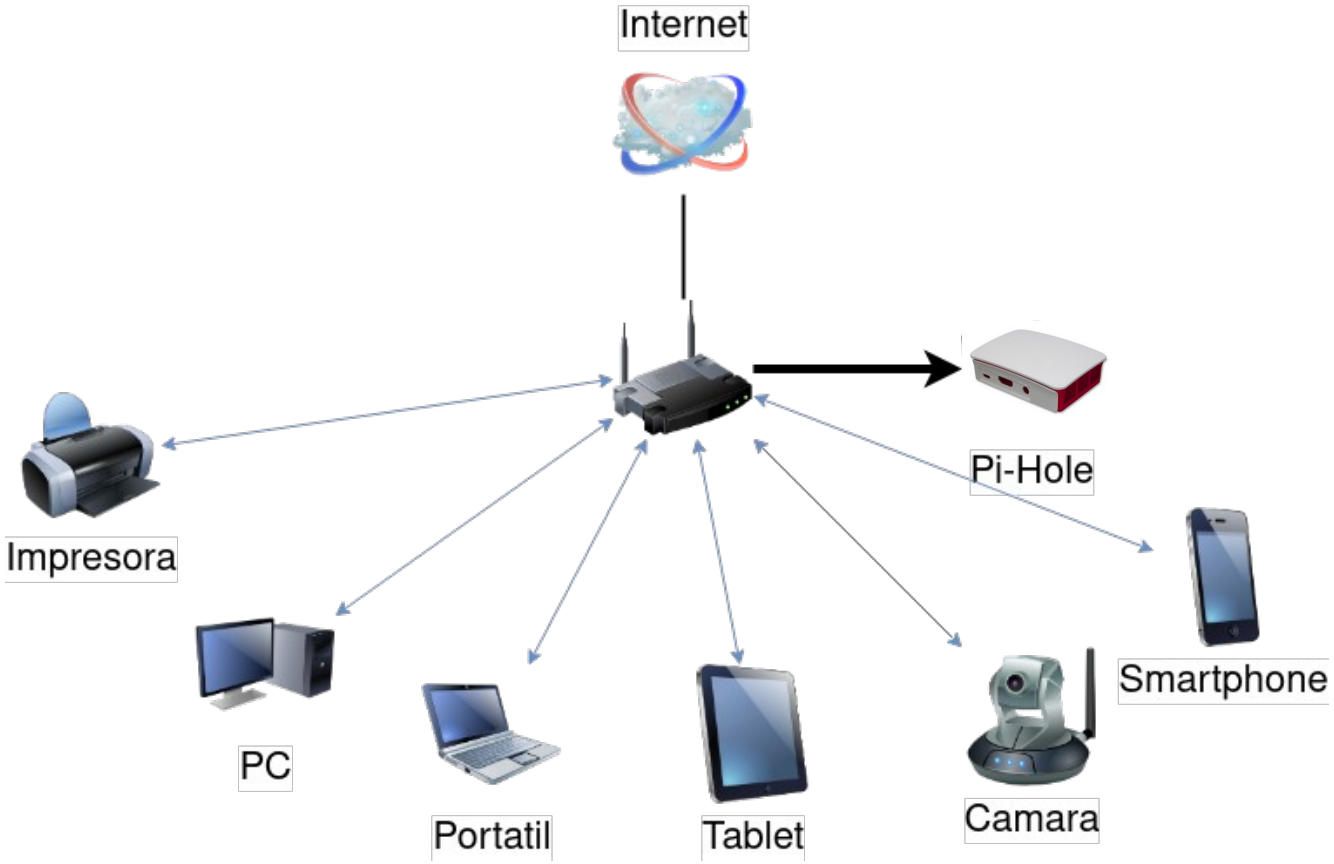
- Contexto:
  - As páxinas web accedese mediante un identificador chamado IP (como por exemplo 140.82.121.3)
  - Os servidores DNS (Domain Name System) transforman os nomes das páxinas a identificadores.



Como funciona?

