

Forum:[Hack Forums](#)

Thread: [anyone have a script to block ads ?](#)

lvl99savage - January 16, 2024, 7:42 am

mainly youtube ads ?

Nostre - January 16, 2024, 7:49 am

Just use Brave. It has an adblocker built in.

Charlie Sheen - January 16, 2024, 8:56 am

(Jan 16, 2024 08:42 AM)lvl99savage Wrote: [\[CITE\]](#) mainly youtube ads ?

Consider buying a YouTube upgrade from someone here in the marketplace. They are usually pretty cheap and it beats using the adblockers. I heard recently YouTube upgraded their website to detect adblocking and stop you from being able to view them. Just a suggestion.

DashPHP - January 16, 2024, 8:59 am

I subscribed to YouTube premium via my bros family account. Fuck those ads.

Yodawarrior2 - January 16, 2024, 12:38 pm

(Jan 16, 2024 08:42 AM)lvl99savage Wrote: [\[CITE\]](#) mainly youtube ads ?

uBlock origin does the job pretty well for me.

Klonopin - January 16, 2024, 9:21 pm

(Jan 16, 2024 01:38 PM)Yodawarrior2 Wrote: [\[CITE\]](#) uBlock origin does the job pretty well for me.

indeed I also recommend ublock-origin.

never seen an ad in years.

Casey666 - January 17, 2024, 7:24 pm

Blocking Internet Ads Using DNS Sinkhole

Technitium DNS Server is an open source software that can be effectively used to block Internet Advertisements (Ads), adware, and malware on your computer or your local network using publicly available block lists.

Combined with DNS-over-TLS and DNS-over-HTTPS, Technitium DNS Server provides a good level security and privacy from network level DNS attacks and from adware. This makes it a must have tool if you are a privacy and security conscious person.

Technitium DNS Server is cross platform and works on Windows, Linux or macOS.

Technitium DNS Server v2.0

How Does It Work?

The Ad blocking feature works using the DNS Sinkhole method. With this feature enabled, for all the blocked domain names, the DNS Server will respond with 0.0.0.0 IPv4 address and :: for IPv6 address making the Ads fail to load making the website you visit free from Ads. This can not only block Ads but also adware, malware, social networks, porn etc. based on the block lists you configure in settings.

On your computer, you need to install the DNS Server and configure your network adapter's DNS settings to use the locally hosted DNS server. Once this is done, you need to configure the Block List URL settings to start blocking Ads. Once the DNS Server loads the block lists, it would respond with 0.0.0.0 IP address for the blocked websites making them fail to load.

You may also install the DNS Server on any spare computer on your network and configure your home or office router with IP address of this spare computer as DNS server in DHCP settings. With this setup, all your computers and devices like mobile phones would use the installed DNS Server blocking Ads and malware domains on all devices without installing any additional software on them.

Configuring Block Lists

To enable Ad blocking, you need to configure Block List URLs in the settings. Known and popular block lists are already listed in the Quick Add drop down list from where you can just click and add those URLs.

Technitium DNS Server Block List Configuration

If you are not sure, just select the Default option from the Quick Add drop down list and a default set of block list URLs would get configured.

Once done, click the Save Settings button at the bottom of the page to save the changes and start the block list download background process. These configured block lists are automatically downloaded every 24 hours to keep the DNS Server blocked zone updated.

If you have the DNS server installed directly on your computer then don't forget to configure your network adapter's DNS server settings to 127.0.0.1 (for IPv4) and ::1 (for IPv6). Without these network configuration changes, the DNS Server won't get any queries to respond to and things won't work as intended.

If you setup the DNS server to be used on the network by all devices then do configure your router's DHCP config and set the IP address of the computer running the DNS server as the DNS for your network. By configuring the router's DHCP, you don't need to manually configure any of your devices on the network.

IPv4 DNS Server Network Configuration

IPv6 DNS Server Network Configuration

That's It!

Once the configuration is done, just check the Dashboard on the web console after a couple of minutes to see the number of blocked domains in the Blocked Zones widget. If there are too many block list URLs configured, it may take a few more minutes for all of them to get downloaded and loaded.