Cjoverkill User Manual :: Anticheat and Filters

Table of contents

1. Overview

CjOverkill Traffic Trade Script has very advanced anticheat filters designed to filter in real time practically all known hitbot attacks and using complex filtering routines based on suspicious behavior patterns to detect and filter even unknown hitbot attacks. All these filtering and anticheat options work completely unattended and in automatic mode without you need to care about them.

This manual explains in detail the following andticheat and filter methods:

- HTTP Request Method Filter
- HTTP Client Filter
- IP Filter
- IP Whitelist
- Country Filter
- Referrer Filter
- Maximum Raw Visits Per IP Anticheat and Filter Protection
- Maximum Clicks Per IP Anticheat and Filter Protection
- Timestamp Anticheat and Filter Protection
- Out of Range Productivity Anticheat Protection
- Proxy Attack Anticheat Protection
- Rampage Mode Filter Protections Setup

2. HTTP Request Method Filter

The HTTP request method filter blocks traffic based on the type of HTTP request it's making. You can access this filter by selecting the "Method Filter" option.

This filter will also filter any traffic that most automated proxy check bots and some security bugs searching spiders will attempt.

Some sites may require the POST method to be enabled, specially if the in.php include is placed on some page that retrieves user comments via POST.

The request method filter is shared between all the sites.

3. HTTP Client Filter

This filter blocks traffic based on the browser signature (HTTP client signature). With this filter you can block any kind of browser or web tool based on it's signature. This includes download bots, spiders, programming libraries used to develop web sucking clients and hitbots, etc...

You can access this filter using the "Client Filter" option.

The client filter is shared between all the sites. Any HTTP client added to that filter will be filtered on all the sites automatically.

4. IP Filter

The IP filter will allow you to filter given IPs or IP ranges. Usually it works completely automatic mode and it will filter any IP engaged in suspicious activities that are not very likely to be performed by humans. The automatic filter will remove IPs after 24 hours. If you add the IPs by hand they will never be removed.

You can access this filter configuration from the "IP Filter" option.

The IP filter is shared between all the sites, so one IP detected as a bot on one site will be automatically filtered on all of them.

5. IP Whitelist

The IP whitelist allws you to whitelist some IP or an IP range. When an IP is whitelisted it will never get filtered nor will be sent to trades or skimmed to external URLs. This whitelist is good if you want to make sure that search engine spiders don't get filtered on your site.

Take a look at the Rampage filter Setup part of this manual for a settings configuration that makes the IP whitelist not needed while being also very agressive against hitbots at the same time.

The IP whitelist is shared between all the sites.

6. Country Filter

The country filter works using a GeoIP database to determine the surfer country. Also some special countries like Anonymouns Proxy and satellite Provider are added to the list in order to allow seamless filtering of anonymous proxies. Each country can be filtered to a different site allowing better segregation of your traffic per geographical location.

You can configure the country filter from the "Country Filter" option in the admin panel. You can also copy the country filter configuration for one site to another site from there.

The country filter is configured per site and it's not shared between one site and another unless you copy the filter configuration from one site to the other.

7. Referrer Filter

The standard blacklist also works as referrer filter allowing you to filter all the traffic comming from a blacklisted domain. This also includes no referrer traffic or traffic sent from another domain but using the trade ID parameter of the blacklisted domain. This option is very useful when blacklisting trades that hitbot your sites because it makes sute that no more hitbot traffic from these sites is axxepted even if they continue sending it after you have stopped trading with them.

You can access the referrer domains blacklist by selecting the "Blacklist" option.

The domains blacklist is shared between all the sites. In addition, any domain that is blacklisted on your network will be unable to signup for trading with your sites.

8. Maximum Raw Visits Per IP Anticheat and Filter Protection

The maximum repetitive visits per IP filter allows you to configure how many times can a given IP visit your site in a 24 hours period. Usually surfers can visit your site 1 to 3 or 4 times in 24 hours, but not 25, so it's quite easy to see that something that makes too many raw visits in a short period is not a surfer but it's a bot.

This option will add the filtered IPs to the IP filter automatically and remove them also automatically when 24 hours have passed since the ofensive behavior.

This option configuration is managed in different ways.
The site settings panel allows you to configure the default parameters for new trades.
The trade Edit option will allow you to confiugure this setting per trade basis. You can also mass edit your trades to change this setting for all your trades too.

9. Maximum Clicks Per IP Anticheat and Filter Protection

The maximum clicks option allows you to configure how many clicks will be accepted as normal per IP before the hitbot trigger is set for that IP. A normal surfer usually doen's name 25 clicks on a normal TGP. Anyways, he could do much more clicks depending on the site kind. In this case it's wise to use some common sense with the configuration. You should also take a look at the Rampage Filter configuration for missconfiguration proof setting.

This option will add the filtered IPs to the IP filter automatically and remove them also automatically when 24 hours have passed since the ofensive behavior.

This option configuration is managed in different ways.
The site settings panel allows you to configure the default parameters for new trades.

The trade Edit option will allow you to confiugure this setting per trade basis. You can also mass edit your trades to change this setting for all your trades too.

10. Timestamp Anticheat and Filter Protection

This filter configuration allows you to configure how much time (in seconds) is too fast for repeated page loads or clicks. The default configuration for this parameter is 1 second. This pretty much discards almost all humans, except the ones that are too excited to see your site :)

This option will add the filtered IPs to the IP filter automatically and remove them also automatically when 24 hours have passed since the ofensive behavior.

This option configuration is managed in different ways.
The site settings panel allows you to configure the default parameters for new trades.
The trade Edit option will allow you to confiugure this setting per trade basis. You can also mass edit your trades to change this setting for all your trades too.

Take a look at the Rampage Mode filter setup for best use of this protection.

11. Out of Range Productivity Anticheat Protection

This anticheat protection allows you to configure the maximum and minimum productivity range for any trade. If the trade goes out of that range it will be considered cheating and the trade will be disabled.

This option configuration is managed in different ways.
The site settings panel allows you to configure the default parameters for new trades.
The trade Edit option will allow you to confiugure this setting per trade basis. You can also mass edit your trades to change this setting for all your trades too.

12. Proxy Attack Anticheat Protection

This anticheat setting allows you to configure the maximum percent of proxy traffic that can be sent to you from a trade. CjOverkill detects the real surfer IP if they use proxy, so that is just a complimentation to the other anticheat settings to help nailing cheating trades even faster.

This option configuration is managed in different ways.
The site settings panel allows you to configure the default parameters for new trades.
The trade Edit option will allow you to confiugure this setting per trade basis. You can also mass edit your trades to change this setting for all your trades too.

13. Rampage Mode Filter Protections Setup

The rampage filter mode is just a filter configuration I gave that name. It allows you to set very strict anticheat and filtering configuration and don't worry about false positives. Also will make sure that search engine spiders will get filtered in a way that will allow them to spider your sites without interfering with your stats.

Put in short... this configuration will stop everything rampaging on your site without harming your trades or your site. This is the default filter configuration for new created sites.

Configutatiopn settings follow:

- **Network Settings:** Bots management = Blacklist: Stop Counting
- **Site Edit:** Default Max Seconds Between Clicks = 1
- **Site Edit:** Repeated IP Protection = Enabled Blacklist IP
- **Site Edit:** Excesive Clicks Protection = Enabled Blacklist IP
- **Site Edit:** All anticheat and filter protections Enabled