Система выявления автоматизированных ботов Clickfraud

Руководство по установке
программного обеспечения

Листов 6

Санкт-Петербург 2025

Оглавление

Аннотация

Под программным обеспечением (далее – ПО) в настоящем документе понимается программное обеспечение **Система выявления автоматизированных ботов Clickfraud**, правообладателем которого является **общество с ограниченной ответственностью "ИНТЕРНЕТ ЗАЩИТА"**.

1 Введение

Данный документ содержит:

- технические требования к инфраструктуре функционирования программного обеспечения;
- руководство по установке программного обеспечения.

2 Технические требования к инфраструктуре функционирования ПО

Для установки программного обеспечения требуется компьютер со следующими системными характеристиками: CPU: 1 логическое ядро, частота – 1,4 ГГц и больше; RAM: 1 Гб и больше; HDD: свободное дисковое пространство – 6 Гб; 64-битная ОС Linux (например, Alt Linux Server).

3 Руководство по установке

Программное обеспечение **Система выявления автоматизированных ботов Clickfraud** реализовано в микросервисной архитектуре и представляет собой набор Docker-контейнеров.

Программное обеспечение поставляется в виде архива с конфигурационными файлами «clickfraud.zip».

Для работы с архивом в системе должен быть установлен пакет unzip, например:

 # apt-get install unzip

Для работы с docker, необходимо установить следующие пакеты:

docker.io

docker-compose-plugin

Ссылка на официальное руководство по установке Docker на дистрибутивы Linux: https://docs.docker.com/engine/install/.

Перед установкой необходимо создать рабочую директорию и разархивировать в неё конфигурационные файлы:

 # mkdir /opt/clickfraud

 # cd /opt/clickfraud

 # unzip clickfraud.zip

3.1 Задание параметров конфигурации сервиса

В файле /opt/clickfraud/clickfraud.env задайте значение для описанных в нем конфигурационных переменных:

- CLICKFRAUD_API_DOMAIN - домен, на который будут отправляться данные для анализа со стороны клиента. Домен указывается без схемы и без порта (порт задаётся другой переменной), т.е. если вы разворачиваете сервис по адресу https://example.com - укажите в качестве домена example.com.

- ALLOWED_CLIENT_DOMAINS - список доменов, запросы от которых разрешены со стороны клиентов и будут обрабатываться сервисом. Домены должны быть указаны в одну строчку, через запятую. К доменам в списке предъявляются те же требования, что и к домену CLICKFRAUD_API_DOMAIN, т.е. без схемы и без порта.

- CLICKFRAUD_API_HTTP_PORT - порт для прослушивания HTTP-запросов, занимаемый контейнером сервиса clickfraud-enterprise-api. Измените значение, если на вашем хосте уже есть процессы, использующие данный порт, в противном случае - оставьте значение по умолчанию.

Задайте данные, по которым сервис будет подключаться к СУБД PostgreSQL:

- В файле /opt/clickfraud/secrets/postgres_username.txt укажите имя пользователя, под которым сервис будет подключаться к базе данных. Имя пользователя указывается в явном виде в одну строчку, файл не должен больше содержать никаких данных.

- В файле /opt/clickfraud/secrets/postgres_password.txt укажите пароль, с использованием которого сервис будет подключаться к базе данных. Пароль указывается в явном виде в одну строчку, файл не должен больше содержать никаких данных.

В файле /opt/caddy/caddy.env задайте значение для описанных в нем конфигурационных переменных:

- В случае, если у вас имеется доверенный SSL сертификат, укажите пути к файлам сертификата и его ключа в качестве значений переменных SSL_CERT_PATH и SSL_CERT_KEY_PATH. Должны быть указаны оба значения. **ВАЖНО**: не указывайте значения для переменной LETS_ENCRYPT_CONSUMER_CERT_EMAIL, если заданы SSL_CERT_PATH и SSL_CERT_KEY_PATH.

- В случае, если у вас нет доверенного SSL сертификата, укажите адрес электронной почты, с использованием которого доверенный сертификат будет получен от сервиса Let's Encrypt, в качестве значения переменной LETS_ENCRYPT_CONSUMER_CERT_EMAIL. **ВАЖНО**: не указывайте значения для переменных SSL_CERT_PATH и SSL_CERT_KEY_PATH, если задан LETS_ENCRYPT_CONSUMER_CERT_EMAIL.