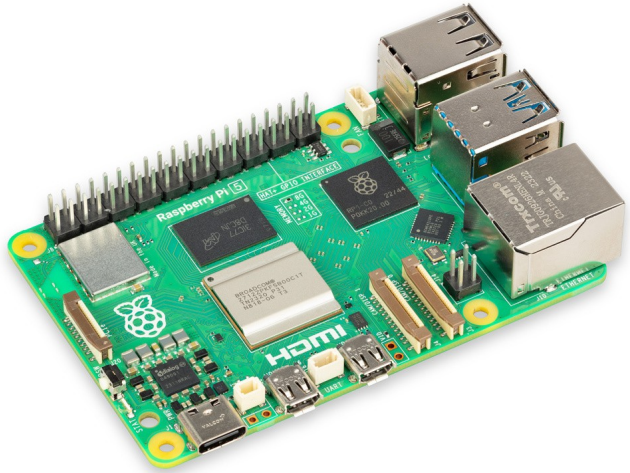
- Pi-Hole actúa coma un servidor DNS
- Todas as páxinas bloqueadas asígnaselles a dirección IP 0.0.0.0
  - 0.0.0.0 é unha dirección inválida
- Para o resto de páxinas, resolverá correctamente o nome dando a IP de verdade.

Como funciona?



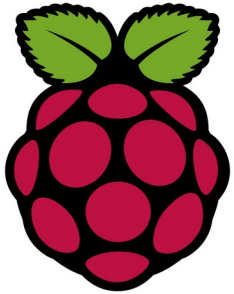
Hardware

- Raspberry Pi
- MicroSD 16 GB
- Cable de alimentación
- Carcasa (opcional)



