

Sites with blacklist of malicious IPs and URLs

It's a good practice to block unwanted traffic to you network and company. For that you can use malicious IPs and URLs lists. Those lists are provided online and most of them for free. They differ in format, data-collection methodology and usage; therefore, you should carefully read about the list you choose before you put it in use. Here is a list of websites and services that are providing up-to-date blacklist of domains with suspicious activities.

Sites with blacklist of malicious IPs and URLs

- [Arbor Networks' Active Threat Level Analysis System \(ATLAS\)](#) "ATLAS is innovative, globally scoped threat analysis and monitoring system" – free
- [Team CYMRU's Bogon prefix](#) "A bogon prefix is a route that should never appear in the Internet routing table" – free
- [FireHOL IP List](#) "This site analyses all available security IP Feeds, mainly related to on-line attacks, on-line service abuse, malwares, botnets, command and control servers and other cybercrime activities." – free
- [Google Safe Browsing](#) "APIs to access the Google Safe Browsing lists of unsafe web resources" – free, restrictions apply
- [hpHosts' Database](#) "A community managed and maintained hosts file that allows an additional layer of protection against access to ad, tracking and malicious websites." – free, automation on request
- [Malc0de's Database](#) "A database of domains hosting malicious executables" – free
- <http://www.dshield.org/ipsascii.html>
- [MalwareDomainList.com Hosts List](#) – free

About LIFARS

LIFARS is an elite cybersecurity firm based in New York City. LIFARS conducts digital forensic investigations, incident response, web application security testing, digital risk assessments and academic research.

- [Malwaredomainlist.com Downloadable list](#) of IP address – free
- [Malware Patrol's open source](#) "The Malware Patrol project is an open source community for sharing malicious URLs." – free or paid subscription
- [MalwareURL](#) "A database with domains with malicious activity" – free with limited access or paid subscription
- [Openphish](#) "OpenPhish uses proprietary Artificial Intelligence algorithms to automatically identify zero-day phishing sites and provide comprehensive, actionable, real-time threat intelligence." – free (for non-commercial use)
- [PhishTank](#) "A phishing sites database - query database via API" – free
- [Project Honey Pot – Directory of Malicious IPs](#) – free, registration required
- [Scumware.org](#) "A list of dangerous domains and URLs" – free
- [ShadowServer](#) "Reports about malicious activities" – free, registration and approval required
- [Squid Blacklist](#) "A leading publisher of blacklists tailored for web content filtering purposes" – paid
- [Zeus Tracker :: Zeus blacklist](#) "It offers various IP- and domain-blacklists that contains known Zeus Command&Control server (C&C) associated with the Zeus crimeware" – free
- [BlockList.de](#) "A free and voluntary service that provides lists of the attackers IP addresses" – free
- [Internet Storm Center's Suspicious Domains List](#) "Various black lists of suspicious domains" – free
- [Networksec.org's Domain Blacklist](#) – free
- [DNSBL Information](#) "It provides a single place where you can check that blacklist status of your mail server's IP address on more than 100 DNS based blacklists" – free
- [IPVoid](#) "A free service used to scan an IP address through multiple DNS-based blacklists and IP reputation services" – free
- [IP Blacklist Cloud](#) "A list of blacklisted IPs by many websites" – free
- [URLBlacklist](#) "A commercial managed URL blacklist service" – paid
- [GitHub: Maravento Blackweb](#) "A blacklist for Squid source code on GitHub" – free
- [Support.clean-mx.com](#) – free for personal use, registration needed

Please keep in mind that most IP addresses are dynamic and that they can be used in the future for legitimate traffic. Hence, it's recommended to use regularly updated blacklists.

About LIFARS

LIFARS is an elite cybersecurity firm based in New York City. LIFARS conducts digital forensic investigations, incident response, web application security testing, digital risk assessments and academic research.