3.2 Загрузка docker-образа системы

Выполните вход в реестр docker для загрузки образа сервиса:

 # docker login registry.gitlab.notissimus.com

Загрузите *образ сервиса:*

 # docker pull registry.gitlab.notissimus.com/notissimus/clickfraud-enterprise:latest

3.3 Запуск системы

Выполните запуск контейнера с системой при помощи следующей команды:

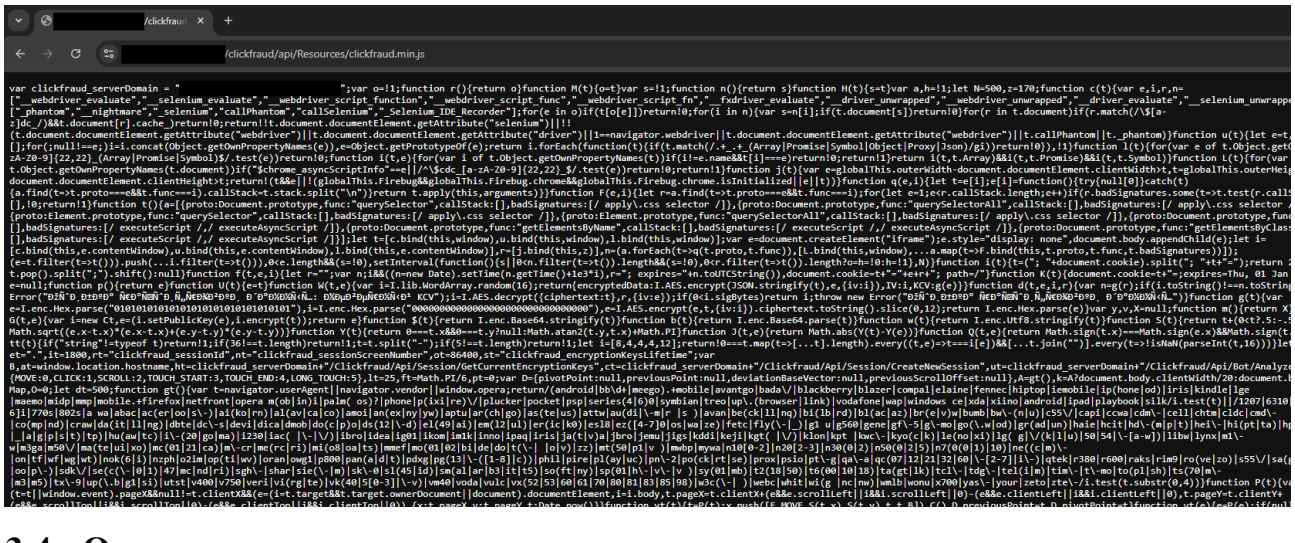
 # docker compose -f /opt/clickfraud/docker-compose.yml --env-file /opt/clickfraud/clickfraud.env up -d

Выполните запуск контейнера с сервисом Caddy при помощи следующей команды:

 # docker compose -f /opt/caddy/docker-compose.yml --env-file /opt/clickfraud/clickfraud.env --env-file /opt/caddy/caddy.env up -d

Теперь все запросы от клиентов по адресу https://${CLICKFRAUD_API_DOMAIN}/clickfraud/api/* и http://${CLICKFRAUD_API_DOMAIN}/clickfraud/api/* будут перенаправляться на работающий контейнер clickfraud-enterprise-api.

В целях тестирования выполните запрос по адресу https://${CLICKFRAUD_API_DOMAIN}/clickfraud/api/Resources/clickfraud.min.js, указав вместо ${CLICKFRAUD_API_DOMAIN} домен, на котором развернут сервис. Если сервис работает корректно, запрос будет выполнен с кодом 200, а результат запроса будет содержать минифицированный JavaScript код:



3.4 Остановка системы

Для остановки работы сервиса clickfraud-enterprise выполните следующую команду:

 # docker compose -p clickfraud-enterprise stop

Для остановки работы сервиса Caddy выполните следующую команду:

 # docker compose -p clickfraud-enterprise-reverseproxy stop