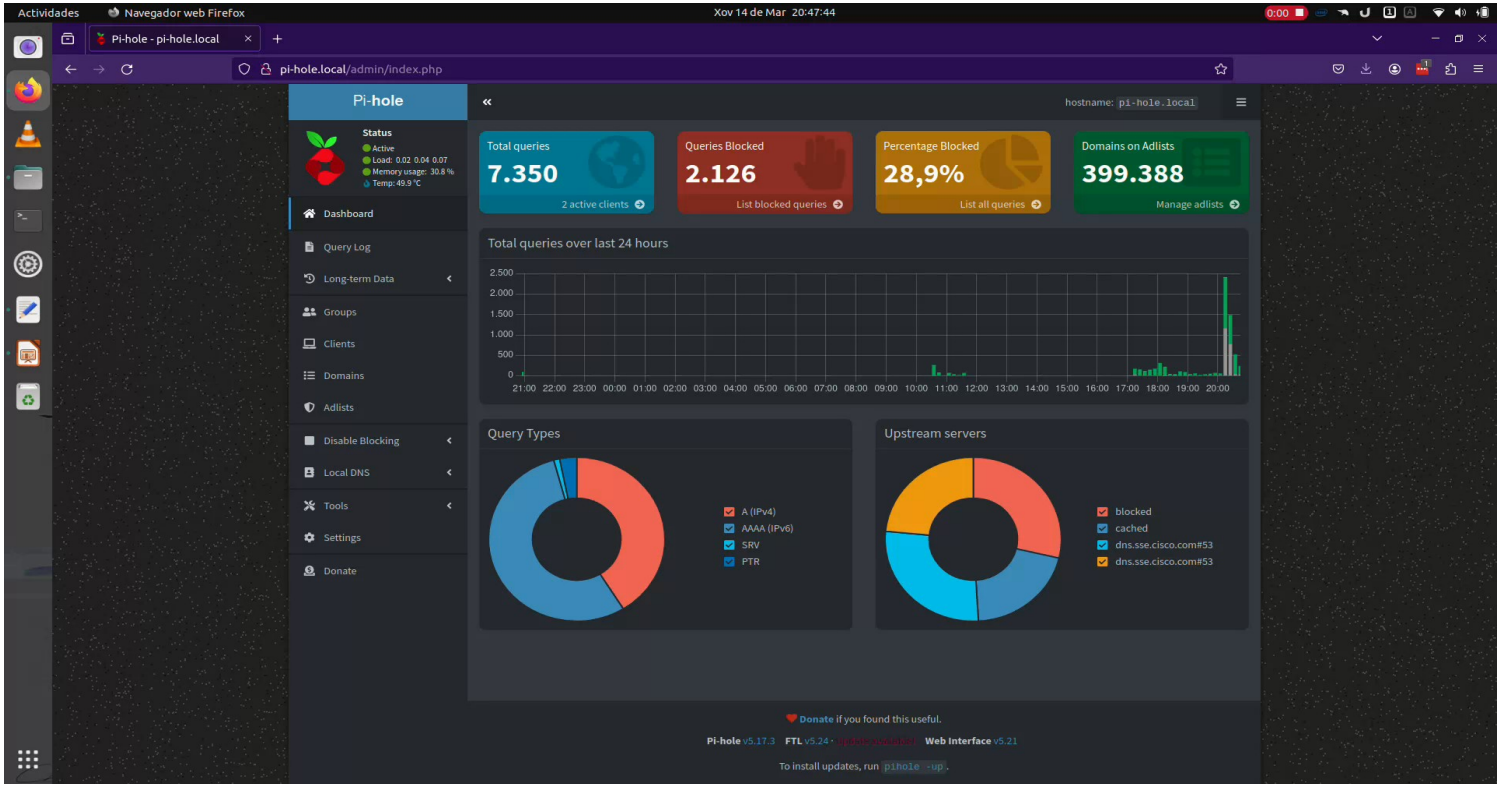
Software

- Sistemas Operativos:
  - Raspberry Pi OS
  - Armbian OS
  - Ubuntu
  - Debian
  - Fedora
- Software de Pi-Hole
  - https://github.com/pi-hole/pi-hole

