Cygna Labs DNS Firewall Feed

The Cygna Labs DNS firewall feed provides the ability to configure your recursive DNS servers to block DNS responses for queries made to known or suspicious domains, IP addresses, and name server names or IP addresses. DNS firewall updates are provided with regular updates several times daily. Firewall updates are conveyed via standard TSIG-signed DNS protocol IXFRs, optionally via secure VPN.

Customers may also add their own feeds to supplement that from Cygna Labs for added customizability. For simplicity, two levels of feeds are provided to ease configuration if desired. Each level includes data from several reputable sources which are updated continually. Cygna Labs is also developing analytics capabilities to proactively detect suspected malware domains for vetting and real-time updating of our DNS firewall feed data.

Level 1: Basic

The Basic set provides basic security against the most well-known attackers, with a minimum of false positives.

- **Abuse.ch lists:**
  - **feodo** – contains command and control center addresses known as contacts for the four variants of the feodo malware trojan
  - **palevo** – contains command and control centers utilized by the palevo botnet kit
  - **sslbl** - a list of "bad" SSL certificates identified by abuse.ch to be associated with malware or botnet activities. SSLBL relies on SHA1 fingerprints of malicious SSL certificates and offers various blacklists
  - **ransomware_rw** - ransomware tracker tracks and monitors the status of domain names, IP addresses and URLs that are associated with fansomware, such as Botnet command and control (C&C) servers, distribution sites and payment sites
  - **zeus** – consists of the set of the known Zeus malware command and control centers
  - **zeus_badips** – contains the IPv4 addresses used by the Zeus trojan

This set of feeds is derived from the abuse.ch community who diligently track crime ware. Their blocklists are very focused. Keep in mind the zeus list may include some false positives as it doesn't exclude hijacked websites. You can use zeus_badips instead.

- **DShield.org list dshield – This feed contains the top 20 attacking class C (/24) subnets, over the last three days.**

- **Spamhaus.org lists**
  - DROP (Don't Route Or Peer) and EDROP are advisory "drop all traffic" lists, consisting of netblocks that are "hijacked" or leased by professional spam or cyber-crime operations (used for dissemination of malware, trojan downloaders, botnet controllers).
  - According to Spamhaus.org: When implemented at a network or ISP's 'core routers', DROP and EDROP will help protect the network's users from spamming, scanning, harvesting, DNS-hijacking and DDoS attacks originating on rogue netblocks.
  - Spamhaus strongly encourages the use of DROP and EDROP by tier-1s and backbones. Spamhaus is very responsive to adapt these lists when a network owner updates them that the issue has been solved.
- **Team-Cymru.org list**
  - bogons or fullbogons
  - These are lists of IP blocks that should not be routed on the internet and thus should not appear in IP packets or DNS query answers.
- **Bambenek Consulting – this feed consists of known, active and non-sinkholed malware command and C&C center IP addresses**

Level 2: Essentials

The Level 2 set provides protection against current brute force attacks. This level may have a small percentage of false positives, mainly due to dynamic IPs being re-used by other users.

OpenBL.org lists

The team of OpenBL tracks brute force attacks on their hosts. They have a very short list for hosts, under their own control, collecting this information, to eliminate false positives. They suggest to use the default blacklist which has a retention policy of 90 days (openbl), but they also provide lists with different retention policies (from 1 day to 1 year). Their goal is to report abuse to the responsible provider so that the infection is disabled.

Blocklist.de lists

Is a network of users reporting abuse mainly using fail2ban. They eliminate false positives using other lists available. Since they collect information from their users, their lists may be subject to poisoning, or false positives. They only include individual IPs (no subnets) which have attacked their users the last 48 hours and their list contains 20.000 to 40.000 IPs (which is small enough considering the size of the internet). Like openbl, their goal is to report abuse back, so that the infection is disabled. They also provide their blocklist per type of attack (mail, web, etc).

Geo-based supersets enable geographic based IP and domain blocking incorporating input from a variety of reputation sources.