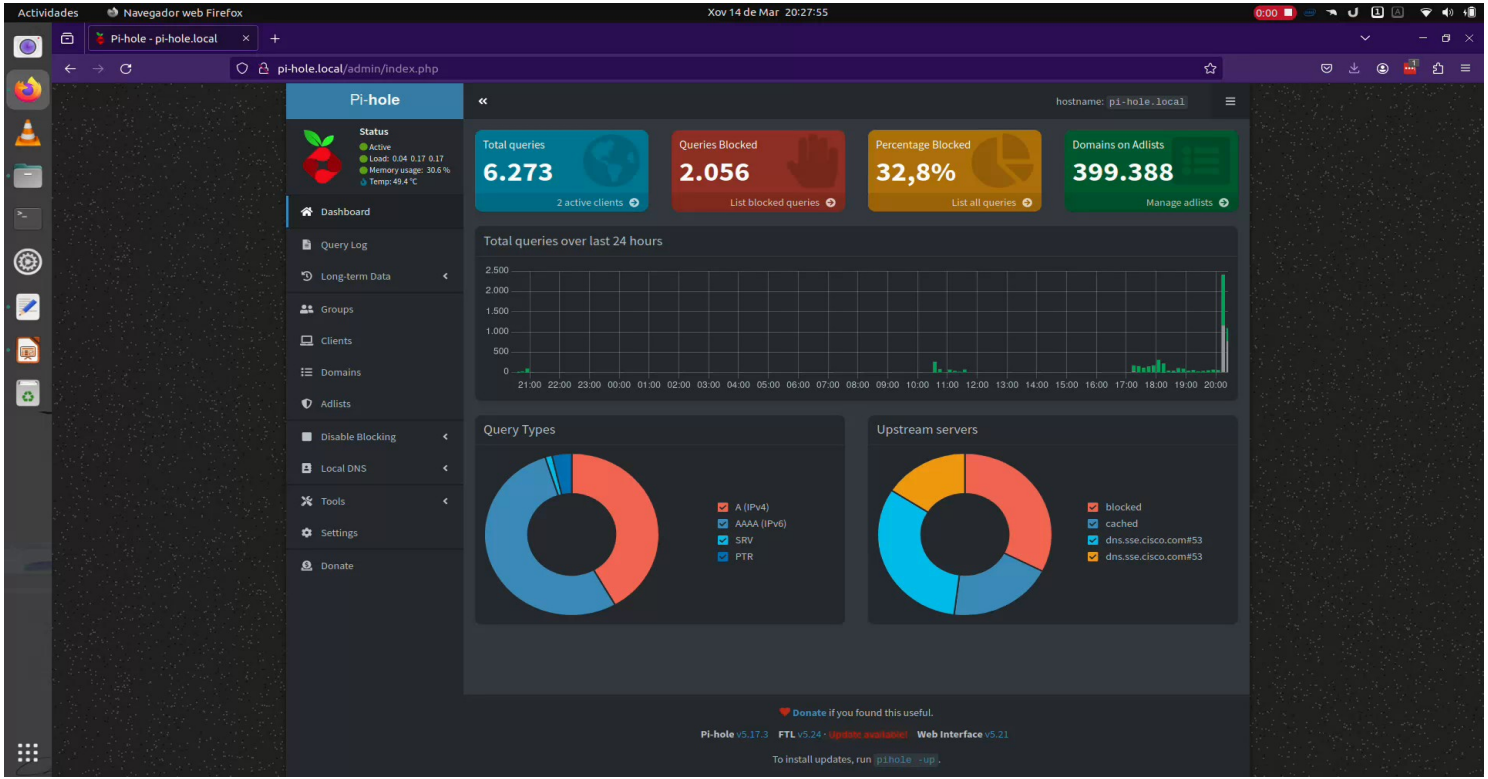


DEMO

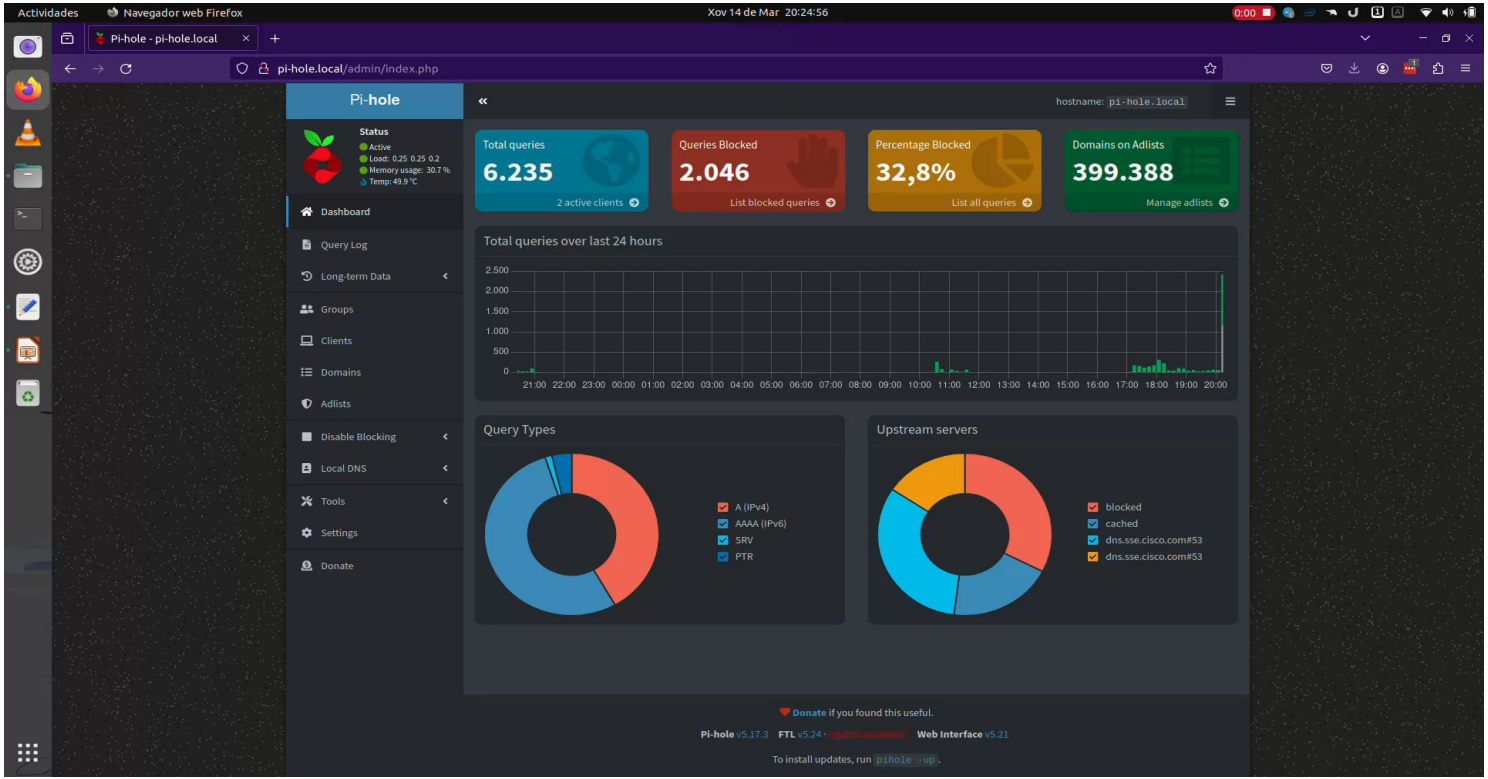
DEMO


Actividades
Navegador web Firefox
Xov 14 de Mar 20:47:44
Pi-hole - pi-hole.local
pi-hole.local/admin/index.php
Pi-hole
hostname: pi-hole.local
Status
Active
Load: 0.02 0.04 0.07
Memory usage: 30.8 %
Temp: 49.9 °C
Dashboard
Query Log
Long-term Data
Groups
Clients
Domains
Adlists
Disable Blocking
Local DNS
Tools
Settings
Donate
Total queries
7.350
2 active clients
Queries Blocked
2.126
List blocked queries
Percentage Blocked
28,9%
List all queries
Domains on Adlists
399.388
Manage adlists
Total queries over last 24 hours
Query Types
A (IPv4)
AAAA (IPv6)
SRV
PTR
Upstream servers
blocked
cached
dns.sse.cisco.com#53
dns.sse.cisco.com#53
Donate if you found this useful.
Pi-hole v5.17.3 FTL v5.24 Web Interface v5.21
To install updates, run pihole -up.

DEMO


Actividades
Navegador web Firefox
Xov 14 de Mar 20:27:55
Pi-hole - pi-hole.local
pi-hole.local/admin/index.php
Pi-hole
hostname: pi-hole.local
Status
Active
Load: 0.04 0.17 0.17
Memory usage: 30.6 %
Temp: 49.4 °C
Dashboard
Query Log
Long-term Data
Groups
Clients
Domains
Adlists
Disable Blocking
Local DNS
Tools
Settings
Donate
Total queries
6.273
2 active clients
Queries Blocked
2.056
List blocked queries
Percentage Blocked
32,8%
List all queries
Domains on Adlists
399.388
Manage adlists
Total queries over last 24 hours
Query Types
A (IPv4)
AAAA (IPv6)
SRV
PTR
Upstream servers
blocked
cached
dns.sse.cisco.com#53
dns.sse.cisco.com#53
Donate if you found this useful.
Pi-hole v5.17.3 FTL v5.24 · Update available! Web Interface v5.21
To install updates, run pihole -up.

DEMO

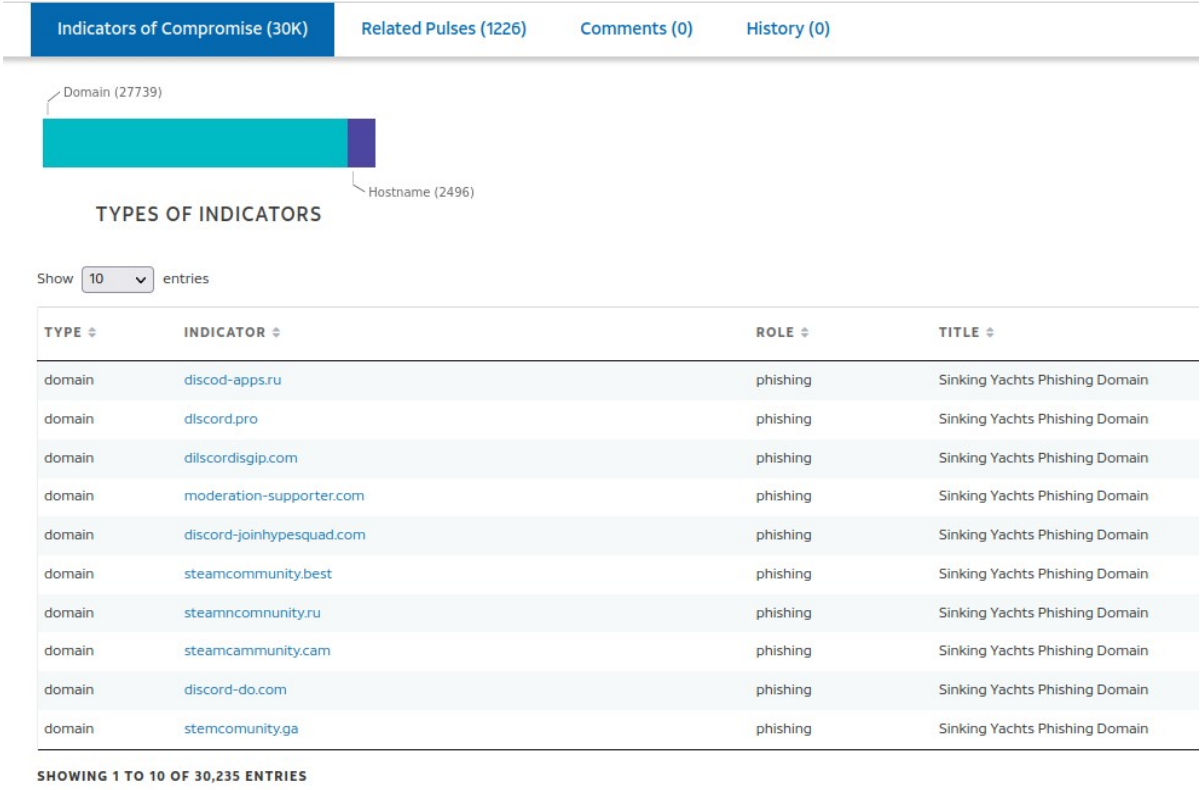

Actividades
Navegador web Firefox
Xov 14 de Mar 20:24:56
Pi-hole - pi-hole.local
pi-hole.local/admin/index.php
Pi-hole
Status
Active
Load: 0.25 0.25 0.2
Memory usage: 30.7 %
Temp: 49.9 °C
hostname: pi-hole.local
Dashboard
Query Log
Long-term Data
Groups
Clients
Domains
Adlists
Disable Blocking
Local DNS
Tools
Settings
Donate
Total queries
6.235
2 active clients
Queries Blocked
2.046
List blocked queries
Percentage Blocked
32,8%
List all queries
Domains on Adlists
399.388
Manage adlists
Total queries over last 24 hours
2.500
2.000
1.500
1.000
500
0
21:00 22:00 23:00 00:00 01:00 02:00 03:00 04:00 05:00 06:00 07:00 08:00 09:00 10:00 11:00 12:00 13:00 14:00 15:00 16:00 17:00 18:00 19:00 20:00
Query Types
A (IPv4)
AAAA (IPv6)
SRV
PTR
Upstream servers
blocked
cached
dns.sse.cisco.com#53
dns.sse.cisco.com#53
Donate if you found this useful.
Pi-hole v5.17.3 FTL v5.24 · update available Web Interface v5.21
To install updates, run pihole -up.

Listas de contido prexudicial

- Steven Black’s ad-hoc list
  - https://github.com/StevenBlack/hosts/
  - Moitas categorías (adware, malware, fakenews, apostas...)
  - Moitas combinacións
  - Máis de 200000 dominios únicos
  - Actualizase diariamente
- CERT’s nacionais
  - https://cert.pl/news/single/ostrzezenia_phishing

Listas de contido prexudicial

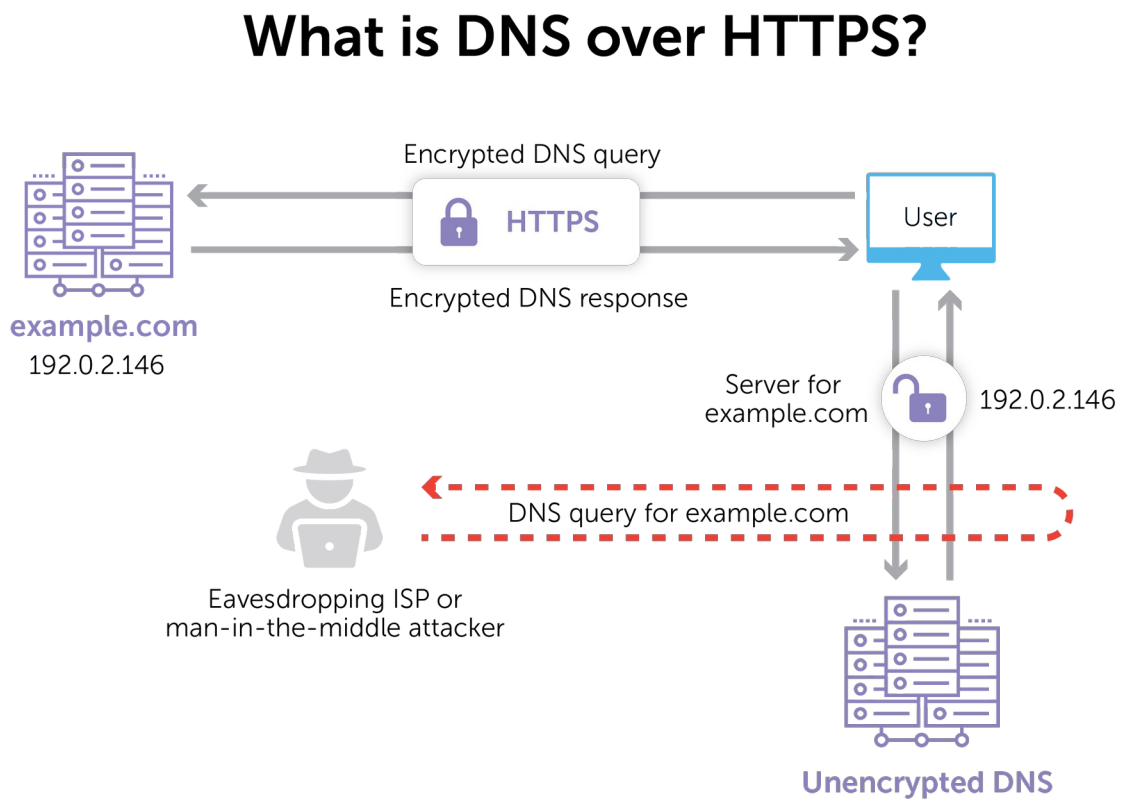
- Existen fontes con listas interesantes pero que teremos que tratar a man.
  - AlienVault
  - OpenPhish
  - Blackbook (https://github.com/stamparm/blackbook)
  - MISP



Limitacións

- Existen programas de escritorio e aplicacións de teléfono móbil que non envían os datos por DNS directamente.
- Estas aplicacións envían os datos por DNS-over-HTTPS
  - Google Chrome
  - Firefox
  - Aplicación de Android de YouTube
- Para que PI-Hole funcione hai que desactivar (onde de poida) DNS-over-HTTPS.

Limitacións



Limitacións

- Se aparece un novo dominio malicioso que non está na lista de bloqueos, poderase acceder igual.
- Pódense chegar a bloquear páxinas lexítimas.

Moitas Gracias!